UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARD CIP-003-11

Lauren A. Perotti
Assistant General Counsel
Sarah P. Crawford
Counsel
North American Electric Reliability Corporation
1401 H Street, N.W., Suite 410
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
lauren.perotti@nerc.net
sarah.crawford@nerc.net

Counsel for the North American Electric Reliability Corporation

December 20, 2024

TABLE OF CONTENTS

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARD CIP-003-11

Pursuant to Section 215(d)(1) of the Federal Power Act ("FPA")[1] and Section 39.5[2] of the Federal Energy Regulatory Commission's ("FERC" or "Commission") regulations, the North American Electric Reliability Corporation ("NERC")[3] hereby submits for Commission approval proposed Reliability Standard CIP-003-11 (Cyber Security – Security Management Controls).[4] The purpose of Reliability Standard CIP-003 is to specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems ("BCS") against compromise that could lead to misoperation or instability in the Bulk Electric System ("BES"). Proposed Reliability Standard CIP-003-11 would mitigate the risks posed by a coordinated attack utilizing distributed low impact BES Cyber Systems by adding controls to authenticate remote users; protecting the authentication information in transit; and

[1] 16 U.S.C. § 824o.

[2] 18 C.F.R. § 39.5 (2024).

[3] The Commission certified NERC as the electric reliability organization ("ERO") in accordance with Section 215 of the FPA on July 20, 2006. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006), *order on reh'g & compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

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

detecting malicious communications to or between assets containing low impact BES Cyber Systems with external routable connectivity.

NERC requests that the Commission approve the proposed Reliability Standard CIP-003-11, as shown in **Exhibit A**, as just, reasonable, not unduly discriminatory or preferential, and in the public interest. NERC also requests that the Commission approve: (i) the associated Implementation Plan (**Exhibit B**), (ii) the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (**Exhibit E**); and (iii) the retirement of proposed Reliability Standard CIP-003-10, or the version of Reliability Standard CIP-003 then in effect.

As required by Section 39.5(a)[5] of the Commission's regulations, this petition presents the technical basis and purpose of the proposed Reliability Standard, a demonstration that the proposed Reliability Standard meets the criteria identified by the Commission in Order No. 672[6] (**Exhibit D**), and a summary of the standard development history (**Exhibit F**). The NERC Board of Trustees adopted the proposed Reliability Standard on December 10, 2024.

I. SUMMARY

The CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats. This approach requires that BES Cyber Systems or Facilities that could have the highest impact to the grid receive the highest level of protections; conversely, the Facilities that have the lowest impact to the grid receive the lowest level of protections.

---

[5] 18 C.F.R. § 39.5(a).

[6] The Commission specified in Order No. 672 certain general factors it would consider when assessing whether a particular Reliability Standard is just and reasonable. *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104 at PP 262, 321-37 [hereinafter Order No. 672], *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006).

In light of cybersecurity events and the evolving threat landscape, the NERC Board of Trustees took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously review and analyze facilities that house low impact BES Cyber Assets to consider the degrees of risk presented by these facilities and report on whether the low impact criteria should be modified.[7] To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts representative of a cross section of industry, called the Low Impact Criteria Review Team. In its report, the Low Impact Criteria Review Team recommended certain revisions to the CIP standards including: (1) Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity; (2) Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity; and (3) Requirement(s) for detection of malicious communications to or between assets containing low impact BES Cyber Systems with external routable connectivity.[8] The NERC Board of Trustees accepted the Low Impact Criteria Review Team's recommendations at its November 2022 meeting.[9]

As discussed in detail herein, proposed Reliability Standard CIP-003-11 would mitigate the risks posed by a coordinated attack utilizing distributed low impact BES Cyber Systems by

---

[7] February 4, 2021 NERC Board of Trustees Meeting Minutes at p. 7 (Withdrawal of Proposed Reliability Standard CIP-002-6), https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Minutes%20-%20BOT%20Open%20-%20Feb%204%202021.pdf.

[8] Exhibit F at Item 4, Low Impact Criteria Review Report – NERC Low Impact Criteria Review Team White Paper (Oct. 2022) [hereinafter LICRT Report] at p. v & 15.

[9] November 16, 2022 NERC Board of Trustees Meeting Minutes at pp. 6-7 (Low Impact Criteria Review Team), https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Minutes%20-%20BOT%20Open%20-%20Nov%2016%202022.pdf.

adding controls to authenticate remote users, protecting the authentication information in transit, and detecting malicious communications to or between assets containing low impact BES Cyber Systems with external routable connectivity.

NERC respectfully requests that the Commission approve proposed Reliability Standard CIP-003-11 and the associated elements as just, reasonable, not unduly discriminatory or preferential, and in the public interest.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[10]

Lauren A. Perotti*
Assistant General Counsel
Sarah P. Crawford*
Counsel
North American Electric Reliability Corporation
1401 H Street NW
Suite 410
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
lauren.perotti@nerc.net
sarah.crawford@nerc.net

Soo Jin Kim*
Vice President, Engineering and Standards
Jamie Calderon*
Director, Standards Development
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595 – facsimile
soo.jin.kim@nerc.net
jamie.calderon@nerc.net

III. REGULATORY BACKGROUND

A. Regulatory Framework

By enacting the Energy Policy Act of 2005,[11] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Bulk-Power System ("BPS"), and with the duties of certifying an ERO that would be charged with developing and

[10] Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of 18 C.F.R. § 385.203(b) to permit the inclusion of more than two people on the service list.

[11] 16 U.S.C. § 824o.

enforcing mandatory Reliability Standards, subject to Commission approval. Section 215(b)(1)[12] of the FPA states that all users, owners, and operators of the BPS in the United States will be subject to Commission-approved Reliability Standards. Section 215(d)(5)[13] of the FPA authorizes the Commission to order the ERO to submit a new or modified Reliability Standard. Section 39.5(a)[14] of the Commission's regulations requires the ERO to file with the Commission for its approval each new Reliability Standard that the ERO proposes should become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes should be made effective.

The Commission is vested with the regulatory responsibility to approve Reliability Standards that protect the reliability of the BPS and to ensure that Reliability Standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest. Pursuant to Section 215(d)(2) of the FPA[15] and Section 39.5(c)[16] of the Commission's regulations, the Commission will give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard.

B. NERC Reliability Standards Development Procedure

The proposed Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process. NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual.[17]

---

12 *Id.* § 824o(b)(1).

13 *Id.* § 824o(d)(5).

14 18 C.F.R. § 39.5(a).

15 16 U.S.C. § 824o(d)(2).

16 18 C.F.R. § 39.5(c)(1).

17 The NERC Rules of Procedure, including Appendix 3A, NERC Standard Processes Manual, are available at https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

In its order certifying NERC as the Commission's ERO, the Commission found that NERC's rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards,[18] and thus satisfy several of the Commission's criteria for approving Reliability Standards.[19] The development process is open to any person or entity with a legitimate interest in the reliability of the BPS. NERC considers the comments of all stakeholders. Stakeholders must approve, and the NERC Board of Trustees must adopt, a new or revised Reliability Standard before NERC submits the Reliability Standard to the Commission for approval.

C. History of the Low Impact Criteria Review

On December 13, 2020, FireEye Inc., a cybersecurity solutions and forensics firm, publicly posted details about an attack on the Orion platform developed by SolarWinds.[20] This attack was particularly damaging for victims because in order to function the SolarWinds Orion platform must have broad and privileged access to the networks it manages, including both the corporate and operational networks of an entity. The breach provided the opportunity for an adversary to monitor network traffic and compromise systems, which could result in disruption of operations.[21]

On December 13, 2020, the U.S. Department of Homeland Security's ("DHS") Cybersecurity and Infrastructure Security Agency ("CISA"), issued Emergency Directive 21-01.[22] This Directive required Federal agencies to take action based on the DHS assessment that a successful compromise from the SolarWinds Orion platform attack would have "grave"

---

18 *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 at P 250 (2006).

19 Order No. 672 at PP 268, 270.

20 LICRT Report, *supra*, at vi.

21 *Id.* at vi.

22 *Id.* at vii.

consequences.[23] On December 15, 2020, the White House National Security Council established a Cyber Unified Coordination Group composed of multiple Federal agencies to coordinate the investigation and remediation of the "significant" cyber incident.[24] On December 17, 2020, CISA issued Alert AA20-352A, directed toward the private sector, which described the attack for industry, the affected products, and the mitigation recommendations.[25]

In response, FERC staff and the NERC Electricity Information Sharing and Analysis Center ("E-ISAC") jointly prepared a white paper[26] emphasizing the need for continued vigilance by the electricity industry related to supply chain compromises and incidents and recommending specific cybersecurity mitigation actions to better ensure the security of the BPS.[27] While focusing primarily on the ongoing cyber event related to the attack on the Orion platform developed by SolarWinds and related Microsoft's 365/Azure Cloud compromise, it also addressed related compromises in products such as Pulse Connect Secure.[28] Because of the wide use of the SolarWinds Orion platform and the adversarial tactics used, even entities that did not install the SolarWinds Orion platform on their networks could still be impacted.[29]

In light of these cybersecurity events and the evolving threat landscape, the NERC Board of Trustees took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis of facilities that house low

---

23 *Id.* at vii.

24 *Id.* at vii.

25 *Id.* at vii.

26 FERC and E-ISAC, SolarWinds and Related Supply Chain Compromise - Lessons for the North American Electricity Industry (July 2021), https://www.nerc.com/pa/CI/ESISAC/Documents/SolarWinds and Related Supply Chain Compromise White Paper.pdf.

27 LICRT Report, *supra*, at vii.

28 *Id.* at vii.

29 *Id.* at vii.

impact BES Cyber Assets.[30] In particular, the NERC Board of Trustees asked that NERC staff and stakeholders consider the degrees of risk presented by various facilities that house low impact BES Cyber Assets and report on whether the low impact criteria should be modified.[31]

To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts representative of a cross section of industry, called the Low Impact Criteria Review Team. The Low Impact Criteria Review Team's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber-attack on low impact BES Cyber Systems. In its report, the Low Impact Criteria Review Team documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommended actions to address those risks. The NERC Board of Trustees accepted the recommendations of the Low Impact Criteria Review Team at its November 16, 2022 meeting, which included further revisions to CIP Reliability Standards.[32]

The Low Impact Criteria Review Team report recognized that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. Specifically, the Low Impact Criteria Review Team conclusions regarding low impact BES Cyber Systems are as follows:

- Individually, low impact BES Cyber Systems are truly low impact to BES reliability. This corresponds to the longstanding work of NERC and the stakeholders to design and operate the BES to withstand the loss of any of its individual assets. A medium or high impact BES Cyber System is more than an impact to a typical single BES Element/Facility. Therefore, the [Low Impact Criteria Review Team] does not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems.[33]

---

30 *Id.* at vii.

31 *Id.* at vii.

32 November 16, 2022 NERC Board of Trustees Meeting Minutes at pp. 6-7 (Low Impact Criteria Review Team); https://www.nerc.com/gov/bot/Agenda highlights and Mintues 2013/Minutes - BOT Open - Nov 16 2022.pdf.

33 LICRT Report, *supra*, at iv & 15.

- The [Low Impact Criteria Review Team] recognizes that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The [Low Impact Criteria Review Team] recommends enhancing the existing low impact category to further mitigate the coordinated attack risk.[34]

The Low Impact Criteria Review Team report recommended the following revisions to the CIP standards: (1) Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity; (2) Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity; and (3) Requirement(s) for detection of malicious communications to or between assets containing low impact BES Cyber Systems with external routable connectivity.[35]

D. Virtualization revisions set forth in proposed Reliability Standard CIP-003-10

NERC serves as the ERO in multiple jurisdictions, each with its own process for recognizing Reliability Standards. To ensure efficient development of standards, it is NERC's general practice that drafting teams revise the version of a Reliability Standard that has most recently been adopted by the NERC Board of Trustees. For this reason, the Project 2023-04 drafting team layered its revisions on top of the virtualization revisions set forth in proposed Reliability Standard CIP-003-10, which is pending before the Commission.[36] The changes that are

---

[34] *Id.* at v & 15.

[35] *Id.* at v & 15.

[36] *See Petition of the N. Am. Elec. Reliability Corp. for Approval of Critical Infrastructure Protection Reliability Standards*, Docket No. RM24-8-000 (July 10, 2024) [hereinafter Virtualization Petition].

proposed in CIP-003-10 are incorporated into CIP-003-11.[37] A detailed discussion of Project 2016-02 and the pending revisions to proposed Reliability Standard CIP-003-10 may be found in the petition in FERC Docket No. RM24-8-000.[38] For reference, the blackline of the proposed virtualization revisions in proposed Reliability Standard CIP-003-10 Attachment 1 Sections 3 and 6 are as follows:

> **Section 3.** Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:
>
> **3.1** Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:
>
> i. ~~between~~Between:
> - a low impact ~~BES Cyber System(s)~~ BCS; or
> - An SCI that supports a low impact BCS

> and a Cyber ~~Asset~~System(s) outside the ~~asset containing low impact BES Cyber System(s);~~:
> - the low impact BCS(s); or
> - the SCI that supports a low impact BCS;

> ii. using a routable protocol when entering or leaving the asset containing the low impact ~~BES Cyber System(s);~~BCS or SCI that supports a low impact BCS; and
>
> iii. not used for time-sensitive ~~protection or control functions between intelligent electronic devices (e.g.,~~ communications ~~using protocol IECTR-61850-90-5 R-GOOSE).~~of Protection Systems.
>
> **3.2** Authenticate all Dial-up Connectivity, if any, that provides access to low impact ~~BES Cyber System(s),~~BCS or SCI that supports a low impact BCS, per ~~Cyber Asset~~system capability.

[37] Exhibit A-2 provides a redline of all of the changes to CIP-003 from currently FERC-approved CIP-003-9 to the currently proposed CIP-003-11 and is inclusive of the changes proposed in CIP-003-10. Exhibit A-3 shows in redline the changes from the most recent NERC Board of Trustees approved version, CIP-003-10, to the proposed CIP-003-11, discussed herein.

[38] *See* Virtualization Petition, *supra*.

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

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

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

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

IV. JUSTIFICATION FOR APPROVAL

In this petition, NERC submits for Commission approval proposed Reliability Standard CIP-003-11 – Cyber Security – Security Management Controls. As discussed below and in **Exhibit C**, the proposed Reliability Standard would enhance reliability by mitigating the risk posed by a coordinated attack utilizing distributed low impact BES Cyber Systems. To address this threat, the proposed standard would add controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications to or between assets containing low impact BES Cyber Systems with External Routable Connectivity.

As discussed in detail below, the proposed standard would merge Sections 3 and 6 in Attachment 1 in order to have a single section for all electronic access with sub-sections providing additional requirements based on the type of access (vendor, dial-up, local, etc.). The drafting team also made conforming changes to Attachment 2 merging Sections 3 and 6 and provided examples of compliance related activities.

As explained in **Exhibit F**, NERC developed the proposed Reliability Standard using NERC's standard development process. This process included multiple public comment and ballot

periods. The NERC Board of Trustees adopted the proposed Reliability Standard on December 10, 2024.

Below, NERC provides an overview of the proposed revisions to Attachments 1 and 2, with a summary of the supporting rationale. Additional information may be found in the Technical Rationale for Proposed Reliability Standard CIP-003-11, included as **Exhibit C** to this petition, as well as the Complete Record of Development, included as **Exhibit F**.

A. Title, Purpose, Applicability, and Requirements

The title of proposed Reliability Standard CIP-003-11 Cyber Security — Security Management Controls remains unchanged from the currently FERC-approved version. The revisions proposed by Project 2023-04 do not include changes to the purpose and applicability sections of the CIP-003 standard. However, as discussed above, because the Project 2023-04 drafting team revised the version of CIP-003 that has been most recently approved by the NERC Board of Trustees, but is currently pending before the Commission for approval,[39] there are several changes to the purpose and applicability sections from the current FERC-approved version, CIP-003-9. The rationale for these changes is not set forth in the instant petition but may be found in the petition for approval of proposed Reliability Standard CIP-003-10.[40]

The only new change that has been made to the requirements by the Project 2023-04 drafting team is the removal of Requirement R1 Part 1.2.6 Vendor electronic remote access security controls. This change reflects the deletion of Attachment 1 Section 6, Vendor Electronic

---

39 *See id.*

40 *See id.* The changes that are proposed in CIP-003-10 and incorporated into CIP-003-11 include the following: the use of the acronym BCS in the purpose; the replacement of the term "Cyber Asset" with "Cyber System" throughout; and the inclusion of a new sub-section under Facilities, Section 4.2.3.3 for Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

Remote Access and Security Controls, which was combined into Attachment 1 Section 3, Electronic Access Controls.

B. Attachment 1

Proposed Reliability Standard CIP-003-11 would revise Attachment 1 by combining Section 3 (Electronic Access Controls) and Section 6 (Vendor Electronic Remote Access and Security Controls) into a new revised Section 3. These sections were identified by the drafting team as ideal locations to propose revisions to CIP-003-11 due to their focus on electronic access controls and vendor electronic remote access security controls.[41] The changes to Section 3 are shown in blackline as follows:[42]

> **Section 3.** Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.
>
> **3.1** For each asset containing low impact ~~BES Cyber Systems~~ BCS identified pursuant to CIP-002 ~~the Responsible Entity shall implement~~ and for SCI that supports a low impact BCS, if any, where electronic access ~~controls to~~ is:
> ~~Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are~~
>
> i. Between:
> • a low impact BCS; or
> • ~~An~~an SCI that supports a low impact BCS
>
> and a Cyber System(s) outside the asset containing:
> • the low impact BCS(s); or
> • the SCI that supports a low impact BCS;

[41] Exhibit C, Technical Rationale at 3.

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

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

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

~~Authenticate~~the Responsible Entity shall implement one or more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic access;

3.1.3 Authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted;

3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System(s) outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- the authentication system used to meet Section 3.1.3, or

- the asset containing low impact BCS or SCI that supports a low impact BCS;

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, the Responsible Entity shall implement one or more control(s) that authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

While merging Sections 3 and 6, the drafting team made conforming changes to certain language. Specifically, the proposed standard would use the phrase "implement controls" to replace "implement a process" or "implement one or more method(s)". This change reflects that a "control" may include an operation, process, procedure, or technology as described in the examples of Attachment 2.[43] Additionally, the proposed standard would remove the word "remote" from the phrase "electronic remote access" as the section would now include all electronic access as described in Attachment 1 Section 3 Part 3.1, (i), (ii), and (iii).[44]

1. Attachment 1, Section 3.1

Proposed Reliability Standard CIP-003-11 Attachment 1 would generally maintain the language used in proposed Reliability Standard CIP-003-10, Section 3.1, subsections (i) - (iii).

a) Section 3.1.1

Proposed Attachment 1 Section 3.1.1 is intended to preserve the language used in proposed Reliability Standard CIP-003-10, Section 3.1.[45]

---

43 *Id.* at 3.

44 *Id.* at 3.

45 Exhibit C, Technical Rationale at 4.

b) Section 3.1.2

Proposed Attachment 1 Section 3.1.2 would expand the scope of Reliability Standard CIP-003 to include all communications, rather than only vendor specific communications.[46] Proposed Section 3.1.2 would require that entities implement controls to detect known or suspected inbound and outbound malicious communications between low impact BES Cyber Systems and a Cyber Asset(s) outside the asset containing low impact BES Cyber Systems.[47] These revisions would enable entities to mitigate the risk posed by malicious communications to or from low impact BES Cyber Systems, while allowing entities flexibility as to where the control is implemented based on their architecture.[48]

c) Section 3.1.3

Proposed Attachment 1 Section 3.1.3 would mitigate the risk of unauthenticated access to networks on which low impact BES Cyber Systems reside. Specifically, the proposed revisions would require entities to implement controls to authenticate users prior to permitting (allowing, establishing, gaining) access to networks containing low impact BES Cyber Systems, or Shared Cyber Infrastructure ("SCI") that supports a low impact BES Cyber System. Thus, each user would be authenticated before they gain access to the network containing low impact BES Cyber Systems.[49] As a result, users would have no ability to enumerate hosts on those networks, scan those networks for vulnerabilities, attempt logons to systems or perform actions on those networks and systems before the entity has authenticated their identity.[50]

---

46 *Id.* at 4.

47 *Id.* at 5.

48 *Id.* at 4-5.

49 The intention of the phrase "each user prior to permitting access to a network(s)…" is meant to include the initial authentication and not all subsequent access to other downstream networks. If there is a collection of sub-networks or Cyber Assets within the network containing low impact BES Cyber Systems, then multiple re-authentications at those levels would not be required by this specific requirement. Technical Rationale at 7.

50 *Id.* at 6.

Proposed Attachment 1 Section 3.1.3 would not require the use of an "Intermediate System" as is prescribed in CIP-005 Requirement R2 for high and medium impact BES Cyber Systems. However, entities who have established or implemented such infrastructure or technologies would be able to use them for authenticating access to the assets containing low impact BES Cyber Systems to satisfy these requirements. The proposed revisions do not prescribe an architecture similar to that used in CIP-005 Requirement R2 because of the impact that such requirements would have on a broad and diverse range of entities and their specific technologies and processes used to meet low impact BES Cyber Systems authentication requirements.[51] For example, it would be excessive to require an entity with a single CIP-003 applicable renewable generation site to implement architectures and technologies (Intermediate Systems) to meet the CIP-005 Requirement R2 Interactive Remote Access requirements. Such an entity may only need a Secure Sockets Layer (SSL) Virtual Private Network (VPN) to an access control device (e.g., firewall) at the one site that authenticates the user prior to allowing access to the network containing low impact BES Cyber Systems on its inside interface. The entity may also choose to authenticate a local non-low impact BES Cyber Systems network first, then control access to the low impact BES Cyber Systems from that access point. Conversely, an entity with many assets distributed over a large geographic area, with a variety of impact categorizations and supporting BES Cyber Systems, may want to use their existing CIP-005 Requirement R2 remote access solutions for all of their sites (centralized access controls). The proposed revisions would allow flexibility for both cases.[52]

---

51 *Id.* at 8.

52 *Id.* at 8.

d) Section 3.1.4

Proposed Attachment 1 Section 3.1.4 would require Responsible Entities to protect the user authentication information (e.g., username, password, multi-factor authentication information, session token, etc.) while in transit between the remote user's Cyber Asset and either the asset containing the low impact BES Cyber Systems or the entity's authentication system used to meet Section 3.1.3.[53] This protection would mitigate the risk of user authentication information being captured, especially as some BES equipment may still require protocols that transmit such information in clear text.[54] The intent is not to specify authentication directly to a particular device but to allow entities that desire to use an existing compliant CIP-005 Requirement R2 Intermediate System, or similar architecture, access to networks containing low impact BES Cyber Systems.[55] While the proposed revisions would not require the use of an "Intermediate System", as is prescribed in CIP-005 Requirement R2 for high and medium impact BES Cyber Systems, entities with such infrastructures in place can, if they choose, use them for access to the assets containing low impact BES Cyber Systems to satisfy the intent of these requirements.[56]

e) Section 3.1.5

Proposed Section 3.1.5 would preserve the language used in proposed Reliability Standard CIP-003-10, Section 6.1 and merge it into revised Section 3. This would require Responsible Entities to implement one or more method(s) for determining vendor electronic access, where permitted, to their low impact BES Cyber Systems, thus increasing an entity's ability to detect,

---

53 *Id.* at 8.

54 *Id.* at 8.

55 *Id.* at 8.

56 *Id.* at 10.

respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access.[57]

f) Section 3.1.6

Proposed Section 3.1.6 would preserve the language used in proposed Reliability Standard CIP-003-10, Section 6.2. This would require Responsible Entities to implement one or more method(s) for disabling vendor electronic remote access, where permitted, for any basis the entity may choose. This would prevent security events and propagation of potential malicious communications that may degrade or have adverse effects upon the entity's assets containing low impact BES Cyber Systems.[58]

2. Attachment 1, Section 3.2

Proposed Section 3.2 would maintain the original intent of proposed Reliability Standard CIP-003-10, Section 3.2.[59]

C. Attachment 2

Proposed Reliability Standard CIP-003-11 Attachment 2 includes the merging of Section 6 into Section 3 to conform with the changes proposed in Attachment 1. The proposed revisions include providing examples of compliance related activities.[60]

D. Enforceability

The proposed Reliability Standard includes measures that support each requirement by clearly identifying what is required and how NERC and the Regional Entities will enforce the requirement. These measures help ensure that the requirements will be enforced in a clear,

---

57 *Id.* at 11.

58 *Id.* at 11.

59 *Id.* at 11.

60 *Id.* at 11.

consistent, and non-preferential manner and without prejudice to any party.[61] Additionally, the proposed Reliability Standard includes VRFs and VSLs. The VRFs and VSLs provide guidance on the way that NERC and the Regional Entities will enforce the requirements of the proposed Reliability Standard. The VRFs and VSLs for the proposed Reliability Standard comport with NERC and Commission guidelines related to their assignment. **Exhibit E** provides a detailed review of the VRFs and VSLs, and the analysis of how the VRFs and VSLs were determined using these guidelines.

E. EFFECTIVE DATE OF THE PROPOSED RELIABILITY STANDARDS

NERC respectfully requests that the Commission approve the proposed Reliability Standard to become effective as set forth in the Implementation Plan provided in **Exhibit B** hereto. The proposed Implementation Plan includes as prerequisites the definitions for "Cyber System", "Shared Cyber Infrastructure", and "Virtual Cyber Asset" pending Commission action in Docket No. RM24-8-000.[62] The proposed Implementation Plan provides that the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the effective date of the Commission's order approving the standard.

With respect to initial compliance with periodic requirements, the Implementation Plan notes that periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to ". . . at least once every 15 calendar months . . .". The Implementation Plan provides that Responsible Entities shall initially comply with Requirement R1, Part 1.2.3 on or before the effective date of CIP-003-11. The Implementation Plan further provides that Responsible Entities shall initially comply with all other periodic

---

61 Order No. 672, *supra*, at P 327.

62 *See* Virtualization Petition, *supra*.

requirements in CIP-003-11 within the periodic timeframes of their last performance under the version of the CIP-003 Reliability Standard then in effect.

The Implementation Plan provides that, entities shall not be required to comply with Requirement R2 as it relates to the implementation of documented cyber security plan(s) addressing Attachment 1 Section 3.1.2 until the later of: (1) April 1, 2029; or (2) the effective date of Reliability Standard CIP-003-11.

The proposed Implementation Plan provides entities with thirty-six (36) months to become compliant with proposed Reliability Standard CIP-003-11. The proposed Implementation Plan reflects the following considerations for entities to implement the new controls of Requirement R2, Attachment 1: (1) the time needed to revise the cyber security policy, plan, and procedures; (2) the time needed to hire and train new staff to implement the new cyber security controls; (3) the time needed to reconfigure system, network, or security architectures; and (4) the time needed to purchase, procure, and install new technologies. The proposed Implementation Plan also reflects consideration of the fact that the effective date of Reliability Standard CIP-003-9 is April 1, 2026; and the requested effective date of proposed Reliability Standard CIP-003-10 is the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the Commission's order approving the standard. In light of these considerations, the proposed Implementation Plan for Reliability Standard CIP-003-11 balances the urgency in the need to implement the standard against the time needed to comply.[63] NERC respectfully requests approval of the proposed Implementation Plan as submitted.

[63] *See* Order No. 672, *supra*, at P 333 ("In considering whether a proposed Reliability Standard is just and reasonable, the Commission will consider also the timetable for implementation of the new requirements, including how the proposal balances any urgency in the need to implement it against the reasonableness of the time allowed for those who must comply to develop the necessary procedures, software, facilities, staffing or other relevant capability.").

F. CONCLUSION

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

- proposed Reliability Standard CIP-003-11, and the associated elements, as shown in **Exhibit A**;
- the Implementation Plan included in **Exhibit B**; and
- the retirement of proposed Reliability Standard CIP-003-10, or the version of Reliability Standard CIP-003 then in effect.

Respectfully submitted,

/s/ Sarah P. Crawford

Lauren A. Perotti
Assistant General Counsel
Sarah P. Crawford
Counsel
North American Electric Reliability Corporation
1401 H Street, N.W., Suite 410
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
lauren.perotti@nerc.net
sarah.crawford@nerc.net

Counsel for the North American Electric Reliability Corporation

December 20, 2024

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A

The Proposed Reliability Standard

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A-1

CIP-003-11 Clean

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final version of the proposed standard. The drafting team is posting the final documents but not conducting a final ballot per the Standard Processes Manual (SPM) section 4.13, which allows the drafting team to conclude the standards action without conducting a final ballot if: (1) the previous ballot achieved at least 85% weighted segment approval; (2) the drafting team made a good faith effort at resolving applicable objections; (3) the drafting team responded in writing to comments as required by section 4.12; and (4) the drafting team is proposing no further changes to the balloted documents. Consistent with these requirements, the last ballot received 93.89% approval. The drafting team has made a good faith effort to resolve objections and responded to comments in writing, including making minor corrections to two of the non-mandatory and enforceable sections of the standard. Per SPM section 2.5: "The only mandatory and enforceable components of a Reliability Standard are the: (1) applicability, (2) Requirements, and the (3) effective dates. The additional components are included in the Reliability Standard for informational purposes and to provide guidance to Functional Entities concerning how compliance will be assessed by the Compliance Enforcement Authority." CIP-003-11 is built on Board Approved CIP-003-10 which was created by Project 2016-02's changes for virtualization.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023
45-day formal comment period with initial ballot	October 24 – December 7, 2023
45-day formal comment period with additional ballot	January 30 – March 14, 2024
30-day formal comment period with additional ballot	June 12 – July 11, 2024
30-day formal comment period with additional ballot	September 11 – October 10, 2024

Anticipated Actions	Date
Board adoption	December 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

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

2. **Number:** CIP-003-11

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-003-11:

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

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

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

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

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

5. Effective Dates: See Implementation Plan for CIP-003-11.

B. Requirements and Measures

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

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

1.1.1. Personnel and training (CIP-004);

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

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

1.1.4. System security management (CIP-007);

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

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

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

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

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

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

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

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

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

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

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

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

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

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

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

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

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

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

   The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

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

   1.3. Compliance Monitoring and Enforcement Program: "Compliance Monitoring and Enforcement Program" or "CMEP" means, depending on the context (1) the NERC Compliance Monitoring and Enforcement Program (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities' compliance with Reliability Standards.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR	impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	the previous approval. (Part 1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the	according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment	Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2023-04
- CIP-003-11 Technical Rationale

Version History

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

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
10	5/9/2024	Adopted by the NERC Board of Trustees.	Modifications made by Project 2016-02.

Version	Date	Action	Change Tracking
10	TBD	FERC approval pending in Docket No. RM24-8-000	
11	TBD	Modified by Project 2023-04	

Attachment 1

Required Sections for Cyber Security Plan(s)

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

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

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

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need, as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or Virtual Cyber Asset (VCA), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, where electronic access is:

i. Between:
- a low impact BCS; or
- an SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:
- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

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

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

the Responsible Entity shall implement one or more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for

both inbound and outbound electronic access;

3.1.3 Authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted;

3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System(s) outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BCS or SCI that supports a low impact BCS;

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, the Responsible Entity shall implement one or more control(s) that authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

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

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

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

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

4.4 Incident handling for Cyber Security Incidents;

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

Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

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

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

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

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

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

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

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

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

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

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

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

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

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

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

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

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

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

1. For Section 3.1.1, documentation showing the permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, such as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BCS or SCI that supports a low impact BCS and a Cyber System outside the asset containing low impact BCS.
   - Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways); or
   - Original equipment manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
    - Anti-malware technologies;
    - Intrusion detection system (IDS)/intrusion prevention system (IPS);
    - Monitor or alert for changes to communication baselines;
    - Logging and alerting configuration for security incident and event management (SIEM) systems or other event correlation systems;
    - Automated or manual log reviews;
    - Alerting; or
    - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted, such as:
    - Authentication mechanism(s) including, but not limited to:
        - Utilization of public key infrastructure (PKI), lightweight directory access protocol (LDAP), remote authentication dial-in user service (RADIUS), and/or similar implemented solutions; or
        - Enforcement of multi-factor authentication (MFA).
    - Virtual private network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
    - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BCS; or
    - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System outside the asset containing low impact BCS or SCI that supports a low impact BCS and
    - The authentication system used to meet Section 3.1.3, or
    - The asset containing low impact BCS or SCI that supports a low impact BCS,

    such as protection mechanism(s) including, but not limited to:
    - Implementation of an encrypted protocol or service (hypertext transfer protocol secure (HTTPS), secure shell (SSH), etc.);
    - Implementation of an IPsec or secure sockets layer (SSL) VPN; or

- Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;
   - Security information management logging alerts;
   - Time-of-need session initiation;
   - Session recording;
   - System logs; or
   - Other operational, procedural, or technical controls.
6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Disabling vendor electronic access user or system accounts;
   - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, remote desktop, remote control, or other hardware or software used for providing vendor electronic access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or
   - Other operational, procedural, or technical controls.
7. For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

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

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

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

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

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A-2

CIP-003-11 Redline to Last FERC-Approved

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final version of the proposed standard. The drafting team is posting the final documents but not conducting a final ballot per the Standard Processes Manual (SPM) section 4.13, which allows the drafting team to conclude the standards action without conducting a final ballot if: (1) the previous ballot achieved at least 85% weighted segment approval; (2) the drafting team made a good faith effort at resolving applicable objections; (3) the drafting team responded in writing to comments as required by section 4.12; and (4) the drafting team is proposing no further changes to the balloted documents. Consistent with these requirements, the last ballot received 93.89% approval. The drafting team has made a good faith effort to resolve objections and responded to comments in writing, including making minor corrections to two of the non-mandatory and enforceable sections of the standard. Per SPM section 2.5: "The only mandatory and enforceable components of a Reliability Standard are the: (1) applicability, (2) Requirements, and the (3) effective dates. The additional components are included in the Reliability Standard for informational purposes and to provide guidance to Functional Entities concerning how compliance will be assessed by the Compliance Enforcement Authority."

CIP-003-11 is built on Board Approved CIP-003-10 which was created by Project 2016-02's changes for virtualization. This version is a redline to last FERC approved CIP-003-9. The following key describes the changes:

Redline Text	Project 2016-02 changes (Version 10)
Redline Text	Project 2023-04 changes

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023
45-day formal comment period with initial ballot	October 24 – December 7, 2023
45-day formal comment period with additional ballot	January 30 – March 14, 2024
30-day formal comment period with additional ballot	June 12 – July 11, 2024
30-day formal comment period with additional ballot	September 11 – October 10, 2024

Anticipated Actions	Date
Board adoption	December 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

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

2. **Number:** CIP-~~003-9~~-003-11

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP ~~-003-9~~-003-11:

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

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

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

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

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

5. Effective Dates: See Implementation Plan for CIP-~~003-9~~003-11.

B. Requirements and Measures

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

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

1.1.1. Personnel and training (CIP-004);

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

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

1.1.4. System security management (CIP-007);

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

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

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

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

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

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

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

~~**1.2.6.** Vendor electronic remote access security controls; and~~

~~**1.2.7.**~~**1.2.6.** Declaring and responding to CIP Exceptional Circumstances.

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

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

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

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

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

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

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

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

C. Compliance

1. **Compliance Monitoring Process**

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

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

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

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

1.3. Compliance Monitoring and Enforcement Program: ~~As defined in the NERC Rules of Procedure,~~ "Compliance Monitoring and Enforcement Program" ~~refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated~~or "CMEP" means, depending on the context (1) the NERC Compliance Monitoring and Enforcement Program (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities' compliance with Reliability ~~Standard~~Standards.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address one of the nine topics required by Requirement R1. (~~R1~~Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (~~R1~~Part 1.1) OR	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address two of the nine topics required by Requirement R1. (~~R1~~Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (~~R1~~Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address three of the nine topics required by Requirement R1. (~~R1~~Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (~~R1~~Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address four or more of the nine topics required by Requirement R1. (~~R1~~Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ BCS as required by Requirement R1. (~~R1~~Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1)

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (~~R1~~Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, but did not address one of the seven topics required by Requirement R1. (Part ~~R~~1.2) OR The Responsible Entity did not complete its review of the one or more	high impact and medium impact ~~BES Cyber Systems~~ BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (~~R1~~Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS, but did not address two of the seven topics required by Requirement R1. (~~R1~~Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS as required by Requirement R1 within 16	high impact and medium impact ~~BES Cyber Systems~~ BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber System~~BCS, but did not address three of the seven topics required by Requirement R1. (Part ~~R~~1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS as required by Requirement R1 within 17	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (~~R1~~Part 1.1) OR The Responsible Entity ~~documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but~~ did not address four or more of the seven topics required by Requirement R1. (Part ~~R~~1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES~~

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (~~R1~~Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (~~R1~~Part 1.2)	calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (~~R1~~Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (~~R1~~Part 1.2)	calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part ~~R~~1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (~~R1~~Part 1.2)	~~Cyber Systems~~ BCS as required by Requirement R1. (~~R1~~Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (~~R~~ Part 1.2)

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity ~~implemented electronic access controls but~~ failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document one or more Cyber Security Incident	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document electronic access	The Responsible Entity ~~documented the physical access controls for its assets containing low impact BES Cyber Systems, but~~ failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but~~ failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity ~~documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its~~	The Responsible Entity failed to document and implement one or more cyber security plan(s) ~~for its assets containing low impact BES Cyber Systems~~ according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to manage its Transient Cyber Asset(s) according to Requirement	controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for electronic access controls but~~ failed to implement authentication for all Dial-up Connectivity ~~that provides access to low impact BES Cyber System(s), per Cyber Asset capability~~ according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity ~~documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to include the process for identification, classification, and response to Cyber Security Incidents according to	~~assets containing low impact BES Cyber Systems, but~~ failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but~~ failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its plan for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the introduction of malicious code for Transient Cyber	

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets, but~~ failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) ~~OR~~ ~~The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)~~	Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according	Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media	

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) ~~OR~~	according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) ~~OR~~ ~~The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)~~	

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		~~The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (Requirement R2)~~		
R3	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has~~ did not identif~~ied~~, by name, a CIP Senior Manager. OR The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 30 calendar days but did	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 40 calendar days but did document this	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 50 calendar days but did document this	The Responsible Entity ~~has used delegated authority for actions where allowed by the CIP standards, but~~ does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	document this change in less than 40 calendar days of the change. (Requirement R4)	change in less than 50 calendar days of the change. (Requirement R4)	change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~

- Implementation Plan for Project 2023-04
- CIP-003-11 Technical Rationale

Version History

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

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

Version	Date	Action	Change Tracking
10	5/9/2024	Adopted by the NERC Board of Trustees.	Modifications made by Project 2016-02.
10	TBD	FERC approval pending in Docket No. RM24-8-000	
11	TBD	Modified by Project 2023-04	

Attachment 1

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

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

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

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

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need, as determined by the Responsible Entity, to (1) the asset or the locations of the low impact ~~BES Cyber Systems~~BCS within the asset, and (2) the Cyber Asset(s) or Virtual Cyber Asset (VCA), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section ~~3.1~~3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact ~~BES Cyber System(s)~~BCS identified pursuant to CIP ~~002, the Responsible Entity shall implement~~ 002 and for SCI that supports a low impact BCS, if any, where electronic access ~~controls to~~is:

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

i. ~~b~~Between:

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

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

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

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

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

the Responsible Entity shall implement one or more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for ~~i~~both inbound and outbound electronic access;

3.1.3 Authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted;

3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System(s) outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BCS or SCI that supports a low impact BCS;

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, the Responsible Entity shall implement one or more control(s) that ~~A~~authenticate all Dial-up Connectivity, if any, that provides access to low impact ~~BES Cyber System(s)~~ BCS or SCI that supports a low impact BCS, per ~~Cyber Asset~~ system capability.

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

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

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

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

4.4 Incident handling for Cyber Security Incidents;

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

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

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

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

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

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

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

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- ~~Review use of live operating system and software executable only from read-only media;~~

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

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

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

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

~~**5.3.1**~~

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

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

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

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

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

Attachment 2

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

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

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

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

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact ~~BES Cyber Systems~~BCS within the asset; and
  b. The Cyber ~~Asset~~System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section ~~3.1~~3.1.1, if any.

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

1. For Section 3.1.1, documentation showing the permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, such as:
   - ~~Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative~~Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact ~~BES Cyber System(s)~~BCS or SCI that supports a low impact BCS and a Cyber ~~Asset(s)~~System outside the asset containing low impact ~~BES Cyber System(s) or lists~~ BCS.

- Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways)~~.~~; or
- Original equipment manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Anti-malware technologies;
   - Intrusion detection system (IDS)/intrusion prevention system (IPS);
   - Monitor or alert for changes to communication baselines;
   - Logging and alerting configuration for security incident and event management (SIEM) systems or other event correlation systems;
   - Automated or manual log reviews;
   - Alerting; or
   - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted, such as:
   - Authentication mechanism(s) including, but not limited to:
     - Utilization of public key infrastructure (PKI), lightweight directory access protocol (LDAP), remote authentication dial-in user service (RADIUS), and/or similar implemented solutions; or
     - Enforcement of multi-factor authentication (MFA).
   - Virtual private network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
   - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BCS; or
   - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System outside the asset containing low impact BCS or SCI that supports a low impact BCS and
   - The authentication system used to meet Section 3.1.3, or
   - The asset containing low impact BCS or SCI that supports a low impact BCS,

such as protection mechanism(s) including, but not limited to:

- Implementation of an encrypted protocol or service (hypertext transfer protocol secure (HTTPS), secure shell (SSH), etc.);
- Implementation of an IPsec or secure sockets layer (SSL) VPN; or
- Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;
   - Security information management logging alerts;
   - Time-of-need session initiation;
   - Session recording;
   - System logs; or
   - Other operational, procedural, or technical controls.
6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Disabling vendor electronic access user or system accounts;
   - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, remote desktop, remote control, or other hardware or software used for providing vendor electronic access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or
   - Other operational, procedural, or technical controls.

~~2.~~7. For Section 3.2, ~~D~~documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the ~~BES Cyber System~~BCS).

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

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

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

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

Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

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

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

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

~~1. For Section 6.1, documentation showing:~~

- ~~steps to preauthorize access;~~
- ~~alerts generated by vendor log on;~~
- ~~session monitoring;~~
- ~~security information management logging alerts;~~
- ~~time-of-need session initiation;~~
- ~~session recording;~~
- ~~system logs; or~~
- ~~other operational, procedural, or technical controls.~~

~~2. For Section 6.2, documentation showing:~~

- ~~disabling vendor electronic remote access user or system accounts;~~

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A-3

Redline to last NERC Board of Trustees-Approved

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final version of the proposed standard. The drafting team is posting the final documents but not conducting a final ballot per the Standard Processes Manual (SPM) section 4.13, which allows the drafting team to conclude the standards action without conducting a final ballot if: (1) the previous ballot achieved at least 85% weighted segment approval; (2) the drafting team made a good faith effort at resolving applicable objections; (3) the drafting team responded in writing to comments as required by section 4.12; and (4) the drafting team is proposing no further changes to the balloted documents. Consistent with these requirements, the last ballot received 93.89% approval. The drafting team has made a good faith effort to resolve objections and responded to comments in writing, including making minor corrections to two of the non-mandatory and enforceable sections of the standard. Per SPM section 2.5: "The only mandatory and enforceable components of a Reliability Standard are the: (1) applicability, (2) Requirements, and the (3) effective dates. The additional components are included in the Reliability Standard for informational purposes and to provide guidance to Functional Entities concerning how compliance will be assessed by the Compliance Enforcement Authority." CIP-003-11 is built on Board Approved CIP-003-10 which was created by Project 2016-02's changes for virtualization.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023
45-day formal comment period with initial ballot	October 24 – December 7, 2023
45-day formal comment period with additional ballot	January 30 – March 14, 2024
30-day formal comment period with additional ballot	June 12 – July 11, 2024
30-day formal comment period with additional ballot	September 11 – October 10, 2024

Anticipated Actions	Date

Board adoption	December 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

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

2. **Number:** CIP-003-~~10~~11

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-003-~~10~~11:

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

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

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

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

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

5. Effective Dates: See ~~"Project 2016-02 Modifications to CIP Standards~~ Implementation Plan~~."~~ for CIP-003-11.

B. Requirements and Measures

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

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

1.1.1. Personnel and training (CIP-004);

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

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

1.1.4. System security management (CIP-007);

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

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

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

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

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

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

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

~~**1.2.6.** Vendor electronic remote access security controls; and~~

~~**1.2.7.**~~**1.2.6.** Declaring and responding to CIP Exceptional Circumstances.

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

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

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

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

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

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

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

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

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

C. Compliance

1. **Compliance Monitoring Process**

1.1. Compliance Enforcement Authority: ~~As defined in the NERC Rules of Procedure,~~ "Compliance Enforcement Authority" ~~(CEA)~~ means NERC or the Regional Entity ~~, or any entity as otherwise designated by an Applicable Governmental Authority,~~ in their respective roles of monitoring and~~/or~~ enforcing compliance with the NERC ~~mandatory and enforceable~~ Reliability Standards ~~in their respective jurisdictions~~.

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

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

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

1.3. Compliance Monitoring and Enforcement Program: ~~As defined in the NERC Rules of Procedure,~~ "Compliance Monitoring and Enforcement Program" or "CMEP" means, depending on the context (1) the NERC Compliance Monitoring and Enforcement Program (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities' compliance with Reliability Standards. ~~refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-~~10~~11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-~~10~~11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR	impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1. (~~R1~~Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of

R #	Violation Severity Levels (CIP-003-~~1~~011)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	the previous approval. (~~R1~~Part 1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-~~1~~011)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the	according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity ~~documented~~ failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Violation Severity Levels (CIP-003-~~10~~11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) ~~OR~~ ~~The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)~~	determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment	Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) ~~OR~~ ~~The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote~~	

R #	Violation Severity Levels (CIP-003-~~1~~011)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) ~~OR~~ ~~The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (Requirement R2)~~	~~access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)~~	
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60

R #	Violation Severity Levels (CIP-003-~~10~~11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of the change. (Requirement R3)			calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project ~~2016-02~~2023-04
- CIP-003-~~10~~11 Technical Rationale

Version History

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

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

Version	Date	Action	Change Tracking
9	3/22/2023	Effective Date	April 1, 2026
10	~~TBD~~5/9/2024	~~Virtualization Modifications~~Adopted by the NERC Board of Trustees.	Modifications made by Project 2016-02.
10	TBD	FERC approval pending in Docket No. RM24-8-000	
11	TBD	Modified by Project 2023-04	

Attachment 1

Required Sections for Cyber Security Plan(s)

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

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

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

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need, as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or Virtual Cyber Asset (VCA~~,~~), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact ~~BES Cyber System(s)~~BCS identified pursuant to CIP-002~~, the Responsible Entity shall implement~~ and for SCI that supports a low impact BCS, if any, where electronic access ~~controls to~~is:

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

i. Between:
- ~~-~~a low impact BCS; or
- ~~An~~an SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:
- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

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

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

~~Authenticate~~the Responsible Entity shall implement one or more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic access;

3.1.3 Authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted;

3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System(s) outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BCS or SCI that supports a low impact BCS;

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, the Responsible Entity shall implement one or more control(s) that authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

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

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

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

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

4.4 Incident handling for Cyber Security Incidents;

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

Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

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

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

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

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

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

1. ~~Documentation~~ For Section 3.1.1, documentation showing ~~that at each asset or group of assets,~~ the ~~routable protocol communication as outlined in Section 3 is restricted by electronic access controls to permit~~permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, ~~except where an entity provides rationale that communications are used for time-sensitive communications of Protection Systems. Examples of~~ such ~~documentation may include, but are not limited to representative~~as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) ~~or lists~~between the low impact BCS or SCI that supports a low impact BCS and a Cyber System outside the asset containing low impact BCS.

- Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways~~)~~.); or
- ~~Documentation~~Original equipment manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Anti-malware technologies;
   - Intrusion detection system (IDS)/intrusion prevention system (IPS);
   - Monitor or alert for changes to communication baselines;
   - Logging and alerting configuration for security incident and event management (SIEM) systems or other event correlation systems;
   - Automated or manual log reviews;
   - Alerting; or
   - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted, such as:
   - Authentication mechanism(s) including, but not limited to:
     - Utilization of public key infrastructure (PKI), lightweight directory access protocol (LDAP), remote authentication dial-in user service (RADIUS), and/or similar implemented solutions; or
     - Enforcement of multi-factor authentication (MFA).
   - Virtual private network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
   - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BCS; or
   - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System outside the asset containing low impact BCS or SCI that supports a low impact BCS and
   - The authentication system used to meet Section 3.1.3, or

- The asset containing low impact BCS or SCI that supports a low impact BCS, such as protection mechanism(s) including, but not limited to:
  - Implementation of an encrypted protocol or service (hypertext transfer protocol secure (HTTPS), secure shell (SSH), etc.);
  - Implementation of an IPsec or secure sockets layer (SSL) VPN; or
  - Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;
   - Security information management logging alerts;
   - Time-of-need session initiation;
   - Session recording;
   - System logs; or
   - Other operational, procedural, or technical controls.
6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Disabling vendor electronic access user or system accounts;
   - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, remote desktop, remote control, or other hardware or software used for providing vendor electronic access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or
   - Other operational, procedural, or technical controls.

~~1.~~7. For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back

modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

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

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

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

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

mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

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

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

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

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

2. For Section 6.2, documentation showing:
   - disabling vendor electronic remote access user or system accounts;
   - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control,

~~or other hardware or software used for providing vendor electronic remote access;~~

- ~~disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;~~
- ~~Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);~~
- ~~administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or~~
- ~~other operational, procedural, or technical controls.~~

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit B

Implementation Plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-04 Modifications to CIP-003
Reliability Standard CIP-003-11

Applicable Standard(s)

- CIP-003-11 – Cyber Security – Security Management Controls

Requested Retirement(s)

- CIP-003-10 – Cyber Security – Security Management Controls[1]

Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- Cyber System
- Shared Cyber Infrastructure
- Virtual Cyber Asset

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

New/Modified/Retired Terms in the NERC Glossary of Terms

- None

[1] If CIP-003-10 is not currently in effect, then the currently effective version of Reliability Standard CIP-003 shall be retired immediately prior to the effective date of CIP-003-11 in the jurisdiction in which the revised standard is becoming effective.

Background

Project 2023-04 addresses modifications to CIP-003-10 in response to recommendations from the Low Impact Criteria Review Team (LICRT), which was formed by the NERC Board of Trustees to consider the potential threat and risk posed by a coordinated cyber-attack on low impact Bulk Electric System (BES) Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommended actions to address those risks. The NERC Board of Trustees accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the standard authorization request (SAR) at its March 22, 2023 meeting. In response to the SAR, Project 2023-04 proposes merging Sections 3 and 6 of CIP-003, Attachments 1 and 2 to consolidate all electronic access requirements. These revisions are captured in Reliability Standard CIP-003-11.

This implementation plan provides additional time for entities to come into compliance with Requirement R2 for the expanded scope of communications that must be monitored to detect known or suspicious malicious communications, from vendor electric remote access in CIP-003-9, to all inbound and outbound electronic access in CIP-003-11 (Attachment 1 Section 3.1.2). In determining additional time was appropriate, the Project 2023-04 drafting team considered that CIP-003-9 will become effective April 1, 2026, and two versions of the CIP-003 standard will be pending regulatory approval (CIP-003-10, CIP-003-11). The drafting team also considered that entities may have already invested significant resources to implement system architecture to monitor vendor remote access in compliance with Reliability Standard CIP-003-9, and that implementing further changes across a large fleet of low impact BES Cyber Systems may require significant additional time and investments. This implementation plan ensures that entities will have at least three years from the effective date of Reliability Standard CIP-003-9 to implement the additional controls contemplated by CIP-003-11, regardless of the date proposed Reliability Standard CIP-003-11 is approved.

The CIP-003-11 changes were made to the NERC Board of Trustees approved version of CIP-003, CIP-003-10 (Virtualization Revisions), which has been filed with the applicable governmental authorities. The use of certain defined terms within CIP-003-11 requires that the definitions for Cyber Systems, Shared Cyber Infrastructure, and Virtual Cyber Asset be approved either concurrently with or before CIP-003-11.

General Considerations

This implementation plan applies only to the CIP-003-11 revisions to the Reliability Standard that have been made by the Project 2023-04 drafting team. The implementation plan does not modify the implementation plan(s) for any other version of CIP-003.

This implementation plan provides entities with thirty-six (36) months to become compliant with the revised Reliability Standard CIP-003-11. This implementation plan reflects the following considerations for entities to implement the new controls of Requirement R2, Attachment 1:

- Revise cyber security policy, plan, and procedures.
- Hire and train new staff to implement the new cyber security controls.
- Reconfigure system, network, or security architectures.
- Purchase, procure, and install new technologies.
- The effective date of CIP-003-9 is April 1, 2026.
- The requested effective date of CIP-003-10 is the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority.

Effective Date

Reliability Standard CIP-003-11

Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and Responsible Entities shall comply initially with those periodic requirements in CIP-003-11 as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.3 on or before the effective date of CIP-003-11. Responsible Entities shall initially comply with all other periodic requirements in CIP-003-11 within the periodic timeframes of their last performance under the version of the CIP-003 Reliability Standard then in effect.

Compliance Date for Requirement R2, Attachment 1 Section 3.1.2

Entities shall not be required to comply with Requirement R2 as it relates to the implementation of documented cyber security plan(s) addressing Attachment 1 Section 3.1.2[2] until the later of: (1) April 1, 2029; or (2) the effective date of Reliability Standard CIP-003-11.

[2] Attachment 1 Section 3.1.2: "Detect known or suspected malicious communications for both inbound and outbound electronic access."

Retirement Date

Reliability Standard CIP-003

Reliability Standard CIP-003-10, or the version of Reliability Standard CIP-003 then in effect, shall be retired immediately prior to the effective date of CIP-003-11 in the jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit C

Technical Rationale

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard
CIP-003-11 – Low Impact BES Cyber Security Criteria Revisions

Introduction
This document is the technical rationale and justification for Reliability Standard CIP-003-11 and includes the rationale for changes in the current proposed version, as well as previous versions of the standard.

It is intended to provide stakeholders and the ERO Enterprise with an understanding of the revisions, technology, and technical concepts of Reliability Standard CIP-003-11. This is not a Reliability Standard and should not be considered mandatory and enforceable.

Background
In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact Bulk Electric System (BES) Cyber Assets. Specifically, this includes the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts, representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber-attack on low impact BES Cyber Systems (LIBCS). In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommended actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the Standard Authorization Request (SAR) at its March 22, 2023 meeting.

The LICRT conclusions regarding LIBCS are as follows:

- Individually, LIBCS are truly low impact to BES reliability. This corresponds to the longstanding work of NERC and the stakeholders to design and operate the BES to withstand the loss of any of its individual assets. A medium or high impact BES Cyber System is more than an impact to a typical single BES Element/Facility. Therefore, the LICRT does not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems.
- LIBCS may introduce BES reliability risks of a higher impact where distributed LIBCS are used for a coordinated attack. The LICRT recommends enhancing the existing low impact category to further mitigate the coordinated attack risk.

The LICRT report recommendations are as follows:

- Requirement(s) for authentication of remote users before granting and subsequently gaining electronic access to networks containing LIBCS at assets containing those systems that have external routable connectivity.

- Requirement(s) for protection of user authentication information in transit for remote electronic access to LIBCS at assets containing those systems that have external routable connectivity.
- Requirement(s) for detection of malicious communications to/between assets containing LIBCS with external routable connectivity.

Rationale for Attachment 1, Section 3 and Section 6

The drafting team's (DT) review of the SAR and industry comment initiated a discussion about the placement of requirements within CIP-003-11. Attachment 1, Section 3 and Attachment 1, Section 6 were identified as ideal locations to integrate the requirements due to their focus on electronic access controls and vendor electronic remote access security controls. The DT investigated two options:

Option A: Modify Sections 3 and 6, integrating the requirements, but keeping the sections separate.
Option B: Merge Sections 3 and 6.

The DT agreed to Option B: Merge Sections 3 and 6. Merging Section 3 and Section 6 would present a single section for all electronic access with sub-sections providing additional requirements based on the type of access (vendor, dial-up, local, etc.). This allows entities to look in one place for all of the electronic access control requirements needed for their assets containing low impact systems, rather than having very similar, and in some cases, overlapping requirements in multiple places within the standard.

While merging Section 3 and 6, the DT made conforming changes to the language. The DT uses the phrase "implement controls" to replace "implement a process" or "implement one or more method(s)". The DT believes a "control" can include an operation, process, procedure, or technology as described in the examples of Attachment 2. Additionally, the word "remote" was removed from the phrase "electronic remote access" as the section now covers all electronic access as described in Section 3, Part 3.1, (i), (ii), and (iii) as those define more specifically the remote nature of the in-scope access.

To clarify scope of requirements for industry and regulators alike, the DT placed the requirements in Attachment 1 Section 3.1 into a logical "if, then" order to further clarify the three identifying low impact asset characteristics or conditions (romanettes i, ii, iii) when implementing controls.

Section 3.1

The objective of the modifications within Section 3.1 is to maintain the original language used in CIP-003-10, Section 3.1, Subsections (i) - (iii). There is one revision to 3.1(iii) replacing the previous language concerning "intelligent electronic devices" with reference to the existing glossary term "Protection Systems" which is a conforming change to the change made by Project 2016-02, CIP-003-10. Figure 1 provides a graphical representation of Section 3.1, Subsections (i)-(iii).

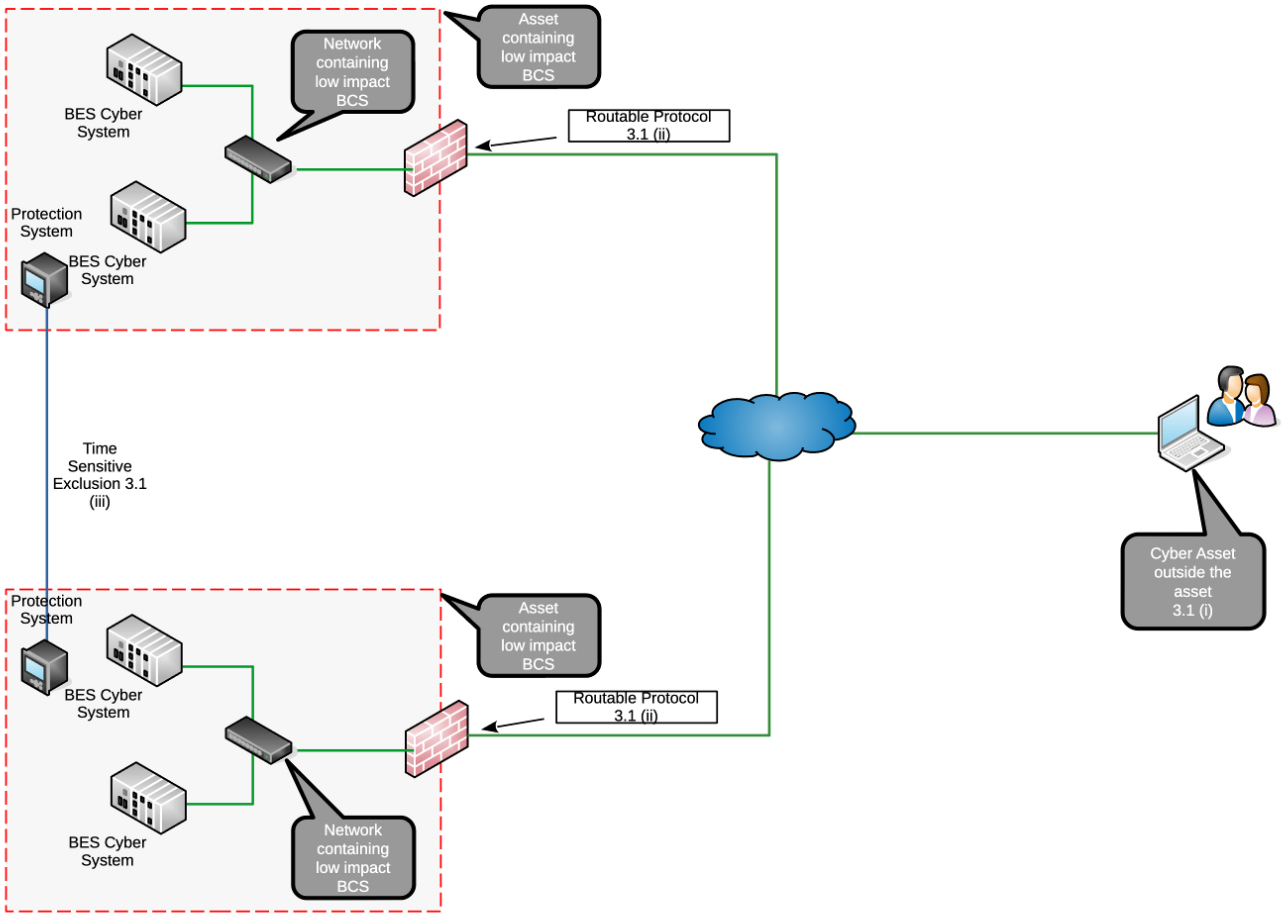


Figure 1

Section 3.1.1

The objective of Section 3.1.1 is to maintain the original language used in CIP-003-10, Section 3.1.

Section 3.1.2

This is an expanded cyber security control outlined in the SAR. The scope is expanded from CIP-003-10, Section 6.3 to include all communications rather than vendor specific communications. The objective of the modifications within Attachment 1 Section 3.1.2 is for entities to mitigate the risk posed by malicious communications to or from LIBCS. The detection of known or suspected malicious communications can be accomplished in several ways. For example, Figure 2 below depicts implementing the control (e.g., Intrusion Detection System (IDS)) in a centralized location (e.g., at a corporate hub site) rather than at every distributed "asset containing LIBCS" such as substations in this example "hub and spoke" model. The obligation in Section 3.1.2 requires that entities implement controls to detect known or suspected inbound and outbound malicious communications between a low impact BES Cyber System and a Cyber

Asset(s) outside the asset containing low impact BES Cyber System(s) thus allowing entity flexibility in where the control is implemented based on their architecture.

The DT considered entities that may use encryption to protect communications between hosts and the impact to the ability to detect known or suspected malicious communications. Because of the differences in entity programs, architectures, technologies and processes, the DT did not prescribe that encrypted communications must be decrypted for deep packet inspection when detecting known or suspected malicious communication. Requiring decryption/inspection/re-encryption may in some cases increase risk through introducing single points of failure or jeopardizing sensitive timing of communications. Entities may detect known or suspected malicious communications through other methods, such as detecting the appearance of abnormal new destination addresses or ports. The DT provided several other examples in Attachment 2. Entities may also choose to perform detection before or after the encryption tunnel occurs.

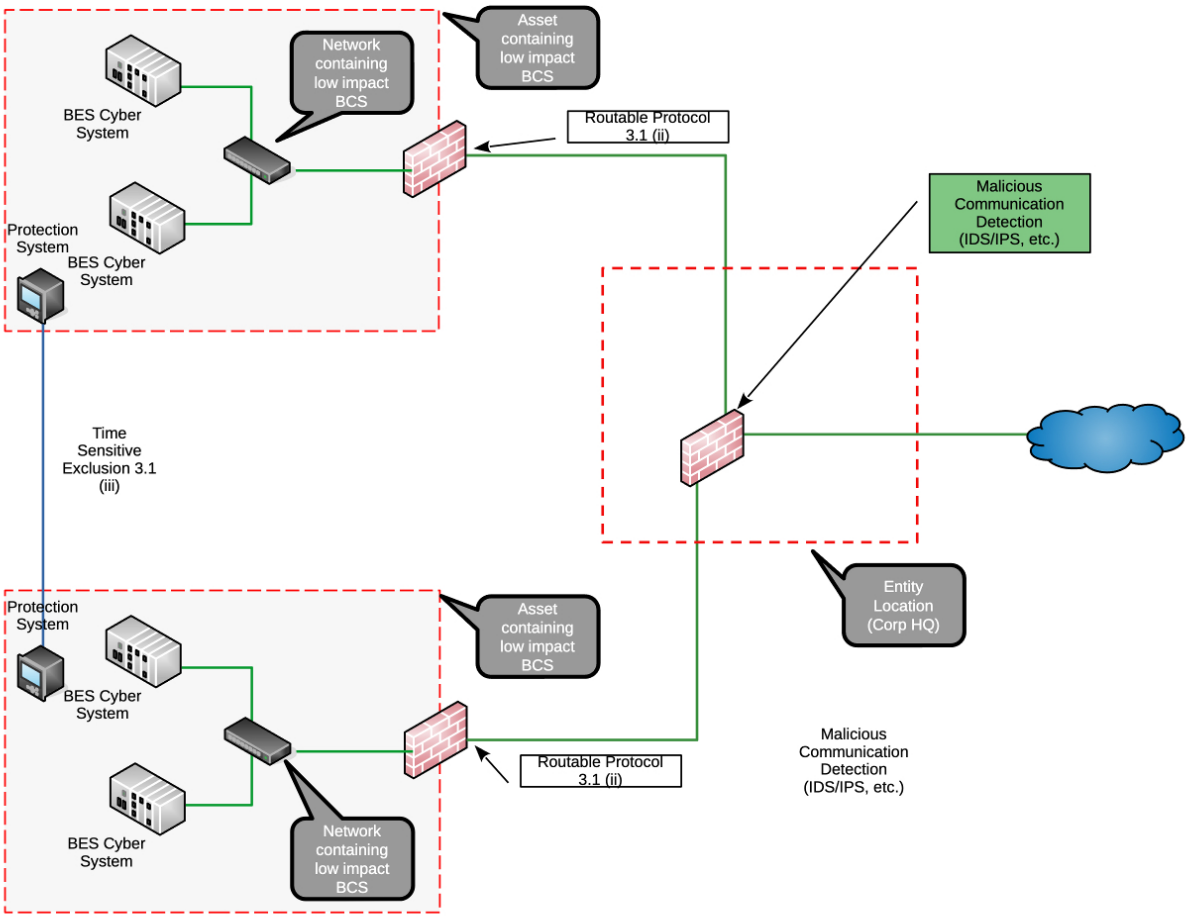


Figure 2

Section 3.1.3

This is a new cyber security control outlined in the SAR that requires entities to implement controls to authenticate users prior to permitting access to networks containing LIBCS. This control mitigates the risk of unauthenticated access to networks on which LIBCS reside. The intent is for each user to be authenticated (verifying a user) *before* they gain access to the "network containing low impact BES Cyber Systems"; thus, they have no ability to enumerate hosts on those networks, scan those networks for vulnerabilities, attempt logons to systems, or perform actions on those networks and systems before the entity has authenticated their user-initiated electronic access. It is important to note that Section 3.1.3 is not applicable to electronic access which sources (is connected) to the LIBCS network. For example, a laptop connected via an Ethernet cable to the LIBCS network would not be required to authenticate prior to accessing the LIBCS to which it is being connected. It is also important to note that the DT did not address specific account types (user or shared) used for authentication. While the intent is for entities to control each user prior to permitting electronic access, the SAR did not prescribe account types or passwords used by users to obtain (via authentication) electronic access. There are multiple methods to authenticate users for the responsible entity to choose.

Figure 3, below, depicts a situation where the authentication of the remote user is not occurring "prior to" but after the user already has access to the "network containing LIBCS" — as the authentication servers are on the same network with the LIBCS. The firewall in this scenario allows the user through to the network on which the LIBCS reside before the user is authenticated, and this does not meet the intent of the requirement.

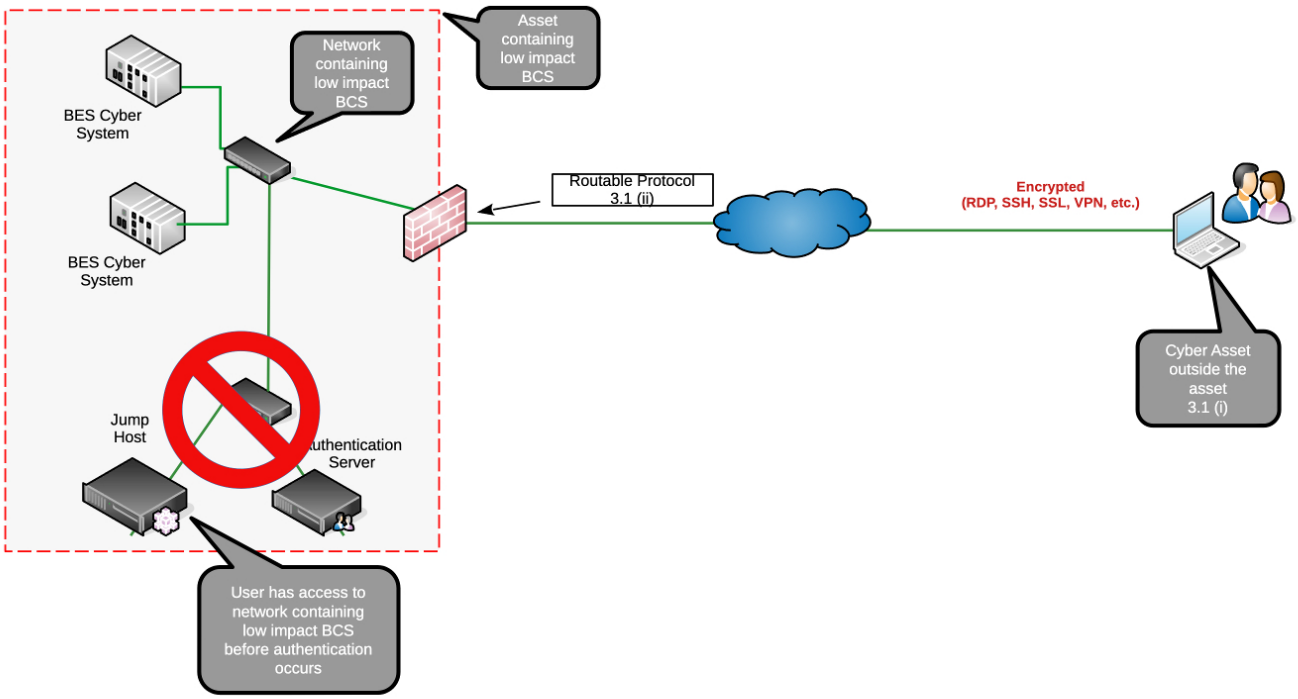


Figure 3

The intention of the phrase “each user prior to permitting access to a network(s)…” is meant to include the initial authentication and not all subsequent access to other downstream networks. If there is a collection of sub-networks or Cyber Assets within the network containing LIBCS, then multiple re-authentications at those levels would not be required by this specific requirement. Regardless of how many subsequent networks or BES Cyber Systems a user may access, as long as the entity’s implemented control(s) have authenticated the user prior to their access to those subsequent networks, that meets the intent. This may include, but is not limited to, configurations where authentication is local device specific authentication or configurations consisting of centralized authentication using technologies such as an access, terminal, or proxy server (“Intermediate System”) which processes authentication to the low impact asset networks through a centralized gateway.

The DT has not required the use of an “Intermediate System” as is prescribed in CIP-005 Requirement R2 for high and medium impact BES Cyber Systems. However, the DT’s intent is that those entities who have established or implemented such infrastructure or technologies may use them for authenticating access

to the assets containing low impact BES Cyber Systems to satisfy these requirements. While prescribing such an architecture as in CIP-005 Requirement R2 would further clarify CIP-003's requirements, the DT has chosen not to prescribe such requirements due to the impact to a broad and diverse range of entities and their specific technologies and processes used to meet low impact BES Cyber Systems authentication requirements. For example, it would be excessive to require an entity with a single CIP-003 applicable renewable generation site to implement architectures and technologies (Intermediate Systems) to meet the CIP-005 Requirement R2 Interactive Remote Access requirements. Such an entity may only need a Secure Sockets Layer (SSL) Virtual Private Network (VPN) to an access control device (e.g., firewall) at the one site that authenticates the user prior to allowing access to the network containing low impact BES Cyber Systems on its inside interface. The entity may also choose to authenticate a local non-low impact BES Cyber Systems network first, then control access to the LIBCS from that access point. Conversely, an entity with many assets distributed over a large geographic area, with a variety of impact categorizations and supporting BES Cyber Systems, may want to use their existing CIP-005 Requirement R2 remote access solutions for all of their sites (centralized access controls). The DT's intent in the CIP-003 language is to allow flexibility for both cases.

The phrase, "through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted" is included in Section 3.1.3 to clarify scoping. As Section 3.1.3 is written at a different granularity of "network(s) containing", which is not mentioned in the romanettes, this phrasing simply clarifies that the intended scope remains those networks through which the specific access described in the Section 3.1 romanettes is subsequently permitted. The romanettes (i), (ii), and (iii) in Section 3.1 define the ultimate access that is in scope, which is from a remote client outside the asset containing the LIBCS and destined for a LIBCS within the asset.

Section 3.1.4

This is a new cyber security control outlined in the SAR. The objective of Attachment 1, Section 3.1.4 is for entities to protect the user authentication information (e.g., username, password, multi-factor authentication (MFA) information, session token, etc.) while in transit between the remote user's Cyber Asset and either the asset containing the low impact BES Cyber Systems or the entity's authentication system used to meet Section 3.1.3. This mitigates the risk of user authentication information being captured, especially as some BES equipment may still require protocols that transmit such information in clear text. The intent is not to specify authentication directly to a particular device but to allow entities that desire to use an existing compliant CIP-005 Requirement R2 Intermediate System, or similar architecture, access to networks containing LIBCS (Figure 4). For example, Figure 4 below depicts protection of the user authentication information to the asset containing a LIBCS.

Figure 5 depicts an alternative example of protecting the user authentication information to/from a central system (i.e. jump host) *before* accessing a network containing a LIBCS. This protection mitigates the unintended disclosure of authentication information for electronic access to low impact cyber systems.

Note that both Figure 4 and Figure 5 have a significant difference from Figure 3 above in that, although the authentication services are also within the asset containing the LIBCS, they are located on a separate network from those containing BES Cyber Systems. In this example, assuming the firewall is configured to only allow authenticated user sessions on the jump host through to the network containing the LIBCS, this would meet the intent of the Section 3.1.3.

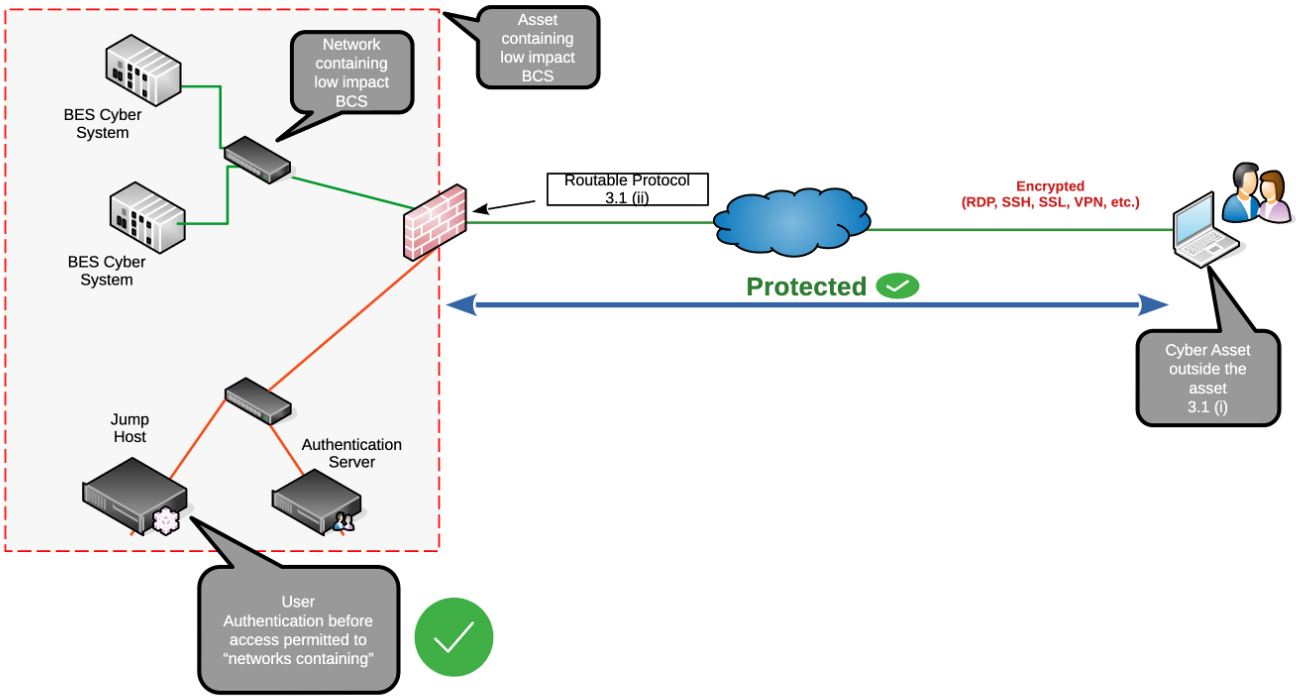


Figure 4

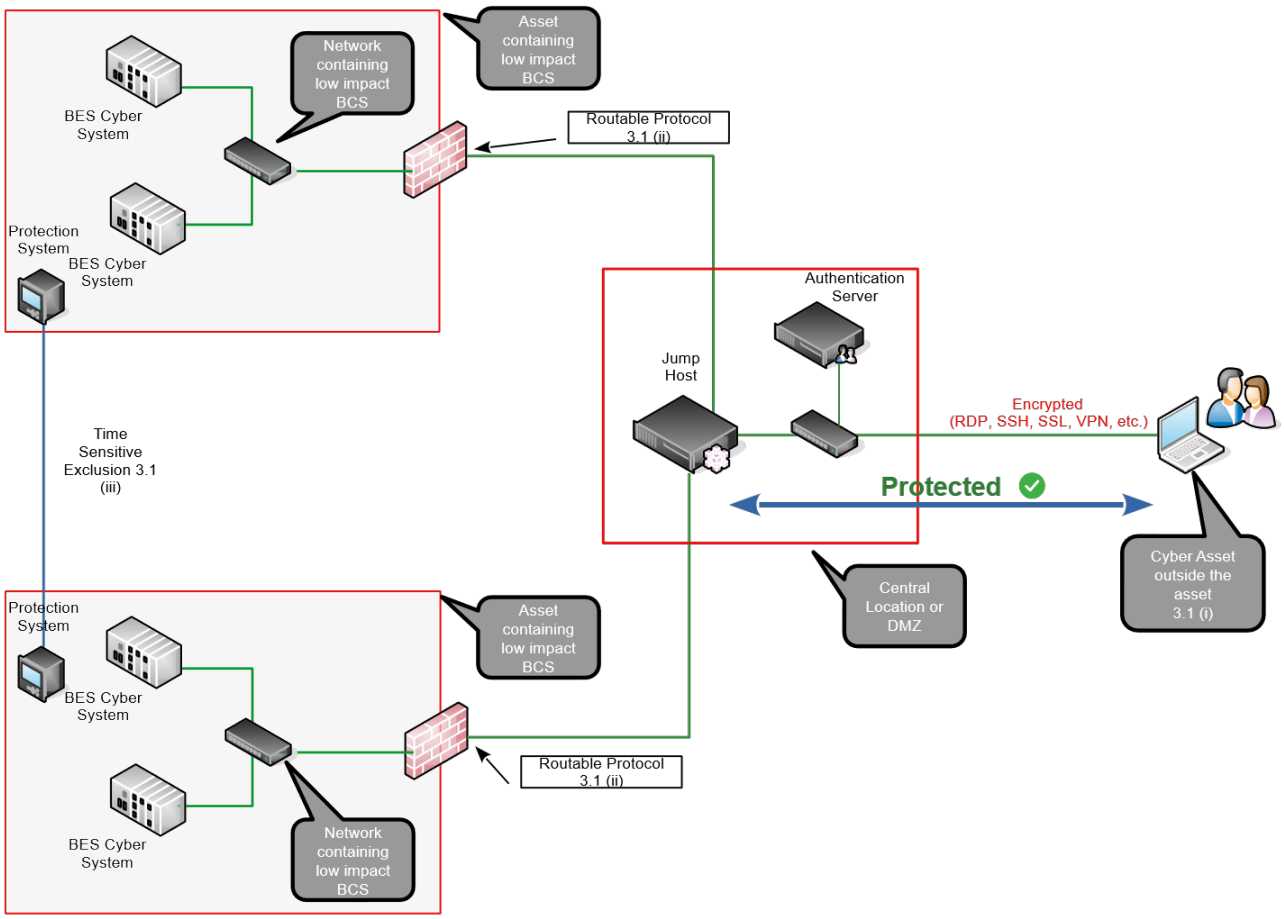


Figure 5

The DT has not required the use of an "Intermediate System" as is prescribed in CIP-005 Requirement R2 for high and medium impact BES Cyber Systems. However, the DT's intent is that those who have such infrastructures in place can, if they choose, use them for access to the assets containing low impact BES Cyber Systems to satisfy the intent of these requirements. While prescribing such an architecture as in CIP-005 Requirement R2 would make the target of CIP-003's requirements clearer to describe, the DT has chosen not to be this prescriptive due to the wide diversity of entities that may have only LIBCS. For example, an entity may have one small renewable generation site that falls under CIP-003 and implementing a full CIP-005 Requirement R2 "Interactive Remote Access with Intermediate System" architecture for access to one site may be excessive. That entity may only need an SSL VPN to an access control device (e.g., firewall) at the one site that authenticates the user and then allows access to the network containing LIBCS on its inside interface. However, an entity with 100 assets with BES Cyber Systems of varying impact categorization over a large geographic area may want to use their CIP-005 Requirement R2 remote access solution for all of their sites. The DT's intent in the CIP-003 language is to allow flexibility for both.

Section 3.1.5

The objective of Section 3.1.5 is to maintain the original language used in CIP-003-10, Section 6.1. One or more method(s) can be identified as part of this electronic access control. Entities must determine vendor electronic remote access, where permitted, to their LIBCS. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access.

Section 3.1.6

The objective of Section 3.1.6 is to maintain the original language used in CIP-003-10, Section 6.2. One or more method(s) can be identified as part of this electronic access control. Entities must have the ability to disable vendor electronic remote access, where permitted, for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing LIBCS.

Section 3.2

The DT made conforming changes to Section 3.2 with the objective to maintain the original intent of CIP-003-10, Section 3.2.

Special Scenarios

One low impact BES Cyber System across more than one asset containing that system.
In this scenario, a low impact BES Cyber System is not entirely located within one asset. For example, a generation resource has the majority of its BES Cyber System components within the site, but its network is extended full-time (e.g., over a dedicated circuit or dedicated VPN) to an operator console located at another site, and the console is part of the single BES Cyber System.

Since the components of the BES Cyber System are all located in "assets containing low impact BES Cyber System", just not a single asset, then this scenario is not in scope as it does not meet the condition of Section 3.1(i) of "between a low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber System(s)." The intent of Section 3.1.3 is authentication of users who are not located within any other "assets containing low impact BES Cyber System." This keeps CIP-003 analogous to the same concept in CIP-005 and the Interactive Remote Access definition that excludes from Interactive Remote Access user access that originates in another of the entity's Electronic Security Perimeters, such that operators in Control Centers are not required to implement CIP-005 Requirement R2 controls such as Intermediate Systems to operate field assets. It also avoids CIP-003 becoming circular when a local user at the BES Cyber System console would need to authenticate prior to permitting access to the extended network they are already on while seated at the console.

Rationale for Attachment 2

The DT made conforming changes to Attachment 2 merging Sections 3 and 6 and provided examples of compliance related activities.

Previous CIP-003 Versions Technical Rationale

Project 2020-03 Supply Chain Low Impact Revisions (CIP-003-9) Technical Rationale
Project 2016-02 Modifications to CIP Standards (CIP-003-10) Technical Rationale

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit D

Order No. 672 Criteria

EXHIBIT D

Order No. 672 Criteria

In Order No. 672,[1] the Commission identified a number of criteria it will use to analyze Reliability Standards proposed for approval to ensure they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. The discussion below identifies these factors and explains how proposed Reliability Standard CIP-003-11 has met or exceeded the criteria.

1. Proposed Reliability Standards must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve that goal.[2]

The proposed Reliability Standard would specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System ("BES"). Specifically, proposed Reliability Standard CIP-003-11 – Cyber Security – Security Management Controls would advance the reliability of the Bulk-Power System ("BPS") by mitigating the risks posed by a coordinated attack utilizing distributed low impact BES Cyber Systems by adding controls to authenticate remote users; protecting the authentication information

---

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

[2] *See id.* at P 321 ("The proposed Reliability Standard must address a reliability concern that falls within the requirements of section 215 of the FPA. That is, it must provide for the reliable operation of Bulk-Power System facilities. It may not extend beyond reliable operation of such facilities or apply to other facilities. Such facilities include all those necessary for operating an interconnected electric energy transmission network, or any portion of that network, including control systems. The proposed Reliability Standard may apply to any design of planned additions or modifications of such facilities that is necessary to provide for reliable operation. It may also apply to Cybersecurity protection.").

See id. at P 324 ("The proposed Reliability Standard must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve this goal. Although any person may propose a topic for a Reliability Standard to the ERO, in the ERO's process, the specific proposed Reliability Standard should be developed initially by persons within the electric power industry and community with a high level of technical expertise and be based on sound technical and engineering criteria. It should be based on actual data and lessons learned from past operating incidents, where appropriate. The process for ERO approval of a proposed Reliability Standard should be fair and open to all interested persons.").

in transit; and detecting malicious communications to or between assets containing low impact BES Cyber Systems with external routable connectivity. Proposed Reliability Standard CIP-003-11 is thus designed to achieve a specific reliability goal and contain a technically sound means to achieve that goal.

2. Proposed Reliability Standards must be applicable only to users, owners, and operators of the bulk power system, and must be clear and unambiguous as to what is required and who is required to comply.[3]

Proposed Reliability Standard CIP-003-11 is clear and unambiguous as to what is required and who is required to comply, in accordance with Order No. 672. The proposed standard is applicable to Balancing Authorities, Distribution Providers, Generator Operators, Generator Owners, Reliability Coordinators, Transmission Operators, and Transmission Owners. The proposed standard clearly articulates the actions that applicable entities must take to comply with the standard.

3. A proposed Reliability Standard must include clear and understandable consequences and a range of penalties (monetary and/or non-monetary) for a violation.[4]

The Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") for proposed Reliability Standard CIP-003-11 comport with NERC and Commission guidelines related to their assignment, as discussed further in **Exhibit E**. The assignment of the severity level for each VSL is consistent with the corresponding requirement, and the VSLs should ensure uniformity and consistency in the determination of penalties. The VSLs do not use any ambiguous terminology,

---

[3] *See id.* at P 322 ("The proposed Reliability Standard may impose a requirement on any user, owner, or operator of such facilities, but not on others.").

See id. at P 325 ("The proposed Reliability Standard should be clear and unambiguous regarding what is required and who is required to comply. Users, owners, and operators of the Bulk-Power System must know what they are required to do to maintain reliability.").

[4] *See id.* at P 326 ("The possible consequences, including range of possible penalties, for violating a proposed Reliability Standard should be clear and understandable by those who must comply.").

thereby supporting uniformity and consistency in the determination of similar penalties for similar violations. For these reasons, the proposed Reliability Standard includes clear and understandable consequences in accordance with Order No. 672.

4. A proposed Reliability Standard must identify clear and objective criteria or measures for compliance, so that it can be enforced in a consistent and non-preferential manner.[5]

Proposed Reliability Standard CIP-003-11 contains measures that support each requirement by clearly identifying what is required to demonstrate compliance. These measures help provide clarity regarding how the requirements would be enforced and help ensure that the requirements would be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party. The measures are substantively unchanged from the currently approved version.

5. Proposed Reliability Standards should achieve a reliability goal effectively and efficiently, but do not necessarily have to reflect "best practices" without regard to implementation cost or historical regional infrastructure design.[6]

The proposed Reliability Standard achieves the reliability goals effectively and efficiently in accordance with Order No. 672. Specifically, the proposed Reliability Standard would achieve the reliability goal of mitigating the risks posed by a coordinated attack utilizing distributed low impact BES Cyber Systems by adding controls to authenticate remote users; protecting the authentication information in transit; and detecting malicious communications to or between assets containing low impact BES Cyber Systems with external routable connectivity.

6. Proposed Reliability Standards cannot be "lowest common denominator," i.e., cannot reflect a compromise that does not adequately protect Bulk-Power System reliability.

---

[5] *See id.* at P 327 ("There should be a clear criterion or measure of whether an entity is in compliance with a proposed Reliability Standard. It should contain or be accompanied by an objective measure of compliance so that it can be enforced and so that enforcement can be applied in a consistent and non-preferential manner.").

[6] *See id.* at P 328 ("The proposed Reliability Standard does not necessarily have to reflect the optimal method, or 'best practice,' for achieving its reliability goal without regard to implementation cost or historical regional infrastructure design. It should however achieve its reliability goal effectively and efficiently.").

Proposed Reliability Standards can consider costs to implement for smaller entities, but not at consequences of less than excellence in operating system reliability.[7]

Proposed Reliability Standard CIP-003-11 does not reflect a "lowest common denominator" approach. The proposed revisions to Attachment 1 would improve the reliability of the BPS by mitigating the risks posed by a coordinated attack utilizing distributed low impact BES Cyber Systems. Specifically, the proposed revisions would add controls to authenticate remote users; protect the authentication information in transit; and detect malicious communications to or between assets containing low impact BES Cyber Systems with external routable connectivity.

[7] *See id.* at P 329 ("The proposed Reliability Standard must not simply reflect a compromise in the ERO's Reliability Standard development process based on the least effective North American practice—the so-called 'lowest common denominator'—if such practice does not adequately protect Bulk-Power System reliability. Although the Commission will give due weight to the technical expertise of the ERO, we will not hesitate to remand a proposed Reliability Standard if we are convinced it is not adequate to protect reliability.").

See id. at P 330 ("A proposed Reliability Standard may take into account the size of the entity that must comply with the Reliability Standard and the cost to those entities of implementing the proposed Reliability Standard. However, the ERO should not propose a 'lowest common denominator' Reliability Standard that would achieve less than excellence in operating system reliability solely to protect against reasonable expenses for supporting this vital national infrastructure. For example, a small owner or operator of the Bulk-Power System must bear the cost of complying with each Reliability Standard that applies to it.").

7. Proposed Reliability Standards must be designed to apply throughout North America to the maximum extent achievable with a single Reliability Standard while not favoring one geographic area or regional model. It should take into account regional variations in the organization and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.[8]

The proposed Reliability Standard would apply consistently throughout North America and does not favor one geographic area or regional model.

8. Proposed Reliability Standards should cause no undue negative effect on competition or restriction of the grid beyond any restriction necessary for reliability.[9]

Proposed Reliability Standard CIP-003-11 would have no undue negative effect on competition and would not unreasonably restrict the available transmission capacity or limit the use of the BPS in a preferential manner.

9. The implementation time for the proposed Reliability Standard is reasonable.[10]

The proposed implementation period, included as **Exhibit B**, for the proposed Reliability Standard is just and reasonable and designed to balance the urgency in the need to implement the standard against the time needed to comply. The proposed Implementation Plan provides that the

---

[8] *See id.* at P 331 ("A proposed Reliability Standard should be designed to apply throughout the interconnected North American Bulk-Power System, to the maximum extent this is achievable with a single Reliability Standard. The proposed Reliability Standard should not be based on a single geographic or regional model but should take into account geographic variations in grid characteristics, terrain, weather, and other such factors; it should also take into account regional variations in the organizational and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.").

[9] *See id.* at P 332 ("As directed by section 215 of the FPA, the Commission itself will give special attention to the effect of a proposed Reliability Standard on competition. The ERO should attempt to develop a proposed Reliability Standard that has no undue negative effect on competition. Among other possible considerations, a proposed Reliability Standard should not unreasonably restrict available transmission capability on the Bulk-Power System beyond any restriction necessary for reliability and should not limit use of the Bulk-Power System in an unduly preferential manner. It should not create an undue advantage for one competitor over another.").

[10] *See id.* at P 333 ("In considering whether a proposed Reliability Standard is just and reasonable, the Commission will consider also the timetable for implementation of the new requirements, including how the proposal balances any urgency in the need to implement it against the reasonableness of the time allowed for those who must comply to develop the necessary procedures, software, facilities, staffing or other relevant capability.").

standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the effective date of the Commission's order approving the standard.

With respect to initial compliance with periodic requirements, the Implementation Plan notes that periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .". The Implementation Plan provides that Responsible Entities[11] shall initially comply with Requirement R1, Part 1.2.3 on or before the effective date of CIP-003-11. The Implementation Plan further provides that Responsible Entities shall initially comply with all other periodic requirements in CIP-003-11 within the periodic timeframes of their last performance under the version of the CIP-003 Reliability Standard then in effect.

Under the proposed Implementation Plan, entities shall not be required to comply with Requirement R2 as it relates to the implementation of documented cyber security plan(s) addressing Attachment 1 Section 3.1.2 until the later of: (1) April 1, 2029; or (2) the effective date of Reliability Standard CIP-003-11.

10. The Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[12]

Proposed Reliability Standard CIP-003-11 was developed in accordance with NERC's Commission-approved processes for developing and approving Reliability Standards. **Exhibit F** includes a summary of the development proceedings for the proposed standard, and details the

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

[12] *See* Order No. 672, *supra*, at P 334 ("Further, in considering whether a proposed Reliability Standard meets the legal standard of review, we will entertain comments about whether the ERO implemented its Commission-approved Reliability Standard development process for the development of the particular proposed Reliability Standard in a proper manner, especially whether the process was open and fair. However, we caution that we will not be sympathetic to arguments by interested parties that choose, for whatever reason, not to participate in the ERO's Reliability Standard development process if it is conducted in good faith in accordance with the procedures approved by the Commission.").

processes followed to develop the proposed standard. These processes included, among other things, public comment and ballot periods. Additionally, all meetings of the drafting team were properly noticed and open to the public.

11. NERC must explain any balancing of vital public interests in the development of proposed Reliability Standards.[13]

NERC has identified no competing public interests regarding the proposed standard. No comments were received that indicated that the proposed standard conflicts with other vital public interests.

12. Proposed Reliability Standards must consider any other appropriate factors.[14]

No other negative factors relevant to whether the proposed Reliability Standard is just and reasonable were identified.

---

[13] *See id.* at P 335 ("Finally, we understand that at times development of a proposed Reliability Standard may require that a particular reliability goal must be balanced against other vital public interests, such as environmental, social and other goals. We expect the ERO to explain any such balancing in its application for approval of a proposed Reliability Standard.").

[14] *See id.* at P 323 ("In considering whether a proposed Reliability Standard is just and reasonable, we will consider the following general factors, as well as other factors that are appropriate for the particular Reliability Standard proposed.").

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit E

Analysis of Violation Risk Factors
and Violation Severity Levels

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2023-04 Modifications to CIP-003

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2023-04 Modifications to CIP-003. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

Justification for VRFs and VSLs

- Requirement R1: There were no changes to VRFs from the previously FERC-approved CIP-003-9 Reliability Standard and only conforming or non-substantive changes to the VSLs.
- Requirement R2: The VRF did not change from the previously FERC-approved CIP-003-9 Reliability Standard. VSL changes are outlined below.
- Requirement R3: There were no changes to VRFs from the previously FERC-approved CIP-003-9 Reliability Standard and only conforming or non-substantive changes to the VSLs.
- Requirement R4: There were no changes to VRFs from the previously FERC-approved CIP-003-9 Reliability Standard and only conforming or non-substantive changes to the VSLs.

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document the electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2)	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security controls according to Requirement R2, Attachment 1,	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to implement three or more controls listed in Requirement R2, Attachment 1, Section 2. (Requirement R2)	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	Section 2. (Requirement R2) OR The Responsible Entity failed to implement one or two controls listed in Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code	OR The Responsible Entity failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code	

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

VSL Justifications for CIP-003-A, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSLs for Requirement R2 are similar to the previous VSLs of CIP-003-9, with a few revisions. Created Moderate and High VSL based on the number of controls implemented. Removed mentions of Attachment 1, Section 6, since Section 6 was merged with Section 3.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Requirement R2 is not a "binary" type requirement. Violation severity levels are clear, quantitative, and non-ambiguous.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The VSL level assignments are consistent with language in Requirement R2 and Attachment 1.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The violation severity levels relate to a single violation. A failure to do multiple portions of Requirement R2, Attachment 1 is considered a single violation.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit F

Summary of Development
and Complete Record of Development

Summary of Development History

The following is a summary of the development record for proposed Reliability Standard – CIP-003-11 – Cyber Security – Security Management Controls developed under Project 2023-04 Modifications to CIP-003.

I. Overview of the Standard Drafting Team

When evaluating a proposed Reliability Standard, the Commission is expected to give "due weight" to the technical expertise of the ERO.[1] The technical expertise of the ERO is derived from the drafting team selected to lead each project in accordance with Section 4.3 of the NERC Standard Processes Manual.[2] For this project, the drafting team consisted of industry experts, all with a diverse set of experiences. A roster of the Project 2023-04 drafting team members is included in **Exhibit G**.

II. Standard Development History

A. Project Initiation

In response to a February 4, 2021 NERC Board of Trustees ("Board") directive, NERC staff formed the Low Impact Criteria Review Team ("LICRT") to analyze the degrees of risk presented by various facilities that house low impact BES Cyber Assets and to report on whether the low impact criteria should be modified. The Board accepted the recommendations of the LICRT at its November 16, 2022 meeting and asked that the recommendations in the report be initiated through the NERC Standards Development Process.

In December 2023, the LICRT submitted a SAR reflecting the recommendations from its report to modify CIP-003-9 to add controls to authenticate remote users, protect the authentication

---

1 Section 215(d)(2) of the Federal Power Act; 16 U.S.C. § 824(d)(2).

2 The NERC *Standard Processes Manual* is available at https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

information in transit, and detect malicious communications for assets containing low impact BES Cyber Systems with external routable connectivity.

B. Standard Authorization Request Development

On March 22, 2023, the Standards Committee accepted the SAR, authorized posting for a 45-day formal comment period, and authorized the solicitation of the drafting team members.[3] The comment period and the nomination period for the SAR drafting team was open from March 31, 2023 – May 15, 2023. The Standards Committee accepted the revised SAR in an Action Without a Meeting on July 27, 2023 and authorized drafting revisions to the standard.[4]

C. First Posting – Comment Period, Initial Ballot, and Non-binding Poll; Supplemental Drafting Team Nominations

On October 18, 2023, the Standards Committee authorized initial posting of proposed Reliability Standard CIP-003-A, the associated Implementation Plan, and other associated documents for a 45-day formal comment period from October 24, 2023 – December 7, 2023, with a parallel initial ballot and non-binding poll on the Violation Risk Factors ("VSFs") and Violation Severity Levels ("VSLs") held during the last 10 days of the comment period from November 28, 2023 – December 7, 2023.[5]

---

[3] NERC, *Meeting Minutes – Standards Committee Meeting* at agenda item 5 (Modifications to CIP-003 Standard Authorization Request) (Mar. 22, 2023), https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/March%20Meeting%20Minutes%20-%20Approved%20April%2019,%202023.pdf.

[4] NERC, *Standards Committee Action without a Meeting Results* (July 31, 2023), https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC%20Action%20without%20a%20Meeting%20Results%20-%20July%2031,%202023.pdf.

[5] NERC, *Meeting Minutes – Standards Committee Meeting* at agenda item 6 (Project 2023-04 Modifications to CIP-003) (Oct. 18, 2023), https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC%20October%20Minutes%20-%20Approved%20November%2015,%202023.pdf.

Concurrently, supplemental drafting team nominations were also authorized and posted from October 24, 2023 – December 7, 2023.[6] The Standards Committee appointed a chair and supplemental members to the Project 2023-04 Drafting Team at its January 17, 2024 meeting.[7]

The initial ballot and non-binding poll results for the proposed Reliability Standard are as follows:

- Proposed Reliability Standard CIP-003-A received 35.04 percent approval, reaching quorum at 92.81 percent of the ballot pool. The non-binding poll for the associated VRFs and VSLs received 32.11 percent supportive opinions, reaching quorum at 91.07 percent of the ballot pool.[8]
- The Implementation Plan received 40.86 percent approval, reaching quorum at 92.15 percent of the ballot pool.[9]

There were 63 sets of responses, including comments from approximately 165 different individuals and approximately 104 companies, representing all 10 industry segments.[10]

D. Second Posting – Comment Period, Additional Ballot, and Non-binding Poll

Proposed Reliability Standard CIP-003-A, the associated Implementation Plan, and other associated documents were posted for a 45-day formal comment period from January 30, 2024 – March 14, 2024, with a parallel additional ballot and non-binding poll held during the last 10 days

---

6 *Id.*

7 NERC, *Meeting Minutes – Standards Committee Meeting* at agenda item 6 (Project 2023-04 Modifications to CIP-003) (Jan. 17, 2024), https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC_Meeting_Minutes-January2024.pdf.

8 Exhibit F at items 24, 26.

9 *Id.* at item 25.

10 *Id.* at item 21.

of the comment period from March 5, 2024 – March 14, 2024. The additional ballot and non-binding poll results for the proposed Reliability Standard are as follows:

- Proposed Reliability Standard CIP-003-A received 60.34 percent approval, reaching quorum at 91.1 percent of the ballot pool. The non-binding poll for the associated VRFs and VSLs received 60.1 percent supportive opinions, reaching quorum at 87.14 percent of the ballot pool.[11]
- The Implementation Plan received 60.95 percent approval, reaching quorum at 90.78 percent of the ballot pool.[12]

There were 71 sets of responses, including comments from approximately 169 different individuals and approximately 111 companies, representing all 10 industry segments.[13]

E. Third Posting – Comment Period, Additional Ballot, and Non-binding Poll

Two versions[14] of proposed Reliability Standard CIP-003, CIP-003-11 and CIP-003-12, along with their the associated Implementation Plans, and other associated documents were concurrently posted on a single ballot for a 30-day formal comment period from June 12, 2024 – July 11, 2024, with a parallel additional ballot and non-binding poll held during the last 10 days

11 *Id.* at items 39, 6415.

12 *Id.* at item 40.

13 *Id.* at item 36.

14 Two versions of CIP-003 were posted on the same ballot. This occurred because two drafting teams (Project 2016-02 and Project 2023-04) were simultaneously revising CIP-003-9. Project 2016-02's work passed final ballot and was approved by the NERC Board of Trustees in May, 2024 and became CIP-003-10 while Project 2023-04 was still in progress and became CIP-003-11. The two versions that were simultaneously posted by the Project 2023-04 team reflected the changes made by Project 2023-04 to CIP-003-9 and then the Project 2023-04 revisions on top of the Project 2016-02 revisions that resulted in CIP-003-10.

of the comment period from July 2, 2024 – July 11, 2024.[15] The additional ballot and non-binding poll results for the proposed Reliability Standards are as follows:

- Proposed Reliability Standards CIP-003-11 and CIP-003-12 received 80.58 percent approval, reaching quorum at 79.11 percent of the ballot pool. The non-binding poll for the associated VRFs and VSLs received 82.22 percent supportive opinions, reaching quorum at 76.43 percent of the ballot pool.[16]
- The Implementation Plan received 64.01 percent approval, reaching quorum at 78.84 percent of the ballot pool.[17]

There were 54 sets of responses, including comments from approximately 154 different individuals and approximately 92 companies representing all 10 industry segments.[18]

F. Fourth Posting – Comment Period, Additional Ballot, and Non-binding Poll

Proposed Reliability Standard CIP-003-11, the associated Implementation Plan, and other associated documents were posted for a 30-day formal comment period from September 11, 2024 – October 10, 2024, with an additional ballot and non-binding poll to be held the final 10 days from October 1, 2024 – October 10, 2024. The additional ballot and non-binding poll results for the proposed Reliability Standard are as follows:

- Proposed Reliability Standard CIP-003-11 received 93.89 percent approval, reaching quorum at 87.67 percent of the ballot pool. The non-binding poll for the associated VRFs and VSLs received 92.75 percent supportive opinions, reaching quorum at 85 percent of the ballot pool.[19]

---

15 *Id*. at items 76, 80.

16 *Id.* at items 57, 59.

17 *Id.* at item 58.

18 *Id.* at item 54.

19 *Id.* at items 71, 73.

- The Implementation Plan received 93.44 percent approval, reaching quorum at 87.03 percent of the ballot pool.[20]

There were 47 sets of responses, including comments from approximately 102 different individuals and approximately 69 companies representing 7 industry segments.[21]

G. Final Documents

The drafting team posted the final documents of CIP-003-11 – Cyber Security – Security Management Controls, but did not conduct a final ballot, per the Standard Processes Manual section 4.13, as the previous ballot achieved at least 85% weighted segment approval and the drafting team proposed no further changes to the balloted documents.[22]

Consistent with these requirements, the last ballot received 93.89% approval. The drafting team made a good faith effort to resolve objections and responded to comments in writing, including making minor corrections to two of the non-mandatory and enforceable sections of the standard.

H. Board of Trustees Adoption

At its December 10, 2024 meeting, the NERC Board of Trustees adopted proposed Reliability Standard CIP-003-11, the Implementation Plan, the VRFs and VSLs, and the retirement of CIP-003-10 or the currently effective version of Reliability Standard CIP-003.[23]

---

[20] *Id.* at item 72.

[21] *Id.* at item 68.

[22] *See id.* at item 81.

[23] NERC, *Board of Trustees Agenda Package Dec. 10, 2024*, Agenda Item 3a (Project 2023-04 Modifications to CIP-003), https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Board_Open_Meeting%20Agenda%20Package%20-%20December%202024%20-%20ATT.pdf.

Complete Record of Development

Project 2023-04 Modifications to CIP-003

Related Files

Status

The drafting team is posting the final documents of **CIP-003-11 – Cyber Security – Security Management Controls,** but not conducting a final ballot, per the Standard Processes Manual (SPM) section 4.13, which allows the drafting team to conclude the standards action without conducting a final ballot if:

- the previous ballot achieved at least 85% weighted segment approval;
- the drafting team made a good faith effort at resolving applicable objections;
- the drafting team responded in writing to comments as required by section 4.12; and
- the drafting team is proposing no further changes to the balloted documents.

Consistent with these requirements, the last ballot received 93.89% approval. The drafting team has made a good faith effort to resolve objections and responded to comments in writing, including making minor corrections to two of the non-mandatory and enforceable sections of the standard.

Per SPM section 2.5: "The only mandatory and enforceable components of a Reliability Standard are the: (1) applicability, (2) Requirements, and the (3) effective dates. The additional components are included in the Reliability Standard for informational purposes and to provide guidance to Functional Entities concerning how compliance will be assessed by the Compliance Enforcement Authority."

Background

In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact Bulk Electric System (BES) Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the SAR at its March 22, 2023 meeting.

Standard Affected: CIP-003-9

Purpose/Industry Need

The LICRT report recognized that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The team recommended enhancing the existing low impact category to further mitigate the coordinated attack risk. The proposed project will revise CIP-003-9 to add controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications assets containing low impact BES Cyber Systems with external routable connectivity.

Subscribe to this project's observer mailing list

Select "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003 Observer List” in the Description Box.

Draft	Actions	Dates	Results	Consideration of Comments
Final Documents **CIP-003-11** Clean **(74)** | Redline to last posted **(75)** | Redline to CIP-003-10 (Last Board Approved) **(76)** Implementation Plan **(77)** **Supporting Materials** Technical Rationale **(78)** VRF/VSL Justifications **(79)** RSAW **(80)**	Info **(81)**	11/13/24		
Draft 4 **CIP-003-11** Clean **(60)** | Redline to CIP-003-10 (Last Board Approved) **(61)** Implementation Plan **(62)** **Supporting Materials** Technical Rationale **(63)** Unofficial Comment Form **(64)** VRF/VSL Justifications **(65)**	Additional Ballot Ballot Open Reminder **(69)** Info **(70)** Vote	10/01/24 - 10/10/24	Ballot Results CIP-003-11 **(71)** Implementation Plan **(72)** Non-binding Poll Results **(73)**	Consideration of Comments **(68)**
	Comment Period Info **(66)** Submit Comments	09/11/24 - 10/10/24	Comments Received **(67)**	

Draft 3 **CIP-003-11** Clean **(42)** | Redline to Last Posted **(43)** | Redline to CIP-003-9 (Last Approved) **(44)** Implementation Plan **(45)** **CIP-003-12** Redline to CIP-003-9 **(46)** Implementation Plan **(47)** **Supporting Materials** Technical Rationale **(48)** Unofficial Comment Form **(49)** VRF/VSL Justifications **(50)** Summary of Changes **(51)**	Additional Ballot Ballot Open Reminder **(55)** Info **(56)** Vote Comment Period Info **(52)** Submit Comments	07/2/24 - 07/11/24 06/12/24 - 07/11/24	Ballot Results CIP-003-11 and CIP-003-12 **(57)** Implementation Plan **(58)** Non-binding Poll Results **(59)** Comments Received **(53)**	Consideration of Comments **(54)**
Draft 2 **CIP-003-A** Clean **(27)** | Redline to Last Posted **(28)** | Redline to Last Approved **(29)** Implementation Plan **(30)** **Supporting Materials** Technical Rationale **(31)** Unofficial Comment Form **(32)** VRF/VSL Justifications **(33)**	Additional Ballot Ballot Open Reminder **(37)** Info **(38)** Vote Comment Period Info **(34)** Submit Comments	03/5/24 - 03/14/24 01/30/24 - 03/14/24	Ballot Results CIP-003-A **(39)** Implementation Plan **(40)** Non-binding Poll Results **(41)** Comments Received **(35)**	Consideration of Comments **(36)**
Draft 1 **CIP-003-A** Clean **(11)** | Redline to Last Approved **(12)** Implementation Plan **(13)** **Supporting Materials** Technical Rationale **(14)** Unofficial Comment Form **(15)** VRF/VSL Justifications **(16)**	Initial Ballot Ballot Open Reminder **(22)** Info **(23)** Vote Join Ballot Pools Comment Period Info **(19)** Submit Comments	11/28/23 - 12/07/23 10/24/23 - 11/27/23 10/24/23 - 12/07/23	**Ballot Results** CIP-003-A **(24)** Implementation Plan **(25)** Non-binding Poll Results **(26)** Comments Received **(20)**	Consideration of Comments **(21)**
Supplemental Drafting Team Nominations **Supporting Materials** Unofficial Nomination Form (Word) **(17)**	Supplemental Nomination Period Info **(18)** Submit Nominations	10/24/23 - 12/07/23		
Standard Authorization Request Clean **(9)** | Redline **(10)**	Accepted by the Standards Committee	07/27/23		
Standard Authorization Request (3) Low Impact Criteria Review Team Report **(4)** **Supporting Materials** Unofficial Comment Form (Word) **(5)**	Comment Period Info **(6)** Submit Comments	03/31/23 - 05/15/23	Comments Received **(7)**	Consideration of Comments **(8)**
Drafting Team Nominations **Supporting Materials** Unofficial Nomination Form (Word) **(1)**	Nomination Period Info **(2)** Submit Nominations	03/31/23 - 05/15/23		

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form

Project 2023-04 Modifications to CIP-003 Standard Authorization Request Drafting Team

Do not use this form for submitting nominations. Use the electronic form to submit nominations for **Project 2023-04 Modifications to CIP-003** Standard Authorization Request (SAR) drafting team members by **8 p.m. Eastern, Monday, May 15, 2023.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form.

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Chris Larson (via email), or at 470-599-3851.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required. A brief description of the desired qualifications, expected commitment, and other pertinent information is included below.

Background

In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact Bulk Electric System (BES) Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the SAR at its March 22, 2023 meeting.

The LICRT report recognized that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The team recommended enhancing the existing low impact category to further mitigate the coordinated attack risk. The proposed project will revise CIP-003-9 to add controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications assets containing low impact BES Cyber Systems with external routable connectivity.

Standard(s) affected: CIP-003-9

Drafting Team activities include participation in technical conferences, stakeholder communications and outreach events, periodic drafting team meetings and conference calls. Approximately one face-to-face meeting per quarter can be expected (on average three full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the drafting team sets forth. NERC is seeking individuals who possess experience in the following areas:

- Experience with CIP-003-9 and Cyber Security Management Controls
- Understanding of BES Cyber Asset Low Impact Criteria
- Understanding of reliability risks associated with BES Cyber Assets and BES Cyber Systems
- Understanding of coordinated attack risks and mitigation options
- Understanding of external routable connectivity (ERC)
- Understanding of authentication for remote users
- Understanding of protection of user authentication information
- Understanding of detection of malicious communications
- Responsible entity compliance related to the areas listed above

Name:	
Organization:	
Address:	
Telephone:	
Email:	
Please briefly describe your experience and qualifications to serve on the requested SAR Drafting Team (Bio):	
If you are currently a member of any NERC drafting team, please list each team here: ☐ Not currently on any active SAR or standard drafting team. ☐ Currently a member of the following SAR or standard drafting team(s):	

If you previously worked on any NERC drafting team please identify the team(s):
☐ No prior NERC SAR or standard drafting team.
☐ Prior experience on the following team(s):
Acknowledgement that the nominee has read and understands both the *NERC Participant Conduct Policy* and the *Standard Drafting Team Scope* documents, available on NERC Standards Resources.
☐ Yes, the nominee has read and understands these documents.

Select each NERC Region in which you have experience relevant to the Project for which you are volunteering:		
☐ MRO ☐ NPCC ☐ RF	☐ SERC ☐ Texas RE ☐ WECC	☐ NA – Not Applicable

Select each Industry Segment that you represent:	
☐	1 — Transmission Owners
☐	2 — RTOs, ISOs
☐	3 — Load-serving Entities
☐	4 — Transmission-dependent Utilities
☐	5 — Electric Generators
☐	6 — Electricity Brokers, Aggregators, and Marketers
☐	7 — Large Electricity End Users
☐	8 — Small Electricity End Users
☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
☐	10 — Regional Reliability Organizations and Regional Entities
☐	NA – Not Applicable

Select each Function[1] in which you have current or prior expertise:	
☐ Balancing Authority	☐ Transmission Operator
☐ Compliance Enforcement Authority	☐ Transmission Owner
☐ Distribution Provider	☐ Transmission Planner
☐ Generator Operator	☐ Transmission Service Provider
☐ Generator Owner	☐ Purchasing-selling Entity
☐ Interchange Authority	☐ Reliability Coordinator
☐ Load-serving Entity	☐ Reliability Assurer
☐ Market Operator	☐ Resource Planner
☐ Planning Coordinator	

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group:			
Name:		Telephone:	
Organization:		Email:	
Name:		Telephone:	
Organization:		Email:	

Provide the name and contact information of your immediate supervisor or a member of your management who can confirm your organization's willingness to support your active participation.			
Name:		Telephone:	
Title:		Email:	

[1] These functions are defined in the NERC Functional Model, which is available on the NERC web site.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-04 Modifications to CIP-003

Nomination Period Open through May 15, 2023

Now Available

Nominations are being sought for **Project 2023-04 Modifications to CIP-003** Standard Authorization Request (SAR) drafting team members through **8 p.m. Eastern, Monday, May 15, 2023.**

Use the electronic form to submit a nomination. Contact Cindy Jackson regarding issues using the electronic form. An unofficial Word version of the nomination form is posted on the Standard Drafting Team Vacancies page and the project page.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

The time commitment for this project is expected to be up to two face-to-face meetings per quarter (on average two full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the review or drafting team sets forth. Team members may also have side projects, either individually or by subgroup, to present to the larger team for discussion and review. Lastly, an important component of the review and drafting team effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful project outcome.

NERC is seeking individuals from organizations who possess experience with CIP-003 Security Management Controls including Generator Owner/Operator, Reliability Coordinator, Balancing Authority, Transmission Owner/Operator, and Distribution Provider.

Previous drafting team experience is beneficial but not required. See the project page and nomination form for additional information.

Next Steps

The Standards Committee is expected to appoint members to the SAR drafting team in June or July 2023. Nominees will be notified shortly after they have been appointed.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Chris Larson (via email) or at 470-599-3851. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Coordinated cyber attack controls for low impact BES Cyber Assets		
Date Submitted:	12/20/2023		
SAR Requester			
Name:	Howard Gugel on behalf of the Low Impact Criteria Review Team		
Organization:	NERC		
Telephone:	404-446-9693	Email:	Howard.gugel@nerc.net
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☒ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☒ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☐ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
In light of recent cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact BES Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The report may be found here.			

Requested information
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
The LICRT conclusions regarding low impact BES Cyber Systems are as follows: • Individually, low impact BES Cyber Systems are truly low impact to BES reliability. This corresponds to the longstanding work of NERC and the stakeholders to design and operate the BES to withstand the loss of any of its individual assets. A medium or high impact BES Cyber System is more than an impact to a typical single BES Element/Facility. Therefore, the team does not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems. • The team recognizes that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The team recommends enhancing the existing low impact category to further mitigate the coordinated attack risk.
Project Scope (Define the parameters of the proposed project):
Modify CIP-003-9 to add controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications assets containing low impact BES Cyber Systems with external routable connectivity.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):
Modify CIP-003-9 to add: • Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity. • Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity. • Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity. To limit the scope of the requirements to only those that have external routable connectivity, the drafting team may need to create a new defined term or modify an existing defined term. For a complete technical justification and technical foundation, please refer to the Low Impact Criteria Review Report.

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impacts are unknown at this time.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
None
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator, Transmission Owner
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
The white paper was developed by industry experts and posted for industry comment prior to being presented to the Board.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
If not completed by the initiation of this SAR: 2016-02 Modifications to CIP Standards 2021-03 CIP-002 Transmission Owner Control Centers
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Reliability Principles	
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
e.g., NPCC	none

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised

1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Low Impact Criteria Review Report

NERC Low Impact Criteria Review Team White Paper

October 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

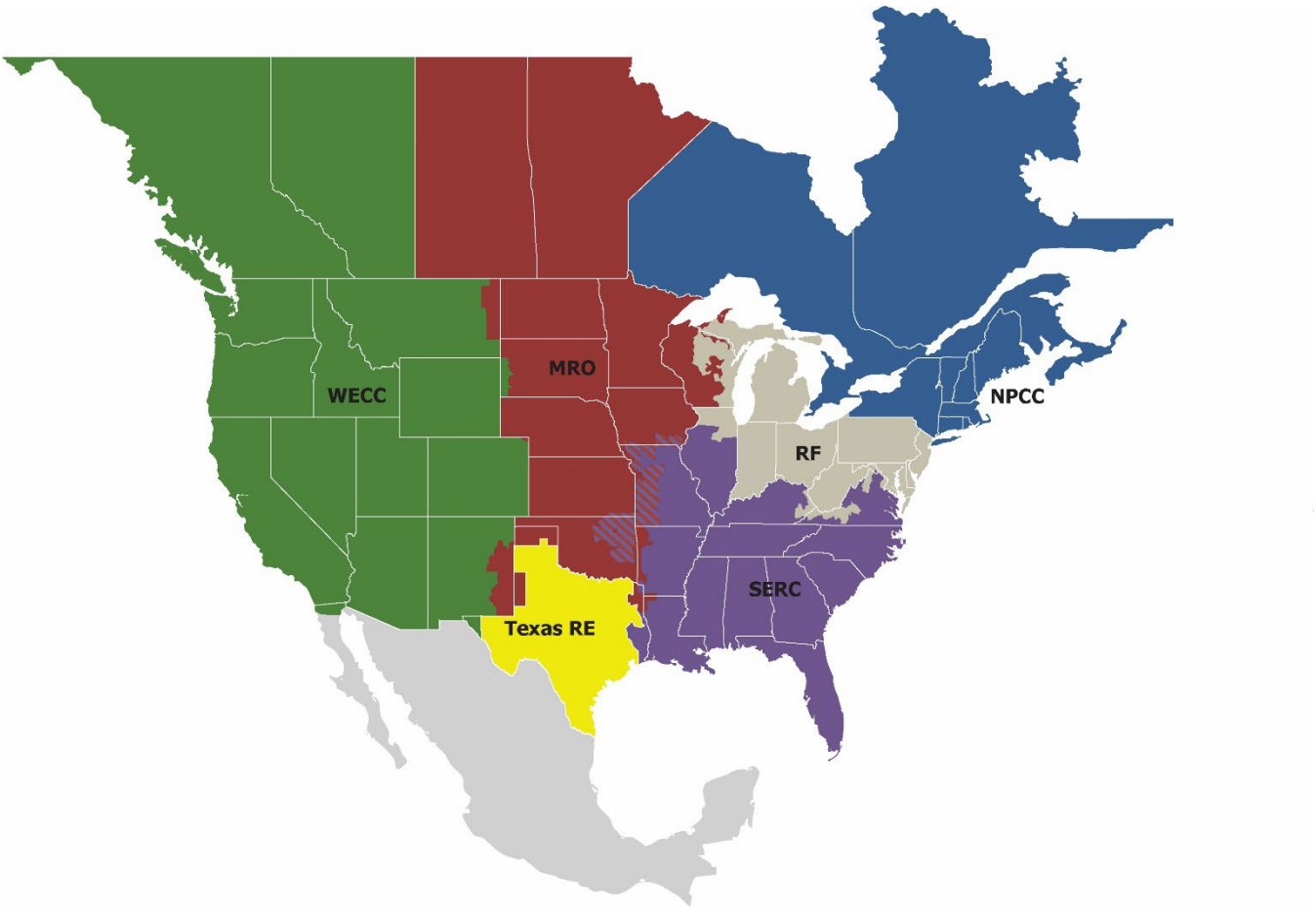
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entity boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

Communications, information technology, and industrial control systems provide various opportunities for adversaries to initiate a coordinated cyber attack, thereby presenting Bulk Electric System (BES) security risk. NERC is committed to using reliability tools to support industry's efforts to mitigate these coordinated cyber attacks risks.

In 2017, NERC developed new and revised critical infrastructure protection (CIP) Reliability Standards to help mitigate cybersecurity risks associated with the supply chain for high and medium impact BES Cyber Systems. These standards, collectively referred to as Supply Chain Standards, consist of new Reliability Standard CIP-013-1 and revised Reliability Standards CIP-010-3 and CIP-005-6. Consistent with the risk-based framework of the NERC CIP Reliability Standards, the Supply Chain Standards are applicable to systems that pose the greatest BES impact. To fully understand these Supply Chain risks, NERC collected registered entity data pursuant to NERC Rules of Procedure Section 1600 request for data or information.

NERC staff's analysis of the data shows that, while an individual compromise to any one low impact BES Cyber Asset facility would generally be a localized event, a coordinated cyber attack with control of multiple facilities may result in an interconnection-wide BES event. The vast majority of transmission station and substation low impact BES Cyber Assets are at facilities that have at most only one line greater than 300 kV or two lines greater than 200 kV (but less than 300 kV). Similarly, the vast majority of generation resource low impact BES Cyber Assets are at facilities that have less than 500 MW. In other words, an individual compromise to any one of these locations (transmission substations or generation resources) would generally be a localized event. However, a coordinated cyber attack with control of multiple facilities may result in an interconnection-wide BES event.

On December 13, 2020, FireEye Inc., a cybersecurity solutions and forensics firm, publicly posted details about an attack on the Orion platform developed by SolarWinds. Underscoring the severity of the event, on December 13, 2020, the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 21-01. This Directive required Federal agencies to take action based on the DHS assessment that a successful compromise from the SolarWinds Orion platform attack would have "grave" consequences.

In light of these recent cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC Staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact BES Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems. In this report, the LICRT documents the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks.

The LICRT conclusions regarding low impact BES Cyber Systems are as follows:

- Individually, low impact BES Cyber Systems are truly low impact to BES reliability. This corresponds to the longstanding work of NERC and the stakeholders to design and operate the BES to withstand the loss of any of its individual assets. A medium or high impact BES Cyber System is more than an impact to a typical single BES Element/Facility. Therefore, the team does not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems.

- The team recognizes that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The team recommends enhancing the existing low impact category to further mitigate the coordinated attack risk.

Those recommendations, sorted by category, are as follows:

CIP Standards Revisions

- Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity.

Security Guidelines

- Develop Security Guideline for protection of communications to and between assets containing low impact BES Cyber Systems across publicly accessible networks.
- Develop Security Guideline for procurement risk evaluation for low impact BES Cyber Systems.
- Develop Security Guideline for entities to voluntarily submit an E-ISAC report for unauthorized physical access attempts to low impact BES Cyber Systems.
- Develop Security Guideline for managing unauthorized remote access, including the practice of limiting station-to-station communications except for certain rare circumstances.

Risk Monitoring

- Continuous monitoring of E-ISAC physical access attempt reports to assets containing low impact BES Cyber Systems to determine if the risk increases over time and should be addressed.

Introduction

In 2017, NERC developed new and revised CIP Reliability Standards to help mitigate cyber security risks associated with the supply chain for high and medium impact BES Cyber Systems. These standards, collectively referred to as Supply Chain Standards, consist of new Reliability Standard CIP-013-1 and revised Reliability Standards CIP-010-3 and CIP-005-6. Consistent with the risk-based framework of the NERC CIP Reliability Standards, the Supply Chain Standards are applicable to the highest-risk systems that have the greatest impact to the grid. When adopting the Supply Chain Standards in August 2017, the NERC Board directed NERC to undertake further action on supply chain issues. Among other things, the Board directed NERC to study the nature and complexity of cyber security supply chain risks, including those associated with low impact assets not currently subject to the Supply Chain Standards and develop recommendations for follow-up actions that will best address identified risks. To understand these risks better, NERC collected data from registered entities pursuant to a request for data or information under Section 1600 of the NERC Rules of Procedure.

NERC staff's analysis of the data collected[1] showed that, while an individual compromise to any one low impact BES Cyber Asset facility would generally be a localized event, a coordinated cyber attack with control of multiple facilities could result in an event that has an interconnection-wide BES reliability impact. The vast majority of transmission station and substation low impact BES Cyber Assets are at locations that have at most only one line greater than 300 kV or two lines greater than 200 kV (but less than 300 kV). Similarly, the vast majority of generation resource low impact BES Cyber Assets are at facilities that have less than 500 MW. In other words, an individual compromise to any one of these facilities (transmission substations or generation resources) would generally be a localized event. However, a coordinated cyber attack with control of multiple facilities could result in an event that has an interconnection-wide BES reliability impact.

Based on the analysis of the data request, NERC staff recommended to the NERC Board at its February 6, 2020 meeting that Reliability Standard CIP-003-8 be modified to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary. The NERC Board approved a resolution at this meeting endorsing this action.

On May 14, 2020, the NERC Board of Trustees (Board) adopted proposed Reliability Standard CIP-002-6. The proposed Reliability Standard CIP-002-6 addressed the recommendation from the Version 5 Transition Advisory Group to clarify the phrase "used to perform the functional obligations of the Transmission Operator (TOP)" in CIP-002-5.1a, Attachment 1, Criterion 2.12.

Specifically, the proposed Reliability Standard CIP-002-6 addressed the applicability of requirements to a Control Center owned by a Transmission Owner (TO) that performs the functional obligations of a TOP. The proposed criterion established an average MVA line loading based on voltage class for BES Transmission Lines operated between 100 and 499 kV. The aggregate weighted value of the BES Transmission Lines must exceed 6,000 to meet the minimum threshold established in Criterion 2.12. In meeting that threshold, associated BES Cyber Systems would be categorized as medium; those Control Centers that did not meet the threshold would have low impact BES Cyber Systems (if not already identified as high).

On December 13, 2020, FireEye Inc., a cybersecurity solutions and forensics firm, publicly posted details about an attack on the Orion platform developed by SolarWinds. For victims, this attack was particularly damaging because in order to function the SolarWinds Orion platform must have broad and privileged access to the networks it manages, including both the corporate and operational networks of an entity. The breach provided the opportunity for an adversary to monitor network traffic and compromise systems, which could result in disruption of operations.

[1] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Supply%20Chain%20Risk%20Assesment%20Report.pdf

Underscoring the severity of the event, on December 13, 2020, the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), issued Emergency Directive 21-01 This Directive required Federal agencies to take action based on the DHS assessment that a successful compromise from the SolarWinds Orion platform attack would have "grave" consequences. On December 15, 2020, the White House National Security Council (NSC) established a Cyber Unified Coordination Group (UCG) composed of multiple Federal agencies to coordinate the investigation and remediation of the "significant" cyber incident. On December 17, 2020, CISA issued Alert AA20-352A, directed toward the private sector, which described the attack for industry, the affected products, and the mitigation recommendations.

In response, the Federal Energy Regulatory Commission (FERC) staff and the NERC Electricity Information and Analysis Sharing Center (EISAC) jointly prepared a white paper[2], emphasizing the need for continued vigilance by the electricity industry related to supply chain compromises and incidents and recommends specific cybersecurity mitigation actions to better ensure the security of the bulk-power system (BPS). While focusing primarily on the ongoing cyber event related to the attack on the Orion platform developed by SolarWinds and related Microsoft's 365/Azure Cloud compromise, it also addresses related compromises in products such as Pulse Connect Secure. Two additional examples of compromises, Microsoft's on-premise Exchange servers, and F5's BIG-IP are discussed to illustrate continued adversary interest and exploitation of ubiquitous software systems.

Because of the wide use of the SolarWinds Orion platform and the adversarial tactics used, even entities that did not install the SolarWinds Orion platform on their networks could still be impacted. For example, the indicators of compromise (IOCs) have been found on networks without the SolarWinds Orion platform. In addition, although the SolarWinds Orion platform may not have been used by entities, their key suppliers may use the product. Should the suppliers be compromised, the supplier in turn could compromise their customers, including those without the SolarWinds Orion platform. In fact, there is evidence technology firms were targeted for this reason.

In light of these recent cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to withdraw CIP-002-6. In doing so, they approved a resolution to withdraw CIP-002-6 and directed NERC Staff, working with stakeholders, recognizing the complexity of the undertaking, to expeditiously complete its broader review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and report on whether those criteria should be modified.

[2] https://www.nerc.com/pa/CI/ESISAC/Documents/SolarWinds and Related Supply Chain Compromise White Paper.pdf

Chapter 1: BES Cyber Systems and Impact Ratings

This chapter provides an overview of the identification and categorization of relevant cyber systems within the North American Bulk Electric System. It describes the history and the current state of this process within the NERC CIP standards and the rationale for the current state, including specific discussion on the low impact category within the NERC CIP standards and the protections required today for the low impact BES Cyber Systems.

BES Cyber System Identification & Impact Categorization

In the NERC CIP standards (specifically CIP-002) from Version 1 to Version 3, entities were required to have their own risk assessment methodology that identified Critical Assets and their supporting Critical Cyber Assets. As is the term 'critical', this categorization was binary in nature; cyber assets were either critical and fully in-scope or non-critical and thus fully out of scope of the standards and their cyber security requirements. Subsequent to FERC Order 706, the CIP standards underwent a large transition leading up to Version 5 that consisted of two foundational changes:

- A transition to a single set of risk-based criteria for all entities to use to identify and categorize their cyber systems that could impact the Bulk Electric System (defined as BES Cyber Systems that consist of BES Cyber Assets , a subset of Cyber Assets)
- The concept that **every** BES Cyber System requires a base level of cyber security protection.

With this transition, the scope of cyber assets under the NERC CIP standards exploded from a smaller number of Critical Cyber Assets to literally millions of BES Cyber Assets across all entities in the North American BES. With a core defining characteristic of "if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment…", the scope of cyber assets covered by the CIP standards increased exponentially.

With this large increase in scope for Version 5, the CIP-002 standard borrowed a concept from the NIST Risk Management Framework and transitioned to a graduated and risk-based approach with the introduction of graduated impact categories: High, Medium, and Low impact. These categories were created in recognition of the fact that every BES Cyber System does not present the same level of risk to the BES. Within the Version 5 CIP-002 standard, Attachment 1 was created that presented a set of defined criteria by which all BES Cyber Systems are categorized into the high, medium, or low impact categories (Appendix C contains the complete impact rating criteria from CIP-002-5.1a). At a very high level, these risk-based impact categories consist of:

- **High impact** – BES Cyber Systems associated with Control Centers that have a large span of control of BES assets
- **Medium impact** – BES Cyber Systems associated with:
  - Larger field assets, such as the more impactful generation resources and Transmission substations that contain 500kV or above 'backbone' Transmission lines or larger 'hub' sites for many Transmission lines
  - Control Centers with a smaller span of control of BES assets
- **Low impact** – Every other BES Cyber System in the Bulk Electric System associated with all other BES Control Centers, transmission resources, and generation resources.

The CIP-002 standard also assigns these impact ratings not to the BES assets themselves (Control Centers, transmission resources, generation resources, etc.) but only to BES Cyber Systems. This recognizes that not every BES Cyber System in an asset is of the same risk or potential impact and a BES Cyber System should be protected at a level commensurate with the risk presented by that cyber system, not simply inherited from the asset it supports. For example, a Transmission substation may have many digital relays within its boundary. Some may be protecting and controlling 500kV major backbone Transmission lines and be of medium impact to the BES, others may be protecting

and controlling a single 100kV line and are of low impact to the BES. The lower impact relay does not inherit a higher impact rating simply due to its proximity to a higher impact BES Cyber System. Within a generation resource, a BES Cyber System that can trip 1500MW or more of generation is a medium impact system, but a system controlling an individual 20MW generator, although it may be located at the same plant site, would be low impact. Therefore, the CIP-002 standard requires the evaluation of BES Cyber Systems with rating criteria and then categorizes each one according to that cyber system's potential impact to the BES. Those that do not fall into the high or medium impact categories default to the low impact category, with the result being that every BES Cyber System receives cyber security protections in a risk-based manner.

This generation example shows how the CIP-002 impact rating criteria alone can incentivize beneficial security changes in the Bulk Electric System. A primary example is Criterion 2.1 from CIP-002 Attachment 1 that requires any "shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection" to be categorized as medium impact. This criterion was established to recognize the elevated risk of a BES Cyber System at a generation resource that could impact enough generation to challenge the average Contingency Reserve that Balancing Authorities are required to maintain per the NERC BAL-002 Disturbance Control standard. This criterion caused entities to evaluate the architectures of their BES Cyber Systems and networks within their generating plants to determine their potential impact. For example, a generating plant with two 800MW units with control system(s) on a single, flat control network or that controlled critical processes on both units could mean that an issue on that BES Cyber System may impact both units, turning a potential 800MW impact into a 1600MW impact. The sudden loss of 1600MW would be greater than the 1500MW threshold representing an average Balancing Authority's Contingency Reserve and rise to a medium impact to the BES. Therefore, due to this criterion in CIP-002, entities across the BES analyzed their architectures and many, upon discovering any such systems, decided to not simply accept that higher level of risk and impact, but to implement projects to rearchitect and segment systems and networks to reduce the potential impact and risk. This criterion resulted in entities taking action to reduce the attack surface and limit the scope of impact of BES Cyber Systems through cyber security practices of good network and system segmentation as the CIP-002 analysis highlighted a higher than necessary risk in their environment.

Low Impact BES Cyber Systems

In recognition of the vast scope of BES Cyber Systems across the North American Bulk Electric System, the CIP standards treat the impact categories differently and in particular the individual cyber assets that make up the low impact BES Cyber Systems. Those BES Cyber Systems with a high or medium impact are treated individually and for some requirements (e.g., security patching) at an individual BES Cyber Asset level. However, identifying and protecting every individual low impact BES Cyber Asset at every BES asset would, due to its scale, dilute focus, and resources away from the higher impact systems. The reason the CIP standards have an "all-in" nature is so that every BES Cyber Asset receives a base level of protection, but those BES Cyber Systems that present a much greater level of risk due to their span of control or impact to the BES are identified and protected.

Therefore, the CIP standards treat the low impact BES Cyber Systems at the level of an "asset containing low impact BES Cyber Systems." This allows for all the low impact BES Cyber Systems to have cyber security requirements applied to them, but at a manageable level grouped by the asset or site. For example, cyber security protections for electronic access to any BES Cyber System can be applied at a site level and thus inherited for all the individual BES Cyber Systems within the site. This is a manageable way to provide base level protections against every BES Cyber System in the Bulk Electric System while focusing efforts on the higher risk, higher level targets of those systems with larger span of control and a much higher level of impact if compromised. As the saying goes, "a focus on everything is a focus on nothing," and CIP-002 incorporates that philosophy.

Low Impact BES Cyber System Cyber Security Requirements

With the philosophy of protecting the myriad individual and lower-risk BES Cyber Systems at a site or asset level, the CIP standards (in this case CIP-003 for low impact BES Cyber Systems) requires both cyber security policies and detailed cyber security plans that cover every low impact BES Cyber System at a BES asset level.

With the incredible scale and diversity of low impact BES Cyber Assets across Control Centers, substations, and generation resources of all types, the idea of having a base cyber security plan with required sections to mitigate high level risk areas rather than prescriptive device-level requirements is a manageable way for all entities to document how they meet the cyber security objectives for the assets containing low impact BES Cyber Systems.

The required cyber security plans that provide a base level of protection for every BES Cyber System must include (as of the date of this paper) sections concerning five areas of risk that cover the main areas of people, process, and technology. These five areas and the rationale behind each are:

- **Cyber Security Awareness** – A core part of cyber security is the people aspect; those who use or maintain such systems and their actions. The cyber security plans, therefore, require a cyber security awareness program that reinforces good security practices.
- **Physical Security Controls** – Another core part of cyber security is protecting physical access to the cyber systems. As has been said, physical access control to a cyber system is vital as many electronic security controls can be overridden if an attacker gains physical access to the system. Therefore, the CIP standards have required that physical access be controlled based on need either (or both) at an asset level or to locations of low impact BES Cyber Systems within the asset, as well as specifically to any cyber assets that control electronic access to the asset (e.g., firewalls protecting external access to the BES Cyber Systems).
- **Electronic Access Control**s – One of the primary risks facing low impact BES Cyber Systems (or any BES Cyber System) is electronic remote access from outside of the asset containing the systems. With the rise of Internet search engines devoted to finding publicly-accessible industrial equipment and control systems, the CIP standards incorporated this section to require the implementation of electronic access controls that permit only needed inbound and outbound routable protocol electronic access to the asset containing lows (and thus all individual low impact systems) from anything outside of the asset; in other words, all remote access must be controlled and limited to only what is necessary. In like manner, any dial-up connectivity must also authenticate the remote client and not provide unauthenticated access to anyone with the correct phone number. With this covering every BES Cyber System in the North American BES, this requirement for electronic access controls has reduced an enormous amount of risk.
- **Cyber Security Incident Response** – While other sections of the entity's cyber security plan have been in the realm of prevent, this section of the plan deals with the "detect, respond, and recover" aspects of cyber security. This requires that every entity with a low impact BES Cyber System have an incident response plan that covers six areas of incident response, including identification, response, reporting, roles and responsibilities, handling, testing, and updating of those plans.
- **Transient Cyber Assets and Removable Media** – One final 'front door' through which malware or other exploits can enter an asset and impact BES Cyber Systems is through the devices that authorized users bring in and directly connect that thus bypass the electronic remote access controls. This required fifth section of the cyber security plan revolves around mitigating the risk of malicious code on devices that 'walk in' and directly connect and covers Transient Cyber Assets such as laptops used for configuration, troubleshooting, maintenance, etc., as well as removable media such as USB thumb drives. This section has the stated security objective of mitigating the risk of the introduction of malicious code from such devices and requires various methods of detecting and mitigating the malicious code threat before connecting to any low impact BES Cyber System.

The NERC CIP standard then covers every low impact BES Cyber System in the North American BES with these requirements that cover people, processes, and technology and require controls at the 'front doors' through which most threats exploit vulnerabilities – electronic remote access to the site, unauthorized physical access to the site, or through devices carried into the site by authorized users.

In addition to having cyber security plans, each entity must also have corresponding cyber security policies that incorporate these areas.

One further area where the CIP standards apply to low impact BES Cyber Systems is for those that reside in a Control Center. In such cases, the CIP-012 standard applies protections to the real time monitoring and assessment data as it is being transmitted between that Control Center and all other Control Centers.

Chapter 2: Current Risk to Low Impact Systems

Risks to BES Cyber Systems are not static because the threats are not static. One of the unique aspects of cyber security risks to BES equipment over others such as weather, environmental, mechanical, or electrical is it is a risk from motivated, intelligent, and adaptable human adversaries. Over time cyber threats have gone from defacing Internet-accessible websites, to exploiting firewall rules, to 'hacking the humans' through phishing, to ransomware, to sophisticated supply chain attacks. As the defenses have adapted to the attacks, the attacker's techniques change as well. Unlike many other risks, cyber security risks are subject to constant adaptation by the adversary.

Risk of Coordinated Attacks

The CIP-002 standards categorize most individual BES Cyber Systems within the BES as low impact. This is reasonable on what has been called the 'largest machine in the world' that stretches across the North American continent and is designed, built, and operated to withstand the loss of portions of itself including any single asset. For example, weather events often cause unavailability of individual substations, lines, and generating units yet the BES remains stable. Having the majority of the individual BES Cyber Systems categorized as low impact is therefore reasonable, given that the assets they support are also of low impact individually. If a line can trip from a lightning strike or a generating resource trip due to a bearing failure, then a trip from a cyber system cause on that same asset is of the same low impact to the BES.

However, the primary risk presented by low impact BES Cyber Systems is not from each individually, but through using cyber means (network connectivity, remote access, etc.) to aggregate the impact across many individual low impact BES Cyber Systems affecting multiple BES assets. This is the risk of a 'coordinated attack', defined for the purposes of this report as:

> *"An orchestrated attack against multiple low impact BES Cyber Systems, independent of Responsible Entity ownership, which has the goal of causing an Adverse Reliability Impact to the BES."*

The ability to simultaneously communicate with many low impact systems across multiple BES assets can allow coordinated attacks whose impact can aggregate to an equivalent medium or high impact to the BES. This aligns with the categorization of high impact BES Cyber Systems that are within larger Control Centers – a centralized system that is a single point with a large 'span of control' from which to perform a coordinated attack across many low or medium impact BES Cyber Systems..

An effective evaluation of risk associated with a distributed and coordinated attack event requires an understanding of the requirements for an attacker to initiate a successful attack. Every successful cyber attack requires motive, method, and opportunity.

- Motive represents the 'what' or the goal an attacker is trying to accomplish. Motive is not always clear, although it is a potential indicator of the most probable risk(s) an organization is likely to face from a cyber attacker. For example, an organization with a strong financial position is more likely to attract attackers with a financial motive. Organizations that understand probable attacker motives are able to effectively prioritize those cybersecurity controls that defend against related attack methods.
- Method represents 'how' the attacker accomplishes their motive and is representative of the ability, complexity, and effectiveness of an attacker.
- Opportunity represents the potential weaknesses in an organization's cybersecurity that an attacker may leverage to achieve their goal.

With these in mind, the LICRT identified several different attack methods that could be used individually or in combination to initiate a coordinated attack against low impact BES Cyber Systems at multiple locations. These attack methods were then ranked based on a compilation of:

- Ease of execution,
- Potential impact to operations, and
- Probability.

The highest ranked category of coordinated attack methods consists of:

- **Unauthorized Remote Access** – Management access by an unauthorized party for malicious intent initiated from an external system, using any communication means available, including compromise of known or unknown access methods, insecure configurations, or system vulnerabilities. This method could be used by an attacker using compromised credentials or a compromised cyber system to access and modify many low impact BES Cyber Systems across several BES assets to implement a coordinated attack.
- **Malicious Software** – Software that enables unauthorized malicious behavior on a target system, such as spyware, ransomware, logic bombs, worms, trojans, keyloggers, etc. Malicious software on one low impact BES Cyber System does not constitute a coordinated attack, however malicious software that can use connectivity to spread to cyber systems in other BES assets and cause wider impact (e.g., ransomware) is the concern from a coordinated attack perspective.

The medium category methods are:

- **Supply Chain Common Service Attack** – Compromise of a service organization that has business relationships with multiple partner organizations to enable the malicious actor to gather sensitive data, initiate unauthorized remote access, deliver malicious code, or initiate any other attack against partner organizations. Examples include, but are not limited to, vendors, Managed (Security) Service Providers (MSP, MSSP), ISO/RTO type communications (ICCP), etc. This method could be used for a coordinated attack if the attacker was able to infiltrate an outside service that has connectivity or control of multiple low impact BES Cyber Systems, not only across multiple BES assets, but especially across multiple entities.
- **Supply Chain Product Compromise** – An attack against one or more suppliers that provide products and/or services in order to initiate a malicious campaign against one or more target organizations. This differs from a common service attack method (that originates externally from a provider) as this is a common product or service installed internally within multiple BES assets or entities. This method could be used for a coordinated attack if the attacker compromised the software/firmware processes of a vendor and embedded malicious code that is then installed in low impact BES Cyber Systems across multiple BES assets or multiple entities.
- **Unauthorized Internal Access by a Single Actor** - Physical access by an unauthorized party or by a party abusing their existing access for malicious intent initiated from an internal system, thus bypassing any network perimeter remote access controls. The attacker then uses any communication means available to launch a coordinated attack by compromising or operating other systems at multiple locations.

The lower category methods are:

- **Denial of Service** – A remote attack that interrupts normal operation, typically by saturating communications (shared or otherwise), interrupting system process capabilities, or initiating a system failure. This could be used as a method of coordinated attack mostly for BES assets that are dependent upon Internet connectivity, typically using Virtual Private Networks (VPN) over a connection to the public Internet. If multiple assets containing low impact BES Cyber Systems are connected to the public Internet, an attacker could direct a large network of compromised machines (i.e., a 'botnet') to flood many assets with traffic simultaneously.

- **Data Manipulation** – Malicious modification of data, typically at the application protocol level, to hide, mislead, or initiate unauthorized changes to target systems. This could be used as a method of coordinated attack if the attacker has access to the network connecting many BES assets containing low impact BES Cyber Systems and operational traffic is not encrypted or otherwise protected from tampering. Spoofing network addresses of valid systems and issuing commands or intercepting and changing data within unencrypted sessions could be used to aggregate impact across multiple sites.
- **Unauthorized Internal Access by Multiple Actors** - Simultaneous physical access at multiple sites by unauthorized parties or by multiple parties abusing their existing access for malicious intent. This attack method requires multiple individuals at multiple locations working in a coordinated fashion towards a single purpose.

Chapter 3: Existing CIP Standards Gap Evaluation

Several risks associated with Low Impact BES Cyber Systems are addressed by the existing CIP standards as described in **Chapter 1** titled "Low Impact BES Cyber System Cyber Security Requirements". In **Chapter 2**, the LICRT analyzed and documented the main coordinated attack methods that could be used by an attacker. This chapter evaluates each of those coordinated attack methods against the existing CIP-003 and CIP-012 standard requirements for assets containing low impact BES Cyber Systems and considers any in-process NERC standards efforts. It then analyzes any remaining gaps that may present opportunities for an attacker to use that method to perform a coordinated attack.

Unauthorized Remote Access

Unauthorized remote access is one of the highest risk coordinated attack methods. As increasing numbers of low impact BES Cyber Systems gain increased remote access capabilities, the threat of unauthorized use of this access grows.

Current CIP Standards Low Impact Requirements

- CIP-003 Electronic Access Controls that permit only necessary inbound and outbound communications to an asset containing low impact BES Cyber Systems, reducing the available remote attack surface.

Current NERC Efforts

- Project 2020-03 – Supply Chain Low Impact Revisions (Modifications to CIP-003-8)
  - By identifying, monitoring, and controlling vendor remote access sessions, the risk of unauthorized remote access is reduced. Also, by detecting malicious communications, insecure configurations and system vulnerabilities are likely to be identified.

Gap Analysis

- No requirement to authenticate users before they are granted access to networks containing low impact BES Cyber Systems, enabling lateral movement to occur between many lows. No authentication is required for remote access using routable protocols, which could result in a compromise that allows easy connection to multiple locations. Without authentication, entities cannot ensure that the sessions within the permitted communication paths are authorized.
- No requirements for strong (multi-factor) authentication of remote access users, allowing use of weak or single factor credentials. Compromised single-factor (ID/Password) credentials could be used by attackers to access multiple lows.
- Suspected suspicious or malicious communications may not be detected and monitored for necessary electronic communications through an otherwise permitted path (see CIP-003 Attachment 1 Section 3). Project 2020-03 will require this only for vendor communications, which will exclude all other non-vendor communications.

Malicious Software

Malicious software that may find an entry point on one low impact BES Cyber System may be able to spread and impact many like systems across multiple BES assets and be used to conduct a coordinated attack. This is another high-risk area due to the increased network connectivity.

Current CIP Standards Low Impact Requirements

- CIP-003 Electronic Access Controls that permit only necessary inbound and outbound communications to an asset containing low impact BES Cyber Systems, which prevent any unnecessary traffic between BES asset sites.
- CIP-003 Transient Cyber Asset and Removable Media requirements that require mitigating the risks of introduction of malicious software to low impact BES Cyber Systems from physically present Cyber Assets and media that connect to low impact BES Cyber Systems.

Current NERC Efforts

- Project 2020-03 – Supply Chain Low Impact Revisions (Modifications to CIP-003-8)
  - Addition of detecting malicious vendor remote access communications by which malware, spyware, ransomware, etc. would be more likely to be identified as it attempts to spread to other BES assets.

Gap Analysis

- Suspected suspicious or malicious communications may not be detected and monitored for necessary electronic communications through an otherwise permitted path (see CIP-003 Attachment 1 Section 3). No active monitoring for malware is required for assets that allow remote connections. Project 2020-03 will require this only for vendor communications, which will exclude all other communications.

Supply Chain Common Service Attack

Common external services with access to low impact BES Cyber Systems at multiple assets within an entity, or especially across multiple entities, are an avenue of coordinated attack.

Current CIP Standards Low Impact Requirements

- CIP-003 Electronic Access Controls that permit only necessary inbound and outbound communications to an asset containing low impact BES Cyber Systems. This reduces the attack surface available to the external service to only what is necessary.
- CIP-012-1 - Cyber Security – Communications between Control Centers (effective 7/1/2022) requires implementing methods to protect confidentiality and integrity of Real-Time Assessment and Real-Time monitoring data while being transmitted between Control Centers. This mitigates the risk of any unauthorized entity or threat actor with access to these external networks to intercept or manipulate this data.

Current NERC Efforts

- Project 2020-03 – Supply Chain Low Impact Revisions (Modifications to CIP-003-8)
  - By identifying, monitoring, and controlling vendor remote access sessions, the risk of unauthorized remote access is greatly reduced. Also, by detecting malicious communications, insecure configurations and system vulnerabilities are likely to be identified.

Gap Analysis

- No requirement to authenticate remote users before they are granted access to networks containing low impact BES Cyber Systems, enabling lateral movement to occur between many lows.

- No requirements for strong (multi-factor) authentication of remote access users, allowing use of weak or single factor credentials. Compromised single-factor (ID/Password) credentials could be used by attackers to access multiple lows.
- Protection of communications across publicly accessible networks only required if between Control Centers.
- Detection of suspicious or malicious electronic communications not required. Project 2020-03 will require this only for vendor communications, which will exclude all other communications.
- Communications to and from an asset containing low impact BES Cyber Systems are not restricted from using publicly accessible networks (e.g., the Internet). Remote systems that are allowed through current electronic access controls could be spoofed if not protected on publicly accessible networks.

Supply Chain Product Compromise

A common product or service that is installed internally within a BES asset or across multiple assets or entities could be used for a coordinated attack if the attacker compromised the software/firmware processes of a vendor and embedded malicious code that begins to compromise other systems across multiple BES assets.

Current CIP Standards Low Impact Requirements

- CIP-003 Electronic Access Controls that permit only necessary inbound and outbound communications to an asset containing low impact BES Cyber Systems, which prevent any unnecessary traffic between BES asset sites.
- CIP-012-1 - Cyber Security – Communications between Control Centers (effective 7/1/2022) requires implementing methods to protect confidentiality and integrity of Real-Time Assessment and Real-Time monitoring data while being transmitted between Control Centers. This mitigates the risk of any unauthorized entity or threat actor with access to these external networks to intercept or manipulate this data.

Current NERC Efforts

- Project 2020-03 – Supply Chain Low Impact Revisions (Modifications to CIP-003-8)
  - Known malicious traffic associated with a supply chain compromise should be identified by implementation of the CIP-003-8 controls. Vendor remote access detections may also inhibit exploitation of supply chain compromise.

Gap Analysis

- No evaluation and mitigation of risks for procurement (i.e., CIP-013 and CIP-010). Not having an evaluation and mitigation of risks for procurement places dependency on controls that rely on detection after a compromise. For example, a product (or multiple products) that has a common dependency (e.g., shared DLL, shared common code) installed in multiple locations.

Unauthorized Internal Access by a Single Actor

Physical access by an unauthorized party or by a party abusing their existing access for malicious intent could initiate a coordinated attack by compromising or operating other systems at multiple locations from their internal location.

Current CIP Standards Low Impact Requirements

- CIP-003 Electronic Access Controls that permit only necessary inbound and outbound communications to an asset containing low impact BES Cyber Systems, which prevent any unnecessary traffic between BES asset

sites. The attacker would need to work within what is allowed outbound at their location and inbound at other locations.

- CIP-003 Physical Access Controls that require physical access be controlled based on need either (or both) at an asset level or to locations of low impact BES Cyber Systems within the asset, as well as specifically to any cyber assets that control electronic access to the asset (e.g., firewalls protecting external access to the BES Cyber Systems).

Current NERC Efforts

- None

Gap Analysis

- Detection and prevention of unauthorized physical access of an individual to initiate an attack against BES Cyber Asset(s) at multiple locations simultaneously from an internal system. By not addressing local physical access, unauthorized use of trusted electronic communication to BES Cyber Asset(s) at multiple locations may not be detected, logged, monitored, or controlled.

Denial of Service Attack

Common network connectivity on a publicly accessible network such as the Internet could be used by an attacker to conduct (Distributed) Denial of Service (DDoS/DoS) coordinated attacks against multiple BES assets containing low impact BES Cyber Systems, either causing boundary devices such as FWs to temporarily fail or cause time-sensitive communications to fail.

Current CIP Standards Low Impact Requirements

- None

Current NERC Efforts

- Project 2020-04 Modifications to CIP-012
  - By implementing protections to ensure the availability of real-time data between Control Centers (all impact levels), such as alternate communication paths, the risk of a denial-of-service attack preventing transmission of real-time data between Control Centers is mitigated or eliminated.

Gap Analysis

- CIP-012 and its protections only apply to Control Centers of all impact levels. It is not known how many other types of BES assets such as substations or generation resources are exposed directly to public networks and thus subject to a DDoS attack from large numbers of compromised Internet devices that could affect enough lows simultaneously to cause an Adverse Reliability Impact.

Data Manipulation

An attacker with access to common network connectivity, particularly on a publicly accessible network such as the Internet, could modify data or issue commands in a coordinated attack against multiple BES assets containing low impact BES Cyber Systems.

Current CIP Standards Low Impact Requirements

- CIP-003 Electronic Access Controls that permit only necessary inbound and outbound communications to an asset containing low impact BES Cyber Systems.

- CIP-012-1 - Cyber Security – Communications between Control Centers (effective 7/1/2022) requires implementing methods to protect confidentiality and integrity of Real-Time Assessment and Real-Time monitoring data while being transmitted between Control Centers. This mitigates the risk of any unauthorized entity or threat actor with access to these external networks to intercept or manipulate this data. By encrypting communications or deploying non-repudiation-based technologies of data between Control Centers, the risk of unauthorized data manipulation is mitigated or eliminated.

Current NERC Efforts

- None

Gap Analysis

- No protection of data in motion, other than that covered by CIP-012-1 between Control Centers.
- Modification of data or commands between BES Cyber Assets at multiple locations could initiate unauthorized control, could compromise situational awareness, and could lead to inadvertent system operator actions.
- Data between Control Centers and substations or generation resources on publicly accessible networks does not require protection of its confidentiality or integrity (i.e., encryption, VPN).
- The electronic access controls in CIP-003 are typically a source/destination address pair that could be spoofed if the communications are not within a defined Virtual Private Network (VPN) required between the source and destination points.

Unauthorized Internal Access by multiple actors

Simultaneous physical access by multiple unauthorized parties at multiple locations could initiate a coordinated attack by compromising or operating systems at multiple locations from their internal locations.

Current CIP Standards Low Impact Requirements

- CIP-003 Physical Access Controls that require physical access be controlled based on need either (or both) at an asset level or to locations of low impact BES Cyber Systems within the asset, as well as specifically to any cyber assets that control electronic access to the asset (e.g., firewalls protecting external access to the BES Cyber Systems).

Current NERC Efforts

- None

Gap Analysis

- Detection and prevention of unauthorized physical access of multiple individuals to initiate a coordinated attack against BES Cyber Asset(s) at multiple locations simultaneously. By not addressing local physical access, unauthorized use by multiple individuals of trusted electronic communication to BES Cyber Asset(s) at multiple locations may not be detected, logged, monitored, or controlled.

Chapter 4: Overall Analysis and Recommendations

In the previous chapter, each of the coordinated attack methods were analyzed for potential gaps in required protection within the CIP standards (accounting for current requirements and drafting efforts already underway). In reviewing each of those identified gaps across all the coordinated attack methods, they fall into five distinct control gaps:

- Lack of authentication of remote users
- Lack of protection of communications to and between low impact BCS across publicly accessible networks
- Lack of detection of malicious communications to/between assets containing low impact BES Cyber Systems
- Undetected unauthorized physical access to lows
- Lack of procurement risk evaluation for lows

Each of these control gaps was analyzed to see where each appeared across all the attack methods as well as the team's recommended risk mitigation priority of each one. The attack method rating from **Chapter 2** is included in the table for reference.

Table 4.1: Attack Methods

Control Gap	Attack Method	Risk Mitigation Priority
Lack of authentication of remote users	Unauthorized Remote Access (High) Supply Chain Common Service Attack (Medium)	High
Rationale: The review identified potential high impact to the BES due to the absence of remote authentication controls. User authentication can mitigate coordinated attack methods via electronic means including some supply chain vendor access gaps, launching electronic attacks after unauthorized physical access, etc. Additionally, the cost to implement could be low, and the ease of compromise is high.		
Lack of protection of communications to and between low impact BCSs across publicly accessible networks	Supply Chain Common Service Attack (Medium) Denial of Service Attack (Low) Data Manipulation (Low)	Medium
Rationale: Theme of risks that may result in the ability to enable address spoofing, man in the middle, and denial of service attacks. High degree of risk mitigation potential for BES sites on the Internet with only firewall protection but no protection of operational traffic on the public network. However, the population of such sites is unknown so the overall risk to BES reliability is unknown.		
Lack of detection of malicious communications to/between assets containing low impact BES Cyber Systems	Unauthorized Remote Access (High) Malicious Software (High) Supply Chain Common Service Attack (Medium) Unauthorized Internal Access by Single Actor (Medium)	High

Table 4.1: Attack Methods		
Control Gap	**Attack Method**	**Risk Mitigation Priority**
Rationale: Risk mitigation depends primarily on type of access and the protocols used to/between sites. If the access is only a single industrial protocol polling an RTU, there is a lower degree of mitigation possible. If access is granted to remotely manage BCS configuration at the site, there is a much higher degree of risk mitigation possible, so this is site and mode dependent.		
Undetected unauthorized physical access to lows	Unauthorized Internal Access by Single Actor (Medium) Unauthorized Internal Access by Multiple Actors (Low)	Low
Rationale: High cost with low probability/likelihood. This is more of a 'launch point' threat from an electronic perspective, i.e., physical access to one remote site should not equate to electronic access to many other sites. This is more effectively mitigated with network security controls such as authentication above.		
Lack of procurement risk evaluation for lows	Supply Chain Product Compromise (Medium)	Medium
Rationale: High cost for all lows. Should evaluate the effectiveness of risk mitigation for procurement of high and medium impact systems prior to expanding scope. Does not detect/prevent the spread of malware or the delivery of commands to perform a coordinated attack.		

In making recommendations for mitigating risks from these gap themes, the LICRT determined three categories of recommendations:

- **CIP Standards Revisions** – recommendations for a Standards Authorization Request (SAR) to address identified gaps with CIP Standard modifications.
- **Security Guidelines** – recommendations that NERC Security Guideline documents be developed to assist entities in identifying and mitigating identified gaps.
- **Risk Monitoring** – recommendations that call for NERC to monitor and/or gather more information to further gauge the risk from identified gaps.

For any recommendations in the *CIP Standards Revisions* category, there are various 'knobs' that can be turned within the standards themselves to tailor the requirements and their scope to the appropriate BES Cyber Systems:

- **Impact Rating Criteria** – The first is to modify the impact rating criteria in CIP-002, Attachment 1 to modify the impact rating BES Cyber Systems must receive based on an identifiable attribute of such systems. This is typically used for 'broad brush' scope changes, affecting an entire category of BES Cyber Systems. If an identifiable category of BES Cyber Systems is recognized as having a different impact level to the BES, the criteria can be modified accordingly to raise or lower the rating they receive in CIP-002.
- **Scope Modifiers**: Secondly, certain cyber security requirements often use scope modifiers to tailor applicability to subsets of an impact category with differing risk attributes. The most common is 'with External Routable Connectivity (ERC)'. A BES Cyber System may be categorized as a medium impact but have an elevated risk if it has ERC and is remotely accessible. Several such modifiers exist, such as: "at Control Centers", "with vendor remote access," and "with Dial-up Connectivity".

- **Requirements:** Lastly, new or modified requirements can be created for the existing impact categories. This allows for the situation when a broad reclassification of impact levels is not necessary, but additional requirements are needed for an existing impact category.

Recommendations

After the analysis documented in this report, the LICRT arrived at the following overall conclusions regarding low impact BES Cyber Systems:

- Low impact BES Cyber Systems are truly low impact to BES reliability *individually* which corresponds to the longstanding work of NERC and the stakeholders to design and operate the BES to withstand the loss of any of its individual parts. A medium or high impact to the BES is more than an impact to a typical single BES Element/Facility. Therefore, the team does not recommend changing the *impact criteria* in CIP-002 for identifying and categorizing *individual* BES Cyber Systems at this time.
- *However*, there are risks to BES reliability from lows that could rise to medium or higher impact through aggregation of impact from a coordinated attack against many distributed low impact BES Cyber Systems. The team does see a need for additional recommendations on the existing low impact category to further mitigate the risk of coordinated attacks.

Those recommendations, sorted by category, are as follows:

CIP Standards Revisions

- Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity.

Security Guidelines

- Develop Security Guideline for protection of communications to and between assets containing low impact BES Cyber Systems across publicly accessible networks.
- Develop Security Guideline for procurement risk evaluation for low impact BES Cyber Systems.
- Develop Security Guideline for entities to voluntarily submit an E-ISAC report for unauthorized physical access attempts to assets containing low impact BES Cyber Systems.
- Develop Security Guideline for managing unauthorized remote access, including the practice of limiting station-to-station communications except for certain rare circumstances.

Risk Monitoring

- Continuous monitoring of E-ISAC physical access attempt reports to assets containing low impact BES Cyber Systems to determine if the risk increases over time and should be addressed.

Appendix A: Low Impact Criteria Review Project and Team

Project Scope: Work with NERC staff to expeditiously complete its broader review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact BES Cyber Systems and report on whether those criteria should be modified. Included is an analysis of risk to the BES from a coordinated attack involving low impact BES Cyber Systems.

Team Formation: Assemble a team of cybersecurity experts and compliance experts that represent a cross section of the industry to fairly represent the understanding of the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems.

The following are the members of the Low Impact Criteria Review Team that produced this report:

- NERC: Howard Gugel (Executive Sponsor), Lonnie Ratliff, Ryan Quint
- APPA: Carter Manucy
- CEA: Cameron Fisher, Henry Bosch
- EEI: Thad Ness, Jay Cribb
- FERC: Kal Ayoub, Michael Keane
- ISO/RTO Council: Tim Beach, Derek Drayer
- LPPC: Adam Gormley
- NRECA: Alice Ireland, Richard (Richie) Field

Appendix B: NERC Board Resolution

The NERC Board Resolution from which the Low Impact Criteria Review project and team was created:

> **WHEREAS,** the Board adopted proposed Reliability Standard CIP-002-6 on May 14, 2020, in which a new criterion was proposed to address the applicability of the CIP Reliability Standards to Control Centers owned by Transmission Owners performing the functional obligations of a Transmission Operator;
> **WHEREAS,** recent cybersecurity events and the evolving threat landscape warrant additional caution regarding any criteria that may permit more entities to categorize BES Cyber System as low impact and therefore subject to fewer requirements in the CIP Reliability Standards;
> **NOW, THEREFORE, BE IT RESOLVED**, that the Board hereby withdraws the proposed Reliability Standard CIP-002-6, as presented to the Board at this meeting.
> **FURTHER RESOLVED**, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities, take such further actions, and make such further filings as are necessary and appropriate to effectuate the intent of the foregoing resolution.
> **FURTHER RESOLVED,** that NERC Staff, working with stakeholders, is directed to promptly conduct further study of the need to readdress the applicability of the CIP Reliability Standards to such Control Centers to safeguard reliability, for the purpose of recommending further action to the Board.
> **FURTHER RESOLVED,** that NERC Staff, working with stakeholders, recognizing the complexity of the undertaking, is directed to expeditiously complete its broader review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and report on whether those criteria should be modified.

Appendix C: CIP-002-5.1a BES Cyber System Categorization

This appendix contains 'Attachment 1' from the NERC CIP-002-5.1a standard that contains the complete impact rating criteria for BES Cyber Systems.

CIP-002-5.1a - Attachment 1
Impact Rating Criteria

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

1. High Impact Rating (H)

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

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

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

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

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

2. Medium Impact Rating (M)

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

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

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

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

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

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

Table C.1: Aggregate Weighted Value Exceeding 3000

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

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

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

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

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

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

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

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

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

3. Low Impact Rating (L)

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

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

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

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2023-04 Modifications to CIP-003

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **Project 2023-04 Modifications to CIP-003 Standard Authorization Request (SAR)** by **8 p.m. Eastern, Monday, May 15, 2023.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Chris Larson (via email), or at 470-599-3851.

Background Information

The proposed project will address the issues identified by the Low Impact Criteria Review Team (LICRT) report, which recognized that low impact Bulk Electric System (BES) Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The LICRT recommended enhancing the existing low impact category to further mitigate the coordinated attack risk. More specifically, the proposed project will modify CIP-003-9 to add controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications for assets containing low impact BES Cyber Systems with external routable connectivity.

Questions

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope, please provide your recommendation and explanation.

   ☐ Yes
   ☐ No

   Comments:

2. Provide any additional comments for the SAR drafting team to consider, if desired.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-04 Modifications to CIP-003 Standard Authorization Request

Formal Comment Period Open through May 15, 2023

Now Available

A 45-day formal comment period for the **Project 2023-04 Modifications to CIP-003** Standard Authorization Request (SAR), is open through **8 p.m. Eastern, Monday, May 15, 2023.**

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The SAR drafting team will review all responses received during the comment period and determine the next steps. For more information, refer to the Standard Processes Manual or the project page.

For more information or assistance, contact Senior Standards Developer, Chris Larson (via email) or at 470-599-3851. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2023-04 Modifications to CIP-003 | SAR
Comment Period Start Date:	3/31/2023
Comment Period End Date:	5/15/2023
Associated Ballots:	

There were 37 sets of responses, including comments from approximately 112 different people from approximately 89 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope, please provide your recommendation and explanation.

2. Provide any additional comments for the SAR drafting team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
WEC Energy Group, Inc.	Christine Kane	3,4,5,6		WEC Energy Group	Christine Kane	WEC Energy Group	3	RF
					Matthew Beilfuss	WEC Energy Group, Inc.	4	RF
					Clarice Zellmer	WEC Energy Group, Inc.	5	RF
					David Boeshaar	WEC Energy Group, Inc.	6	RF
Tacoma Public Utilities (Tacoma, WA)	Jennie Wike	1,3,4,5,6	WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Ryan Strom	Buckeye Power, Inc.	5	RF
					kylee Kropp	Sunflower Electric Power Corporation	1	MRO
					Nikki Carson-Marquis	Minnkota Power Cooperative	NA - Not Applicable	MRO

MRO	Jou Yang	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Chris Bills	City of Independence, Power and Light Department	5	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO
					Christopher Bills	City of Independence Power & Light	3,5	MRO
					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern Power Administration	1	MRO
					Matthew Harward	Southwest Power Pool, Inc. (RTO)	2	MRO
					Bryan Sherrow	Board of Public Utilities	1	MRO
					Terry Harbour	Berkshire Hathaway Energy - MidAmerican Energy Co.	1	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Shonda McCain	Omaha Public Power District	6	MRO
					George E Brown	Pattern Operators LP	5	MRO
					George Brown	Acciona Energy USA	5	MRO

					Jaimin Patel	Saskatchewan Power Cooperation	1	MRO
					Kimberly Bentley	Western Area Power Administration	1,6	MRO
					Jay Sethi	Manitoba Hydro	1,3,5,6	MRO
					Michael Ayotte	ITC Holdings	1	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	1,3,4,5,6		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Jim Howell, Jr.	Southern Company - Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC

Alain Mukama	Hydro One Networks, Inc.	1	NPCC
Deidre Altobell	Con Edison	1	NPCC
Jeffrey Streifling	NB Power Corporation	1	NPCC
Michele Tondalo	United Illuminating Co.	1	NPCC
Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
Randy Buswell	Vermont Electric Power Company	1	NPCC
James Grant	NYISO	2	NPCC
John Pearson	ISO New England, Inc.	2	NPCC
Harishkumar Subramani Vijay Kumar	Independent Electricity System Operator	2	NPCC
Randy MacDonald	New Brunswick Power Corporation	2	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
David Burke	Orange and Rockland	3	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC

					David Kwan	Ontario Power Generation	4	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Sean Cavote	PSEG	4	NPCC
					Jason Chandler	Con Edison	5	NPCC
					Tracy MacNicoll	Utility Services	5	NPCC
					Shivaz Chopra	New York Power Authority	6	NPCC
					Vijay Puran	New York State Department of Public Service	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					John Hastings	National Grid	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
					Joshua London	Eversource Energy	1	NPCC
Western Electricity Coordinating Council	Steven Rueckert	10		WECC	Steve Rueckert	WECC	10	WECC
					Phil O'Donnell	WECC	10	WECC

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope, please provide your recommendation and explanation.

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC requests consideration of collapsing the low impact requirements with CIP-005 and CIP-007 instead of continuing to have a separate requirement within CIP-003 for low impact. If the requirements cannot be collapsed into those standards, ATC requests consideration that the defined ESP term does not extend to low impact; and, there is therefore no External Routable Connectivity applicable either. This SAR may need to introduce formally a L-ESP and L-ERC, which would also then possibly include Low-EACMS and Intermediate Systems. ATC also supports EEI and NSRF comments.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6 - WECC, Group Name Tacoma Power

Answer	No
Document Name	

Comment

Tacoma Power does not agree with the proposed scope described in the SAR.

This SAR is proposing more strict controls for low impact BCS with ERC than the controls currently required in CIP-005 for medium impact BCS without ERC. By imposing more strict controls on low impact BCS with ERC, this is upending the CIP-002 categorization. The NERC Standards establish low/medium/high impacts in CIP-002 and fulfill Requirements based on this impact in the other CIP Standards. A low impact BCS should not have more controls than a medium impact BCS. This SAR is placing greater emphasis, and more restrictive controls, on lows with IP connectivity than medium impact BCS without ERC. This begs the question of whether medium BCS without ERC should now be classified as low impact, and lows with IP connectivity should be classified as medium impact. In summary, the amount of controls applied to a type of asset should be dependent on its categorization. Tacoma Power does not agree with creating a precedent for applying greater controls to low impact BCS.

Tacoma Power is also concerned that the scope of this SAR is broad, and as a result, will be difficult to implement. For example, the term “remote access” used in the Detailed Description section is not defined and depending on how an entity defines this term, it will impact the scope of the Requirement(s). The SAR should clarify whether “remote access” is referring to north-south or east-west communication.

Lastly, instead of focusing on asset-level detection, Tacoma Power recommends that the SAR should focus on defining and establishing an Electronic Security Perimeter (ESP) for low impact BCS, and then requiring detection/monitoring of malicious communication at the ESP boundary. This approach is easier to understand and implement than focusing on new Requirements based on asset-level detection. Tacoma Power recommends re-wording the third bullet in the Detailed Description section to the following:

“Requirement(s) for establishing an ESP for low impact BES Cyber Systems with external routable connectivity, and detecting malicious communications at the ESP boundary.” If the SAR drafting team keeps the approach for requiring asset-level detection, then Tacoma Power recommends changing the “to/between” language in the third bullet to “inbound and outbound” to align with the CIP-003-9 Section 6.3 language, as follows: “Requirement(s) for detection of **inbound and outbound malicious communications between assets** containing low impact BES Cyber Systems with external routable connectivity.”	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The NAGF does not support the proposed scope as described in the SAR. The narrative needs to be revised to state, “malicious communications to/between assets”. The “to/between” is missing in the current form of the SAR scope. The NAGF also requests clarification as to the context, objective, and measurability for “protection of user authentication information in transit.” There is ambiguity and confusion as to where protection responsibility extends outside of the Low Impact Facility. Lastly, the NAGF requests clarity on the term “malicious” and its definition relating to the scope of the types of communication to be detected between Low Impact BES Cyber Systems with ERC.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Regarding Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity, BPA suggests mimicking CIP-005 R2.2. Regarding Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity: this raises the bar of Low with ERC higher than Medium with ERC and creates misalignment in the standards. BPA suggests coordinating this change after changes to Medium ERC so utilities can address the greater risk first.	
Likes 0	

Dislikes 0	
Response	
Alison MacKellar - Constellation - 5,6	
Answer	No
Document Name	
Comment	
Constellation Aligns with the NAGF to vote in the negative to Question 1. Constellation agrees with comments from the NAGF and agrees with comments provided by Exelon and IEEE and does not agree with voting in the affirmative. Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Joseph Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments of EEI and MRO NSRF	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
PNMR does not agree with the scope as described in the SAR.	

While PNMR does agree that coordinated attacks present risk, it is unclear as to the realized risk associated with a coordinated attack utilizing multiple low-impact BES Cyber Systems. As it would be difficult to quantify the number of low-impact systems needed to be utilized in a potential coordinated attack and with uncertain findings as to the use of low-impact systems to conduct a coordinated attack, PNMR believes the potential risk to the BES from such attacks does not sufficiently correlate with the proposed authentication and detection controls which would be a vast expansion of scope.

The NERC Low Impact Criteria Review Report references the risk of coordinated attacks on low impact BES Cyber Systems for those systems that are determined by the CIP-002 Standards. However, the CIP-002 categorization of BES Cyber Systems is not intended to take into account the effect of a coordinated attack in determining the categorization of a BES Cyber System. This language seems to attempt to change the purpose and muddy the scope of the CIP-002 Standard.

PNMR also has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 5,6

Answer	No
Document Name	

Comment

Constellation Aligns with the NAGF to vote in the negative to Question 1. Constellation agrees with comments from the NAGF and agrees with comments provided by Exelon and IEEE and does not agree with voting in the affirmative.

Kimberly Turco on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

Answer	No
Document Name	

Comment

NST strongly suggests not using the phrase, "external routable connectivity" as a qualifier for identifying low impact assets containing BES Cyber Systems that would be subject to any proposed new requirements, notwithstanding the fact the LICRT report uses it. We likewise see no need to "create a new defined term or modify an existing defined term." We respectfully note that an earlier Standard Drafting Team's attempt to define a low impact version of External Routable Connectivity, "LERC," was abandoned for lack of industry support. It is our opinion that the SAR and new SDT can

and should use the existing language from CIP-003-8 Attachment 1 Section 3 Part 3.1 to identify low impact assets containing BES Cyber Systems that would be subject to any proposed new requirements.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

The cost impact to modify the low impact criteria could potentially be significant. Depending on the encryption requirements for authentication, latency might be added to communication at remote sites.

The current wording in bullet points 2 and 3 of the scope suggests applying new, more rigorous and potentially very costly standards to Low Impact systems before applying to High and Medium Impact systems. This creates additional burden on Low Impact before addressing the risks within the higher impact systems. The intent and interpretation of the phrase “protection of user authentication information in transit for remote access”(e.g. encrypting username and password information in transit between low impact systems), could negatively impact reliability when encryption introduces latency in critical communications. Also, the proposed requirement “for detection of malicious communications to/between assets containing low impact BES Cyber Systems” could have conflicting or confusing requirements with upcoming regulation regarding "Internal Network Security Monitoring.”

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	No
Document Name	

Comment

While a coordinated cyber-attack on low impact BCS could be impactful to the BES, it would only be temporary. A coordinated physical attack would be more likely and have a significantly greater impact to the BES. Further ANY allowed electronic access to and from low impact BCS should be legitimate traffic per CIP-003 required Electronic Access Controls.

For easy numbers sake, let’s say 10% of all connected low impact BCS are controlled by low impact Control Centers and the low impact Control Centers are included in that 10%. That would mean 90% of all low impact BCS, that have ERC, already have required Electronic Access Controls. If the low impact controls fail, 90+% of low impact BCS are connected to a higher upstream (medium and high Control Centers at RC, BA, TOP, GOP) BCS which have required Electronic Access Points with stricter access controls and malicious communication detection required. The upstream BCS cyber security controls are in place to detect malicious communications.

Low impact BCS have requirements to detect malicious communication for vendor communications. Thus if a coordinated attack takes place, it would take significant resources unless backdoor/trojan was installed along the software supply chain making traffic appear legitimate, which in that case NO control would detect the nefarious connections, just as in the Solarwinds case. With different entities, using different manufacturers of Cyber Assets in their BCS, even with a distributed supply chain attack, the attack would have a relative small footprint unless the adversaires were able to attack supply chain at multiple vendors and execute a simultaneous attack. That likelihood is incredibly low.

A coordinated physical attack is more likely than a coordinated cyber-attack on low impact BCS. A coordinated planned physical attack on major transmission and generation assets would have a significantly greater impact on the US and last significantly longer than any cyber-attack. A coordinated physical attack would much easier to execute than coordinated cyber-attack on low impact BCS, if an adversary were trying to impact the reliability of the BES. If a coordinated attack on low impact BCS was executed, it should already be detected by existing controls.

Responding directly to the SAR: how would adding requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity reduce the risk of a coordinated attack? To remotely access a low impact BCS, it has to already be permitted by the entity's Electronic Access Controls. If traffic is not approved by the entity, it would be blocked per CIP-003 R2. Thus the access control already exists or an attacker has already bypassed all controls. Further, most attacks leverage vulnerabilities not usernames and passwords to bypass authentication completely.

A coordinated attack would have to come from within multiple entities, with enough combined low impact BCS to cause a BES reliability issue, which already have cybersecurity controls in place, as the traffic would have to be allowed or a well-planned distributed physical installation of nefarious Cyber Assets in a low impact BCS or distributed supply chain attack, or a distributed physical cyber-attack. In any case again these would be short lived attacks compared to a physical attack. If an adversary has to physically go to a location to attack it, physical damage is more than likely what is going to be done at a minimum. We are not suggesting the necessity of usernames and passwords is irrelevant, we are suggesting that this is already a best practice and don't need a new requirement due to the existing controls along with best practices.

There are already requirements to detect malicious Vendor communications. There still aren't requirements for medium impact BCS to have malicious communication detections. This has been brought a number of times.

From a SAR perspective on malicious communication detection, it could have been written this way when it was added to CIP-003 previously. The current proposed change in our opinion should be modified to detect all malicious communications entering or leaving a low impact BCS, not just detecting malicious communications from Vendor remote access, as it is now or as it's written in the SAR from low impact to low impact. Combining the requirement into a singular requirement covering the entire scope of BCS to BCS communications would make the requirement significantly easier to comply with. If we are going to require detections and look at this from a risk lense, we should be monitoring all traffic in and out of a low impact BCS, not just looking specifically where traffic is destined to or from ie low to low or vendor.

Considering the probability and impact, a coordinated cyber-attack on low impact BCS could possibly impact the reliability of the BES. But in this case, when considering risk and modifying requirements to close gaps, we should also consider the longevity of the impacts compared to other risks and prioritize. While a distributed cyber-attack on the BES could impact the reliability of the BES, the longevity of the impact would be much shorter than a physical attack even without sound backup plans.

With protections and controls already in place for low impact BCS, we don't feel adding more requirements to protect against a distributed cyber-attack on the BES will close any real gaps. The highest identified risks in the report are covered by existing controls.

If we are going add these controls to low impact BCS, what about potentially completely unprotected systems that an entity may have that are non BES which may also traverse the same networks? Are there going to be additional controls there? What about corporate systems that traverse the same networks, are we going to add controls there too to protect against a distributed attack, as low impact BCS are often in an enclave off corporate networks?

Likes 0	
Dislikes 0	

Response

Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	

The project scope includes the use of External Routable Connectivity in which the current definition requires the boundary of Electronic Security Perimeter which does not apply to Low Impact BES Cyber System. Further clarificiation in the socpe is required as it is unclear whether boundary is at outside of the network of Low Impact BES Cyber System or outside of the asset containing the Low Impact BES Cyber System.

It is unclear what "remote access" is included in the scope. Is it the user interactive access initiated from outside of the network of Low Impact BES System or outside of the asset containing Low Impact BES System(s)?

Likes 0	
Dislikes 0	
Response	

Jonathan Robbins - AES - AES Corporation - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	

AES Clean Energy supports the MRO NSRF's comments on this Unofficial Comment Form - see below.

"The MRO NSRF agrees with the intent of the proposed scope of the SAR. However, the security controls should be scoped as “to or from BES Cyber Systems that reside within low-impact assets and Cyber Assets that exist outside of the low-impact asset.” This language more appropriately scopes the types of devices that need to be in scope of the CIP-003 Standard and excludes Cyber Assets at a low-impact asset that are not scoped as BES (e.g., corporate communication). The MRO NSRF suggests the following language to be used in the SAR:

Project Scope (Define the parameters of the proposed project):

Modify CIP-003-9 to add security controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications to or from BES Cyber Systems with external routable connectivity that reside within low-impact assets and Cyber Assets that exist outside of the low-impact asset.

Detailed Description:

Modify CIP-003-9 to add:

- Requirement(s) for authentication of remote users before access is granted to BES Cyber Systems with external routable connectivity that are located within low impact assets.
- Requirement(s) for protection of user authentication information in transit for remote access to or from low impact BES Cyber Systems with external routable connectivity located within low impact assets.
- Requirement(s) for detection of malicious communications sent to or from BES Cyber Systems with external routable connectivity that reside within low impact assets and Cyber Assets that exist outside the low impact cyber asset.

Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Jou Yang - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The MRO NSRF agrees with the intent of the proposed scope of the SAR. However, the security controls should be scoped as “to or from networks for BES Cyber Systems that reside within low-impact assets and Cyber Assets that exist outside of the low-impact asset.” This language more appropriately scopes the systems that need to be in scope of the CIP-003 Standard and excludes other types of systems at a low-impact asset that should not be in scope. (e.g., corporate communication). The MRO NSRF suggests the following language to be used in the SAR: Project Scope (Define the parameters of the proposed project): Modify CIP-003-9 to add security controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications on BES Cyber Systems networks that reside within low-impact assets and Cyber Assets that exist outside of the low-impact asset. Detailed Description: Modify CIP-003-9 to add:	

- Requirement(s) for authentication of remote users before access is granted to the networks of BES Cyber Systems that are located within low-impact assets.
- Requirement(s) for protection of user authentication information in transit for remote access to networks for low-impact BES Cyber Systems located within low-impact assets.
- Requirement(s) for detection of malicious communications sent on networks to or from BES Cyber Systems that reside within low-impact assets.

Likes 0	
Dislikes 0	

Response

Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	Yes
Document Name	

Comment

MidAmerican agrees with the proposed scope, but urges NERC to make the clarifications requested in EEI and MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 1,3

Answer	Yes
Document Name	

Comment

Exelon is aligning with EEI's response to this question.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment
Southern Company agrees with the EEI comments.

Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	

Comment
CenterPoint Energy Houston Electric, LLC (CEHE) supports the intent of the proposed scope of the SAR. The proposed enhancements add controls to authenticate remote users and protect information in-transit; however, CEHE is concerned specifically with this bulleted item from the SAR, "*Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity*." This language needs to be clarified. CEHE supports the comments as submitted by the Edison Electric Institute (EEI) as it relates to the proposed language for the "Project Scope" of the SAR.

Likes 0	
Dislikes 0	

Response

TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	

Comment
Southern Indiana Gas and Electric Company d/b/a CenterPoint Energy Indiana South (SIGE) would like to thank the SAR Standards Drafting Team for the opportunity to provide feedback on Project 2023-04 – Modifications to CIP-003. SIGE agrees with the proposed scope of the SAR and supports the comments as submitted by the Edison Electric Institute (EEI) as it relates to the proposed language for the "Project Scope" of the SAR.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes

Document Name	

Comment

Duke Energy agrees with the proposed scope and supports EEI comments.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI supports the intent of the proposed scope of the SAR noting that it closely aligns with the findings of NERC's Low Impact Criteria Review Team (LICRT). While we support this SAR, there are issues that need to be clarified:

1. The LICRT recommendation is limited in scope to communications to and from BES Cyber Systems and while there may be other systems at those locations containing low impact BES Cyber Systems (e.g., corporate communications, etc.), these other assets and their communications should be considered as outside the scope of this SAR.
2. The term external routable connectivity (ERC), as included in the recommendations of this SAR, applies to communications as currently established according to CIP-003, Attachment 1, Section 3.1. Given the term is already defined for medium and high impact BES Cyber Systems, the meaning and how it relates to Low Impact Cyber systems and assets will likely result in confusion without a separate definition. We suggest the SDT define Low Impact ERC.
3. Lastly, the scope of the requirement for the detection of "malicious communications to or between assets containing low impact BES Cyber System with external routable connectivity" should be limited to the detection of external communications to and between facilities containing low impact BES Cyber Systems and not all internal communications within a facility network at a discrete location.

We also suggest that the Project Scope language be modified (bold text) as follows:

Modify CIP-003-9 to add security controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications **to networks** containing low impact BES Cyber Systems **from Cyber Assets outside the assets, for those assets** with external routable connectivity.

Additionally, we suggest that the third bulleted recommendation contained in the Detailed Description section of the SAR include the following modification (bold text) to address our concern regarding the intended scope.

Requirement(s) for detection of malicious communications **sent to or from networks** containing low impact BES Cyber Systems **from Cyber Assets outside the asset, at assets** with external routable connectivity.

Likes 0	
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3,4,5,6, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
WEC Energy Group supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 1,3,6	
Answer	Yes
Document Name	
Comment	
NextEra Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy agrees with EEI's comments which state: EEI supports the intent of the proposed scope of the SAR noting that it closely aligns with the findings of NERC's Low Impact Criteria Review Team (LICRT). While we support this SAR, there are issues that need to be clarified: 1. The LICRT recommendation is limited in scope to communications to and from BES cyber systems and while there may be other systems at those locations containing low impact BES Cyber Systems (e.g., corporate communications, etc.), these other assets and their communications should be considered as outside the scope of this SAR.	

2. The term external routable connectivity (ERC), as included in the recommendations of this SAR, applies to communications as currently established according to CIP-003, Attachment 1, Section 3.1. Given the term is already defined for medium and high impact BES Cyber Systems, the meaning and how

it relates to Low Impact Cyber systems and assets will likely result in confusion without a separate definition. We suggest the SDT define Low Impact ERC.

3. Lastly, the scope of the requirement for the detection of "malicious communications to or between assets containing low impact BES Cyber System with external routable connectivity" should be limited to the detection of external communications to and between facilities containing low impact BES Cyber Systems and not all internal communications within a facility network at a discrete location.

We also suggest that the Project Scope language be modified (bold text) as follows:

Modify CIP-003-9 to add security controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications assets to networks containing low impact BES Cyber Systems from Cyber Assets outside the assets, for those assets with external routable connectivity.

Additionally, we suggest that the third bulleted recommendation contained in the Detailed Description section of the SAR include the following modification (bold text) to address our concern regarding the intended scope.

Requirement(s) for detection of malicious communications to/between sent to or from networks assets containing low impact BES Cyber Systems from Cyber Assets outside the asset, at assets with external routable connectivity.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Evergy - 1,3,5,6 - MRO

Answer	Yes
Document Name	

Comment

Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) to question #1.

Likes 0	
Dislikes 0	

Response

Michelle Amarantos - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

AZPS agrees with and the proposed scope, however we believe that the use of the CIP-002 categorization language “asset that contains a low impact BES Cyber Systems” may lead to confusion. Modifications should only address communications to low impact BCS at an asset. An asset may contain networks or communications unrelated to the low impact BCS. These unrelated networks appear to be within scope with the current language.

We suggest the Project Scope language be modified as follows:

Modify CIP-003-9 to add security controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications at assets containing low impact BES Cyber Systems with external routable connectivity. Modifications will only address communications from outside the asset to low impact BES Cyber Systems with external routable connectivity.

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Hydro-Quebec (HQ) - 1 - NPCC

Answer	Yes
Document Name	

Comment

While we agree with the overall proposed scope, we offer the following comments as suggsted improvements:

The proposed scope depends on the definition of “external routable connectivity” which is not a defined term and is not part of this SAR’s scope. Recommend this SAR’s scope expand by including what “low impact BES Cyber Systems at assets containing those systems that have external routable connectivity” means. A NERC-defined term should be capitalized. In this SAR, every instance of “external routable connectivity” is lowercase which suggests the SAR is not using a defined term. The NERC-defined term depends on ESP. Lows do not have ESPs. Lending more credibility to the conclusion this SAR is not using a defined term. This SAR’s source is the Low Impact Criteria Review Team report which includes “Electronic Access Controls” as a risk which includes “require the implementation of electronic access controls that permit only needed inbound and outbound routable protocol electronic access to the asset containing lows (and thus all individual low impact systems) from anything outside of the asset.” Most CIP-003 interpretations were for the location, not the asset. Both auditors and implementers need a consistent interpretation. What is the boundary? How does one know internal vs external?

Request one term with a definition instead of “remote” and “external.” We need clarification of remote/external to what?
Consider the impact of “demarcation of” / “asset boundary” in CIP-003
Request clarification of other terms used in CIP-003. Suggest this is an opportunity to consolidate terms and reduce industry confusion
User-initiated interactive access (CIP 3 Reference Model 5, concerning Low Impact)
Inbound and outbound electronic access (CIP 3, Section 3)
Inbound electronic access (CIP 3 Reference Model 5, concerning Low Impact)
Indirect access (CIP 3 Reference Model 6,9)
Vendor electronic remote access (proposed CIP 3)
Lower case “erc” that the SAR proposes
Does this include system-to-system? Does this include Interactive Remote Access?

Likes 0	
Dislikes 0	

Response	
Lori Frisk - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports the comments provided by Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	

Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	Yes
Document Name	
Comment	

While we agree with the overall proposed scope, we offer the following comments as suggested improvements.

The proposed scope depends on the definition of “external routable connectivity” which is not a defined term and is not part of this SAR’s scope. Recommend this SAR’s scope expand by including what “low impact BES Cyber Systems at assets containing those systems that have external routable connectivity” means. A NERC-defined term should be capitalized. In this SAR, every instance of “external routable connectivity” is lowercase which suggests the SAR is not using a defined term. The NERC-defined term depends on ESP. Lows do not have ESPs. Lending more credibility to the conclusion this SAR is not using a defined term. This SAR’s source is the Low Impact Criteria Review Team report which includes “Electronic Access Controls” as a risk which includes “require the implementation of electronic access controls that permit only needed inbound and outbound routable protocol electronic access to the asset containing lows (and thus all individual low impact systems) from anything outside of the asset.” Most CIP-003 interpretations were for the location, not the asset. Both auditors and implementers need a consistent interpretation. What is the boundary? How does one know internal vs external?

Request one term with a definition instead of “remote” and “external.” We need clarification of remote/external to what?
Consider the impact of “demarcation of” / “asset boundary” in CIP-003
Request clarification of other terms used in CIP-003. Suggest this is an opportunity to consolidate terms and reduce industry confusion
User-initiated interactive access (CIP 3 Reference Model 5, concerning Low Impact)
Inbound and outbound electronic access (CIP 3, Section 3)
Inbound electronic access (CIP 3 Reference Model 5, concerning Low Impact)
Indirect access (CIP 3 Reference Model 6,9)
Vendor electronic remote access (proposed CIP 3)
Lower case “erc” that the SAR proposes
Does this include system-to-system? Does this include Interactive Remote Access?

Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Kuehne - AEP - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karla Weaver - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	
The proposed scope depends on the definition of “external routable connectivity” which is not a defined term and is not part of this SAR’s scope. Recommend this SAR’s scope expand by including what “low impact BES Cyber Systems at assets containing those systems that have external	

routable connectivity” means. A NERC-defined term should be capitalized. In this SAR, every instance of “external routable connectivity” is lowercase which suggests the SAR is not using a defined term. The NERC-defined term depends on ESP. Lows do not have ESPs. Lending more credibility to the conclusion this SAR is not using a defined term. This SAR’s source is the Low Impact Criteria Review Team report which includes “Electronic Access Controls” as a risk which includes “require the implementation of electronic access controls that permit only needed inbound and outbound routable protocol electronic access to the asset containing lows (and thus all individual low impact systems) from anything outside of the asset.” Most CIP-003 interpretations were for the location, not the asset. Both auditors and implementers need a consistent interpretation. What is the boundary? How does one know internal vs external?

Request one term with a definition instead of “remote” and “external.” We need clarification of remote/external to what?

Consider the impact of “demarcation of” / “asset boundary” in CIP-003

Request clarification of other terms used in CIP-003. Suggest this is an opportunity to consolidate terms and reduce industry confusion

User-initiated interactive access (CIP 3 Reference Model 5, concerning Low Impact)

Inbound and outbound electronic access (CIP 3, Section 3)

Inbound electronic access (CIP 3 Reference Model 5, concerning Low Impact)

Indirect access (CIP 3 Reference Model 6,9)

Vendor electronic remote access (proposed CIP 3)

Lower case “erc” that the SAR proposes

Does this include system-to-system? Does this include Interactive Remote Access?

Likes 0	
Dislikes 0	

Response

2. Provide any additional comments for the SAR drafting team to consider, if desired.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC	
Answer	
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	
Document Name	
Comment	
We would like to thank the SDT for allowing us to provide feedback.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
The current scope wording could require implementation of complex, time-consuming solutions that could negatively impact reliability with minimal security benefit. Adding these specific technical requirements to CIP-003-9 may cause confusion with similar requirements currently included in CIP-005-7 and CIP-007-6. Including these detailed, technical requirements in CIP-003-9 instead of with other ESP controls in CIP-005-7 increases the likelihood of non-compliance because CIP-003-9 is intended to define security management controls at the cyber program level rather than at the detailed technical level. In addition, we suggest clarification on the Detailied Description to Modify CIP-003-9 to include:	

Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.

Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

Answer	
Document Name	

Comment

NST suggests the following:

New requirement(s) for "protection of user authentication information in transit" should specify what such protections are meant to accomplish, e.g., "confidentiality protection for user authentication information in transit."

New requirement(s) for "detection of malicious communications to/between assets" containing low impact BES Cyber Systems" should be "to or from assets containing low impact BES Cyber Systems."

The SAR's "Date Submitted" field appears to have a typo.

Likes 0	
Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5

Answer	
Document Name	

Comment

We agree Project 2023-04 (Modifications to CIP-003) impacts 2016-02 (Modifications to CIP Standards) and 2021-03 (CIP-002 Transmission Owner Control Centers). The industry is trying to resolve earlier issues from multiple SDTs simultaneously updating CIP Standards. It appears there will likely be significant overlap and possible contradiction in required CIP-002 changes between both the ongoing Project 2016-02 project and the proposed Project 2021-03 projects, we previously recommended that Project 2016-02 completes before Project 2021-03 project proceeds. We extend this recommendation to Projects 2023-04 and 2023-05 (Internal Network Security Monitoring) because CIP Requirements and definitions are deeply intertwined. Correcting

one issue has caused issues elsewhere. Multiple projects updating the same Requirements and definitions cost the industry money. Entities invest in implementing the new language. Only to see that investment lost a few months later when another project changes that language – see LERC and LEAP.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 5,6	
Answer	
Document Name	
Comment	
Constellation has no additional comments Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	
We agree Project 2023-04 (Modifications to CIP-003) impacts 2016-02 (Modifications to CIP Standards) and 2021-03 (CIP-002 Transmission Owner Control Centers). The industry is trying to resolve earlier issues from multiple SDTs simultaneously updating CIP Standards. It appears there will likely be significant overlap and possible contradiction in required CIP-002 changes between both the ongoing Project 2016-02 project and the proposed Project 2021-03 projects, we previously recommended that Project 2016-02 completes before Project 2021-03 project proceeds. We extend this recommendation to Projects 2023-04 and 2023-05 (Internal Network Security Monitoring) because CIP Requirements and definitions are deeply intertwined. Correcting one issue has caused issues elsewhere. Multiple projects updating the same Requirements and definitions cost the industry money. Entities invest in implementing the new language. Only to see that investment lost a few months later when another project changes that language – see LERC and LEAP.	
Likes 0	

Dislikes 0	
Response	
Chantal Mazza - Hydro-Quebec (HQ) - 1 - NPCC	
Answer	
Document Name	
Comment	
We agree Project 2023-04 (Modifications to CIP-003) impacts 2016-02 (Modifications to CIP Standards) and 2021-03 (CIP-002 Transmission Owner Control Centers). The industry is trying to resolve earlier issues from multiple SDTs simultaneously updating CIP Standards. It appears there will likely be significant overlap and possible contradiction in required CIP-002 changes between both the ongoing Project 2016-02 project and the proposed Project 2021-03 projects, we previously recommended that Project 2016-02 completes before Project 2021-03 project proceeds. We extend this recommendation to Projects 2023-04 and 2023-05 (Internal Network Security Monitoring) because CIP Requirements and definitions are deeply intertwined. Correcting one issue has caused issues elsewhere. Multiple projects updating the same Requirements and definitions cost the industry money. Entities invest in implementing the new language. Only to see that investment lost a few months later when another project changes that language – see LERC and LEAP.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter	
Answer	
Document Name	
Comment	
FirstEnergy seeks the SAR’s direction to cross check all existing projects for potential encompassing of standards that may be affected.	
Likes 0	
Dislikes 0	
Response	
Joseph Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	

Xcel Energy supports the comments of EEI and MRO NSRF	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5,6	
Answer	
Document Name	
Comment	
N/A Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
BPA suggests adding “Where capable” or “Where technically feasible” to these requirements. Low sites often have the most outdated technology and some of the controls recommended may not be doable at the sites.	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3,4,5,6, Group Name WEC Energy Group	
Answer	
Document Name	
Comment	

WEC Energy Group supports the comments submitted by the MRO NSRF.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	
Document Name	

Comment

The NAGF does not have any additional comments.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6 - WECC, Group Name Tacoma Power

Answer	
Document Name	

Comment

Tacoma Power recommends that when developing the CIP-003-X redlines, the SDT should provide additional clarification as to how these changes are different than the work being performed in response to the FERC Order on internal network security monitoring. As currently written in the SAR, it's not clear whether Project 2023-04 will address internal (east-west) or external (north-south) network monitoring.

Additionally, the SDT should consider if there's a security benefit to monitoring encrypted communications and if there are benefits, how entities will monitor these encrypted communications.

Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	
Document Name	

Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	
Document Name	
Comment	
ATC requests NERC consider the timing of this SAR alongside the emerging study to evaluate Internal Network Security Monitoring (INSM) for low impact, as well as the inflight effort for 2016-02 to enable for virtualization. Having multiple drafting teams focused on modifications to the same CIP Standard creates potential for confusion and reduces the ability to attain steady state for these regulations. ATC also supports EEI and NSRF comments.	
Likes 1	Tacoma Public Utilities (Tacoma, WA), 1,3,4,5,6, Wike Jennie
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Jou Yang - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	

Comment
The MRO NSRF has concerns with the use term “external routable connectivity” There is already a defined term External Routable Connectivity that applies to high and medium-impact BES Cyber Systems and not to low impact. The term used on this SAR has a different meaning or is applied in a different way than for the defined term. For this reason, the MRO NSRF requests that the drafting team either uses a different term or defines low impact External Routable Connectivity.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	
Document Name	

Comment
MISO supports the comments submitted by the MRO NSRF.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - AES - AES Corporation - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	

Comment
None

Likes 0	
Dislikes 0	

Response

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name: 2023-04 Modifications to CIP-003 | SAR
Comment Period Start Date: 3/31/2023
Comment Period End Date: 5/15/2023
Associated Ballot(s):

There were 37 sets of responses, including comments from approximately 112 different people from approximately 89 companies representing 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, contact Director, Standards Development Latrice Harkness (via email) or at (404) 858-8088.

Questions

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope, please provide your recommendation and explanation.

2. Provide any additional comments for the SAR drafting team to consider, if desired.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
WEC Energy Group, Inc.	Christine Kane	3,4,5,6		WEC Energy Group	Christine Kane	WEC Energy Group	3	RF
					Matthew Beilfuss	WEC Energy Group, Inc.	4	RF
					Clarice Zellmer	WEC Energy Group, Inc.	5	RF
					David Boeshaar	WEC Energy Group, Inc.	6	RF
Tacoma Public Utilities (Tacoma, WA)	Jennie Wike	1,3,4,5,6	WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC

					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Ryan Strom	Buckeye Power, Inc.	5	RF
					kylee Kropp	Sunflower Electric Power Corporation	1	MRO
					Nikki Carson-Marquis	Minnkota Power Cooperative	NA - Not Applicable	MRO
MRO	Jou Yang	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Chris Bills	City of Independence, Power and Light Department	5	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO

Christopher Bills	City of Independence Power & Light	3,5	MRO
Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
Marc Gomez	Southwestern Power Administration	1	MRO
Matthew Harward	Southwest Power Pool, Inc. (RTO)	2	MRO
Bryan Sherrow	Board of Public Utilities	1	MRO
Terry Harbour	Berkshire Hathaway Energy - MidAmerican Energy Co.	1	MRO
Terry Harbour	MidAmerican Energy Company	1,3	MRO
Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO

					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Shonda McCain	Omaha Public Power District	6	MRO
					George E Brown	Pattern Operators LP	5	MRO
					George Brown	Acciona Energy USA	5	MRO
					Jaimin Patel	Saskatchewan Power Cooperation	1	MRO
					Kimberly Bentley	Western Area Power Administration	1,6	MRO
					Jay Sethi	Manitoba Hydro	1,3,5,6	MRO
					Michael Ayotte	ITC Holdings	1	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	1,3,4,5,6		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF

					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Jim Howell, Jr.	Southern Company - Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC

Alain Mukama	Hydro One Networks, Inc.	1	NPCC
Deidre Altobell	Con Edison	1	NPCC
Jeffrey Streifling	NB Power Corporation	1	NPCC
Michele Tondalo	United Illuminating Co.	1	NPCC
Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
Randy Buswell	Vermont Electric Power Company	1	NPCC
James Grant	NYISO	2	NPCC
John Pearson	ISO New England, Inc.	2	NPCC
Harishkumar Subramani Vijay Kumar	Independent Electricity System Operator	2	NPCC
Randy MacDonald	New Brunswick	2	NPCC

	Power Corporation		
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
David Burke	Orange and Rockland	3	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
David Kwan	Ontario Power Generation	4	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
Glen Smith	Entergy Services	4	NPCC
Sean Cavote	PSEG	4	NPCC

					Jason Chandler	Con Edison	5	NPCC
					Tracy MacNicoll	Utility Services	5	NPCC
					Shivaz Chopra	New York Power Authority	6	NPCC
					Vijay Puran	New York State Department of Public Service	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					John Hastings	National Grid	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
					Joshua London	Eversource Energy	1	NPCC
Western Electricity	Steven Rueckert	10		WECC	Steve Rueckert	WECC	10	WECC

Coordinating Council					Phil O'Donnell	WECC	10	WECC

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope, please provide your recommendation and explanation.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
ATC requests consideration of collapsing the low impact requirements with CIP-005 and CIP-007 instead of continuing to have a separate requirement within CIP-003 for low impact. If the requirements cannot be collapsed into those standards, ATC requests consideration that the defined ESP term does not extend to low impact; and, there is therefore no External Routable Connectivity applicable either. This SAR may need to introduce formally a L-ESP and L-ERC, which would also then possibly include Low-EACMS and Intermediate Systems. ATC also supports EEI and NSRF comments.	
Likes 0	
Dislikes 0	
Response	
The SDT notes that for entities with only low-impact BES Cyber Systems (BCS), the relevant CIP standards are confined to CIP-002 and CIP-003. The SDT asserts the LICRT recommendations would not justify a reorganization of these standards across other standards that today are specific to high or medium impact. The SDT agrees that the concept of "ERC" for lows, defined in terms of ESPs, needs to be considered and a new glossary term potentially proposed that fits the low impact paradigm. This is included in the SAR and will be considered during standards drafting.	
Jennie Wike - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6 - WECC, Group Name Tacoma Power	
Answer	No
Document Name	

Comment
Tacoma Power does not agree with the proposed scope described in the SAR. This SAR is proposing more strict controls for low impact BCS with ERC than the controls currently required in CIP-005 for medium impact BCS without ERC. By imposing more strict controls on low impact BCS with ERC, this is upending the CIP-002 categorization. The NERC Standards establish low/medium/high impacts in CIP-002 and fulfill Requirements based on this impact in the other CIP Standards. A low impact BCS should not have more controls than a medium impact BCS. This SAR is placing greater emphasis, and more restrictive controls, on lows with IP connectivity than medium impact BCS without ERC. This begs the question of whether medium BCS without ERC should now be classified as low impact, and lows with IP connectivity should be classified as medium impact. In summary, the amount of controls applied to a type of asset should be dependent on its categorization. Tacoma Power does not agree with creating a precedent for applying greater controls to low impact BCS. Tacoma Power is also concerned that the scope of this SAR is broad, and as a result, will be difficult to implement. For example, the term “remote access” used in the Detailed Description section is not defined and depending on how an entity defines this term, it will impact the scope of the Requirement(s). The SAR should clarify whether “remote access” is referring to north-south or east-west communication. Lastly, instead of focusing on asset-level detection, Tacoma Power recommends that the SAR should focus on defining and establishing an Electronic Security Perimeter (ESP) for low impact BCS, and then requiring detection/monitoring of malicious communication at the ESP boundary. This approach is easier to understand and implement than focusing on new Requirements based on asset-level detection. Tacoma Power recommends re-wording the third bullet in the Detailed Description section to the following: “Requirement(s) for establishing an ESP for low impact BES Cyber Systems with external routable connectivity, and detecting malicious communications at the ESP boundary.” If the SAR drafting team keeps the approach for requiring asset-level detection, then Tacoma Power recommends changing the “to/between” language in the third bullet to “inbound and outbound” to align with the CIP-003-9 Section 6.3 language, as follows:

"Requirement(s) for detection of **inbound and outbound malicious communications between assets** containing low impact BES Cyber Systems with external routable connectivity."	
Likes 0	
Dislikes 0	

Response

The SDT notes that the required cyber security program for lows is not stricter than the required program for mediums w/o ERC. Medium impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to the level of individual cyber systems. The LICRT report pointed to the risk of routable external connectivity that can be used as an avenue of *coordinated* attacks against multiple assets containing low impact BCS and the SAR is addressing requirements that can mitigate that risk. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The SDT asserts that low impact BCS with external routable protocol remote access is a potential higher risk in that one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums.

The SDT agrees that the term "remote access" is not defined in the SAR, but it is essentially described in the current CIP-003, Attachment 1, Section 3.1 and referenced in Section 6 for vendor remote access. Modifications to these sections will take this into account as the team moves from the SAR to standards drafting.

The SDT agrees with concerns expressed for malicious communication detection and has made modifications to that bullet to refer to the access defined in CIP-003, Attachment 1, Section 3.1 to clarify intent. The SDT does not foresee a need to extend the ESP Glossary term to lows in order to meet the objectives of this SAR and desires to leave the future drafting open to describing the type of communications for which this detection is required, but leave the implementation of how and where to the entities depending on their architectures and circumstances. The SDT also notes that while the ESP Glossary term needs to be maintained for compatibility with long-defined high and medium impact requirements, as other network security models such as Zero Trust Architectures are implemented over time, the SDT does not foresee propagating the term to lows at this time.

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The NAGF does not support the proposed scope as described in the SAR. The narrative needs to be revised to state, “malicious communications to/between assets”. The “to/between” is missing in the current form of the SAR scope. The NAGF also requests clarification as to the context, objective, and measurability for “protection of user authentication information in transit.” There is ambiguity and confusion as to where protection responsibility extends outside of the Low Impact Facility. Lastly, the NAGF requests clarity on the term “malicious” and its definition relating to the scope of the types of communication to be detected between Low Impact BES Cyber Systems with ERC.	
Likes 0	
Dislikes 0	
Response	
The SDT agrees with the concerns expressed for malicious communication detection and has made modifications to that bullet to refer to the access defined in CIP-003, Attachment 1, Section 3.1 to clarify intent. The SDT asserts that the SAR as a “scope of work” document is defining the team’s scope regarding the two mentioned items, 1) the protection of user authentication in transit, and 2) the definition of “malicious”. When drafting revisions to CIP-003-9, the SDT will draft the specific requirement language, definitions, and measures to meet the SAR scope. The SDT agrees with concerns on the term “malicious” and has modified the SAR accordingly to use the previously approved language from other CIP standards of “known or suspected malicious communications”.	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
Regarding Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity, BPA suggests mimicking CIP-005 R2.2. Regarding Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity: this raises the bar of Low with ERC higher than Medium with ERC and creates misalignment in the standards. BPA suggests coordinating this change after changes to Medium ERC so utilities can address the greater risk first.

Likes 0	
Dislikes 0	

Response
The SDT will take into account the CIP-005 R2.2 concepts during the future drafting phase. Thank you for the comment. As to the issue of these requirements for lows being higher than medium impact, please see the Tacoma Power response.

Alison MacKellar - Constellation - 5,6	
Answer	No
Document Name	

Comment
Constellation Aligns with the NAGF to vote in the negative to Question 1. Constellation agrees with comments from the NAGF and agrees with comments provided by Exelon and IEEE and does not agree with voting in the affirmative. Alison Mackellar on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	
Response	
Please see the SDT response to NAGF, Exelon, and EEI (assuming IEEE is an autocorrect typo) comments.	
Joseph Gatten - Xcel Energy, Inc. - 1,3,5,6 – ,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments of EEI and MRO NSRF	
Likes 0	
Dislikes 0	
Response	
Please see response to EEI and MRO NSRF comments.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
PNMR does not agree with the scope as described in the SAR. While PNMR does agree that coordinated attacks present risk, it is unclear as to the realized risk associated with a coordinated attack utilizing multiple low-impact BES Cyber Systems. As it would be difficult to quantify the number of	

low-impact systems needed to be utilized in a potential coordinated attack and with uncertain findings as to the use of low-impact systems to conduct a coordinated attack, PNMR believes the potential risk to the BES from such attacks does not sufficiently correlate with the proposed authentication and detection controls which would be a vast expansion of scope. The NERC Low Impact Criteria Review Report references the risk of coordinated attacks on low impact BES Cyber Systems for those systems that are determined by the CIP-002 Standards. However, the CIP-002 categorization of BES Cyber Systems is not intended to take into account the effect of a coordinated attack in determining the categorization of a BES Cyber System. This language seems to attempt to change the purpose and muddy the scope of the CIP-002 Standard. PNMR also has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.	
Likes 0	
Dislikes 0	
Response	
The SDT agrees that CIP-002 does indeed categorize individual BCS according to that individual system's potential impact. The SDT agrees CIP-002 does not take coordinated attacks into account when categorizing individual BCS. However, that does not preclude the body of CIP standards from having requirements addressing the risk of using network access to aggregate impact of many compromised systems across multiple sites, which is the basis of the LICRT report's recommendations. The SDT sees no conflict between the impact rating of an individual system (per CIP-002) and a requirement in CIP-003's required cyber security plan to mitigate the risks from aggregation of many assets containing lows. The SDT disagrees that this muddies the scope of CIP-002. The SDT notes that for entities with only low-impact BCS, the relevant CIP standards are confined to CIP-002 and CIP-003. The SDT asserts the LICRT recommendations would not justify a reorganization of these standards across other standards that today are specific to high or medium impact.	
Kimberly Turco - Constellation - 5,6	
Answer	No

Document Name	
Comment	
Constellation Aligns with the NAGF to vote in the negative to Question 1. Constellation agrees with comments from the NAGF and agrees with comments provided by Exelon and IEEE and does not agree with voting in the affirmative. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Please see the SDT response to NAGF, Exelon, and EEI (assuming IEEE is an autocorrect typo) comments.	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	No
Document Name	
Comment	
NST strongly suggests not using the phrase, "external routable connectivity" as a qualifier for identifying low impact assets containing BES Cyber Systems that would be subject to any proposed new requirements, notwithstanding the fact the LICRT report uses it. We likewise see no need to "create a new defined term or modify an existing defined term." We respectfully note that an earlier Standard Drafting Team's attempt to define a low impact version of External Routable Connectivity, "LERC," was abandoned for lack of industry support. It is our opinion that the SAR and new SDT can and should use the existing language from CIP-003-8 Attachment 1 Section 3 Part 3.1 to identify low impact assets containing BES Cyber Systems that would be subject to any proposed new requirements.	
Likes 0	

Dislikes 0	

Response

The SDT agrees that the issues associated with using ERC-like terminology in regards to assets containing low impact BCS is problematic and should be resolved. The SDT agrees that this connectivity is essentially defined in CIP-003 Attachment 1, Section 3.1. In the future standard drafting efforts, the SDT will consider making that language a different defined term so that it can be used in all the places in which it needs to be referenced and avoid these issues in the future.

The SDT notes that the term LERC has been in the NERC Glossary in the past, but asserts it was not abandoned for lack of industry support. When filed with FERC and approved in Order 822, FERC noted an unintended consequence in the LERC definition and its interplay with the LEAP definitions and the requirement language. Project 2016-02 was formed to address FERC Order 822 and retired the two terms to quickly eliminate the issue and instead described the connectivity and electronic access controls required in CIP-003, Attachment 1, Section 3. However, as pointed out, there remains a need to refer to this type of connectivity in regards to lows and the SDT will consider during its standard drafting phase whether a new defined term, based on the description in Section 3, Part 3.1 is needed.

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

The cost impact to modify the low impact criteria could potentially be significant. Depending on the encryption requirements for authentication, latency might be added to communication at remote sites.

The current wording in bullet points 2 and 3 of the scope suggests applying new, more rigorous and potentially very costly standards to Low Impact systems before applying to High and Medium Impact systems. This creates additional burden on Low Impact before addressing the risks within the higher impact systems. The intent and interpretation of the phrase “protection of user authentication information in transit for remote access”(e.g. encrypting username and password information in transit between low impact systems), could negatively impact reliability when encryption

introduces latency in critical communications. Also, the proposed requirement “for detection of malicious communications to/between assets containing low impact BES Cyber Systems” could have conflicting or confusing requirements with upcoming regulation regarding "Internal Network Security Monitoring.”	
Likes 0	
Dislikes 0	
Response	
The SDT will take into account the impacts to entities of the requirements during the drafting phase. However, the SDT notes that the scope is protection of user authentication information during transit used for remote access, and that most common protocols used for this purpose (RDP, SSH, etc.) are encrypted by default in order to protect such information. The SDT notes that some legacy protocols (Telnet, FTP, etc.) that may still be in use are based on clear text transmission of user authentication information, and that should be protected. Many today use VPN’s or other tunneling technology to protect such information. It is surmised that many already use RDP or SSH within SSL VPN’s to site firewalls, thus having “double” encryption without inducing undue latency for this type of user interactive remote access. The SDT does not at this point in time foresee this being an undue burden but will keep this in mind during the drafting phase. The SDT notes that the FERC Order for INSM is currently scoped to high impact and medium impact w/ERC and should not conflict with this effort at this time.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	
While a coordinated cyber-attack on low impact BCS could be impactful to the BES, it would only be temporary. A coordinated physical attack would be more likely and have a significantly greater impact to the BES. Further ANY	

allowed electronic access to and from low impact BCS should be legitimate traffic per CIP-003 required Electronic Access Controls.

For easy numbers sake, let's say 10% of all connected low impact BCS are controlled by low impact Control Centers and the low impact Control Centers are included in that 10%. That would mean 90% of all low impact BCS, that have ERC, already have required Electronic Access Controls. If the low impact controls fail, 90+% of low impact BCS are connected to a higher upstream (medium and high Control Centers at RC, BA, TOP, GOP) BCS which have required Electronic Access Points with stricter access controls and malicious communication detection required. The upstream BCS cyber security controls are in place to detect malicious communications.

Low impact BCS have requirements to detect malicious communication for vendor communications. Thus if a coordinated attack takes place, it would take significant resources unless backdoor/trojan was installed along the software supply chain making traffic appear legitimate, which in that case NO control would detect the nefarious connections, just as in the SolarWinds case. With different entities, using different manufacturers of Cyber Assets in their BCS, even with a distributed supply chain attack, the attack would have a relative small footprint unless the adversaries were able to attack supply chain at multiple vendors and execute a simultaneous attack. That likelihood is incredibly low.

A coordinated physical attack is more likely than a coordinated cyber-attack on low impact BCS. A coordinated planned physical attack on major transmission and generation assets would have a significantly greater impact on the US and last significantly longer than any cyber-attack. A coordinated physical attack would much easier to execute than coordinated cyber-attack on low impact BCS, if an adversary were trying to impact the reliability of the BES. If a coordinated attack on low impact BCS was executed, it should already be detected by existing controls.

Responding directly to the SAR: how would adding requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity reduce the risk of a coordinated attack? To remotely access a low impact BCS, it has to already be permitted by the entity's Electronic Access Controls. If traffic is not approved by the entity, it would be blocked per CIP-003 R2. Thus the access control already exists or an attacker has already bypassed all controls. Further, most attacks leverage vulnerabilities not usernames and passwords to bypass authentication completely.

A coordinated attack would have to come from within multiple entities, with enough combined low impact BCS to cause a BES reliability issue, which already have cybersecurity controls in place, as the traffic would have to be allowed or a well-planned distributed physical installation of nefarious Cyber Assets in a low impact BCS or distributed supply chain attack, or a distributed physical cyber-attack. In any case again these would be short lived attacks compared to a physical attack. If an adversary has to physically go to a location to attack it, physical damage is more than likely what is going to be done at a minimum. We are not suggesting the necessity of usernames and passwords is irrelevant, we are suggesting that this is already a best practice and don't need a new requirement due to the existing controls along with best practices.

There are already requirements to detect malicious Vendor communications. There still aren't requirements for medium impact BCS to have malicious communication detections. This has been brought a number of times.

From a SAR perspective on malicious communication detection, it could have been written this way when it was added to CIP-003 previously. The current proposed change in our opinion should be modified to detect all malicious communications entering or leaving a low impact BCS, not just detecting malicious communications from Vendor remote access, as it is now or as it's written in the SAR from low impact to low impact. Combining the requirement into a singular requirement covering the entire scope of BCS to BCS communications would make the requirement significantly easier to comply with. If we are going to require detections and look at this from a risk lens, we should be monitoring all traffic in and out of a low impact BCS, not just looking specifically where traffic is destined to or from i.e. low to low or vendor.

Considering the probability and impact, a coordinated cyber-attack on low impact BCS could possibly impact the reliability of the BES. But in this case, when considering risk and modifying requirements to close gaps, we should also consider the longevity of the impacts compared to other risks and prioritize. While a distributed cyber-attack on the BES could impact the reliability of the BES, the longevity of the impact would be much shorter than a physical attack even without sound backup plans.

With protections and controls already in place for low impact BCS, we don't feel adding more requirements to protect against a distributed cyber-attack on the BES will close any real gaps. The highest identified risks in the report are covered by existing controls.

If we are going add these controls to low impact BCS, what about potentially completely unprotected systems that an entity may have that are non BES which may also traverse the same networks? Are there going to be additional controls there? What about corporate systems that traverse the same networks, are we going to add controls there too to protect against a distributed attack, as low impact BCS are often in an enclave off corporate networks?	
Likes 0	
Dislikes 0	

Response

The SDT agrees that any allowed electronic access to and from low impact BCS should be legitimate traffic per CIP-003's required Electronic Access Controls. However, this typically means the access is controlled (typically via a firewall) and all the firewall rules are justified as "necessary" per Section 3. An entity could enable Remote Desktop Protocol (RDP) on a BCS for remote support, deem the RDP port (3389) necessary to be open through the firewall to untrusted external networks, and require no authentication of who is using that port before they enter the local network and have access to the BCS.

The SDT notes as one example that typically entity personnel that have remote access into the entity's substations have access to all. As certain BCS devices in these locations may only have some sort of password or PIN authentication without a concept of an individual "user", having requirements to authenticate users before access to the networks containing such devices mitigates the risk of access to many such sites in a coordinated attack.
The SDT agrees that these are best practices and many already have such protections in place. However, it is not strictly prohibited by the standards for an entity to put a BCS behind a firewall that simply has RDP, SSH, FTP, Telnet, and other ports deemed "necessary" open to the public Internet, allowing adversaries access directly to BCS and the ability to attempt exploitation of any vulnerabilities in those services. Authenticating users before access to such networks is granted will mitigate the risk of any Internet citizen being able to "knock on the door" of a BCS through the Attachment 1, Section 3 open ports.

The SDT agrees with the comments concerning detecting malicious communications being broader than just vendor communications. Previous SDTs' scope was limited to 'supply chain' risks thus driving that SAR's detection scope. This

current SDT, when it enters the drafting phase, will consider how to simplify the malicious communication detection requirements as the scope is broader with this SAR. As to the longevity of impact from a coordinated cyber attack vs. a physical attack, the SDT notes that there are scenarios where some BES Cyber Systems could be manipulated in ways to cause physical damage to BES assets, thus equating the impact timeframe. As to the scope of cyber security controls for non-BES devices or networks, the SAR (and NERC Standards in general) are limited to BES reliability, and the scope of CIP-003 is outlined in Section 4.3 of the standard, which for entities other than DP is all BES Facilities. This SAR does not extend beyond that. As the SDT enters the drafting phase, it will keep in mind the distinction of differing networks, such as corporate networks, that are outside of the scope of BCS.	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	
The project scope includes the use of External Routable Connectivity in which the current definition requires the boundary of Electronic Security Perimeter which does not apply to Low Impact BES Cyber System. Further clarification in the scope is required as it is unclear whether boundary is at outside of the network of Low Impact BES Cyber System or outside of the asset containing the Low Impact BES Cyber System. It is unclear what "remote access" is included in the scope. Is it the user interactive access initiated from outside of the network of Low Impact BES System or outside of the asset containing Low Impact BES System(s)?	
Likes 0	
Dislikes 0	
Response	
The SDT agrees that the concept of “ERC” for lows, defined in terms of ESPs, needs to be considered and a new glossary term potentially proposed that fits the low impact paradigm. This is included in the SAR and will be considered during	

standards drafting. The SDT has made some clarifying modifications to the SAR regarding remote access and will refine requirement language during the standards drafting phase.	
Jonathan Robbins - AES - AES Corporation - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	

AES Clean Energy supports the MRO NSRF's comments on this Unofficial Comment Form - see below.

"The MRO NSRF agrees with the intent of the proposed scope of the SAR. However, the security controls should be scoped as “to or from BES Cyber Systems that reside within low-impact assets and Cyber Assets that exist outside of the low-impact asset.” This language more appropriately scopes the types of devices that need to be in scope of the CIP-003 Standard and excludes Cyber Assets at a low-impact asset that are not scoped as BES (e.g., corporate communication). The MRO NSRF suggests the following language to be used in the SAR:

Project Scope (Define the parameters of the proposed project):

Modify CIP-003-9 to add security controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications to or from BES Cyber Systems with external routable connectivity that reside within low-impact assets and Cyber Assets that exist outside of the low-impact asset.

Detailed Description:

Modify CIP-003-9 to add:

- Requirement(s) for authentication of remote users before access is granted to BES Cyber Systems with external routable connectivity that are located within low impact assets.
- Requirement(s) for protection of user authentication information in transit for remote access to or from low impact BES Cyber Systems with external routable connectivity located within low impact assets.

• Requirement(s) for detection of malicious communications sent to or from BES Cyber Systems with external routable connectivity that reside within low impact assets and Cyber Assets that exist outside the low impact cyber asset.	
Likes 0	
Dislikes 0	
Response	
See response to MRO NSRF.	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
See response to MRO NSRF.	
Jou Yang - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	

The MRO NSRF agrees with the intent of the proposed scope of the SAR. However, the security controls should be scoped as “to or from networks for BES Cyber Systems that reside within low-impact assets and Cyber Assets that exist outside of the low-impact asset.” This language more appropriately scopes the systems that need to be in scope of the CIP-003 Standard and excludes other types of systems at a low-impact asset that should not be in scope. (e.g., corporate communication). The MRO NSRF suggests the following language to be used in the SAR: Project Scope (Define the parameters of the proposed project): Modify CIP-003-9 to add security controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications on BES Cyber Systems networks that reside within low-impact assets and Cyber Assets that exist outside of the low-impact asset. Detailed Description: Modify CIP-003-9 to add: • Requirement(s) for authentication of remote users before access is granted to the networks of BES Cyber Systems that are located within low-impact assets. • Requirement(s) for protection of user authentication information in transit for remote access to networks for low-impact BES Cyber Systems located within low-impact assets. • Requirement(s) for detection of malicious communications sent on networks to or from BES Cyber Systems that reside within low-impact assets.	
Likes 0	

Dislikes 0	
Response	
The SDT thanks you for the support of the SAR. The SDT agrees with the issue of overly inclusive scope (i.e., corporate networks) and has modified the SAR to provide better clarity in the 'Detailed Description' section of the SAR and then modified the 'Project Scope' section to refer to it.	
Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	Yes
Document Name	
Comment	
MidAmerican agrees with the proposed scope, but urges NERC to make the clarifications requested in EEI and MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you and see the response to EEI and MRO NSRF comments.	
Kinte Whitehead - Exelon - 1,3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI's response to this question.	

Likes 0	
Dislikes 0	
Response	
See response to EEI comments.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the EEI comments.	
Likes 0	
Dislikes 0	
Response	
See response to EEI comments.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) supports the intent of the proposed scope of the SAR. The proposed enhancements add controls to authenticate remote users and protect information in-transit; however, CEHE is concerned specifically with this bulleted item from the SAR, "*Requirement(s) for detection of malicious communications*	

to/between assets containing low impact BES Cyber Systems with external routable connectivity." This language needs to be clarified. CEHE supports the comments as submitted by the Edison Electric Institute (EEI) as it relates to the proposed language for the "Project Scope" of the SAR.	
Likes 0	
Dislikes 0	
Response	
The SDT agrees with the concern and has made changes to the detection bullet within the SAR. Also, please see responses to EEI comments.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Southern Indiana Gas and Electric Company d/b/a CenterPoint Energy Indiana South (SIGE) would like to thank the SAR Standards Drafting Team for the opportunity to provide feedback on Project 2023-04 – Modifications to CIP-003. SIGE agrees with the proposed scope of the SAR and supports the comments as submitted by the Edison Electric Institute (EEI) as it relates to the proposed language for the "Project Scope" of the SAR.	
Likes 0	
Dislikes 0	
Response	
See response to EEI comments.	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes

Document Name	
Comment	
Duke Energy agrees with the proposed scope and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
See response to EEI's comments.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

EEI supports the intent of the proposed scope of the SAR noting that it closely aligns with the findings of NERC's Low Impact Criteria Review Team (LICRT). While we support this SAR, there are issues that need to be clarified:

1. The LICRT recommendation is limited in scope to communications to and from BES Cyber Systems and while there may be other systems at those locations containing low impact BES Cyber Systems (e.g., corporate communications, etc.), these other assets and their communications should be considered as outside the scope of this SAR.
2. The term external routable connectivity (ERC), as included in the recommendations of this SAR, applies to communications as currently established according to CIP-003, Attachment 1, Section 3.1. Given the term is already defined for medium and high impact BES Cyber Systems, the meaning and how it relates to Low Impact Cyber systems and assets will likely result in confusion without a separate definition. We suggest the SDT define Low Impact ERC.

3. Lastly, the scope of the requirement for the detection of "malicious communications to or between assets containing low impact BES Cyber System with external routable connectivity" should be limited to the detection of external communications to and between facilities containing low impact BES Cyber Systems and not all internal communications within a facility network at a discrete location.

We also suggest that the Project Scope language be modified (bold text) as follows:

Modify CIP-003-9 to add security controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications **to networks** containing low impact BES Cyber Systems **from Cyber Assets outside the assets, for those assets** with external routable connectivity.

Additionally, we suggest that the third bulleted recommendation contained in the Detailed Description section of the SAR include the following modification (bold text) to address our concern regarding the intended scope.

Requirement(s) for detection of malicious communications **sent to or from networks** containing low impact BES Cyber Systems **from Cyber Assets outside the asset, at assets** with external routable connectivity.

Likes 0	
Dislikes 0	

Response

The SDT thanks you for the support.

For point #1, the SDT agrees and has made changes to the SAR to clarify that networks that do not contain BCS are not the intended scope of this effort.

For point #2, the SDT agrees and this issue is included in the SAR as it allows the SDT to create a glossary term if needed.

For point #3, the SDT agrees and similar to point #1, has made modifications to the SAR to clarify the scope is the BCS related communications as described in CIP-003, Attachment 1, Section 3.1.	
Christine Kane - WEC Energy Group, Inc. - 3,4,5,6, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
WEC Energy Group supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
See response to MRO NSRF.	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 1,3,6	
Answer	Yes
Document Name	
Comment	
NextEra Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	

See response to EEI.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	

FirstEnergy agrees with EEI's comments which state:

EEI supports the intent of the proposed scope of the SAR noting that it closely aligns with the findings of NERC's Low Impact Criteria Review Team (LICRT). While we support this SAR, there are issues that need to be clarified:

1. The LICRT recommendation is limited in scope to communications to and from BES cyber systems and while there may be other systems at those locations containing low impact BES Cyber Systems (e.g., corporate communications, etc.), these other assets and their communications should be considered as outside the scope of this SAR.

2. The term external routable connectivity (ERC), as included in the recommendations of this SAR, applies to communications as currently established according to CIP-003, Attachment 1, Section 3.1. Given the term is already defined for medium and high impact BES Cyber Systems, the meaning and how

it relates to Low Impact Cyber systems and assets will likely result in confusion without a separate definition. We suggest the SDT define Low Impact ERC.

3. Lastly, the scope of the requirement for the detection of "malicious communications to or between assets containing low impact BES Cyber System with external routable connectivity" should be limited to the detection of external communications to and between facilities containing low impact BES Cyber Systems and not all internal communications within a facility network at a discrete location.

We also suggest that the Project Scope language be modified (bold text) as follows:

Modify CIP-003-9 to add security controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications assets to networks containing low impact BES Cyber Systems from Cyber Assets outside the assets, for those assets with external routable connectivity. Additionally, we suggest that the third bulleted recommendation contained in the Detailed Description section of the SAR include the following modification (bold text) to address our concern regarding the intended scope. Requirement(s) for detection of malicious communications to/between sent to or from networks assets containing low impact BES Cyber Systems from Cyber Assets outside the asset, at assets with external routable connectivity.	
Likes 0	
Dislikes 0	
Response	
See response to EEI's comments.	
Alan Kloster - Evergy - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) to question #1.	
Likes 0	
Dislikes 0	
Response	
See response to EEI' comments.	
Michelle Amarantos - APS - Arizona Public Service Co. - 1,3,5,6	

Answer	Yes
Document Name	
Comment	

AZPS agrees with and the proposed scope, however we believe that the use of the CIP-002 categorization language "asset that contains a low impact BES Cyber Systems" may lead to confusion. Modifications should only address communications to low impact BCS at an asset. An asset may contain networks or communications unrelated to the low impact BCS. These unrelated networks appear to be within scope with the current language.

We suggest the Project Scope language be modified as follows:

Modify CIP-003-9 to add security controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications at assets containing low impact BES Cyber Systems with external routable connectivity. Modifications will only address communications from outside the asset to low impact BES Cyber Systems with external routable connectivity.

Likes 0	
Dislikes 0	
Response	

The SDT agrees with the concern and has modified the SAR to point to the scope of communications as that already defined in Attachment 1, Section 3.1.

Chantal Mazza - Hydro-Quebec (HQ) - 1 - NPCC	
Answer	Yes
Document Name	
Comment	

While we agree with the overall proposed scope, we offer the following comments as suggested improvements:

The proposed scope depends on the definition of “external routable connectivity” which is not a defined term and is not part of this SAR’s scope. Recommend this SAR’s scope expand by including what “low impact BES Cyber Systems at assets containing those systems that have external routable connectivity” means. A NERC-defined term should be capitalized. In this SAR, every instance of “external routable connectivity” is lowercase which suggests the SAR is not using a defined term. The NERC-defined term depends on ESP. Lows do not have ESPs. Lending more credibility to the conclusion this SAR is not using a defined term. This SAR’s source is the Low Impact Criteria Review Team report which includes “Electronic Access Controls” as a risk which includes “require the implementation of electronic access controls that permit only needed inbound and outbound routable protocol electronic access to the asset containing lows (and thus all individual low impact systems) from anything outside of the asset.” Most CIP-003 interpretations were for the location, not the asset. Both auditors and implementers need a consistent interpretation. What is the boundary? How does one know internal vs external? Request one term with a definition instead of “remote” and “external.” We need clarification of remote/external to what? Consider the impact of “demarcation of” / “asset boundary” in CIP-003 Request clarification of other terms used in CIP-003. Suggest this is an opportunity to consolidate terms and reduce industry confusion User-initiated interactive access (CIP 3 Reference Model 5, concerning Low Impact) Inbound and outbound electronic access (CIP 3, Section 3) Inbound electronic access (CIP 3 Reference Model 5, concerning Low Impact) Indirect access (CIP 3 Reference Model 6,9) Vendor electronic remote access (proposed CIP 3) Lower case “erc” that the SAR proposes Does this include system-to-system? Does this include Interactive Remote Access?

Likes 0	
Dislikes 0	
Response	

The SDT agrees that the issues associated with using ERC-like terminology in regards to assets containing low impact BCS is problematic and should be resolved. The SDT agrees that this connectivity is essentially defined in CIP-003 Attachment 1, Section 3.1. In the future standard drafting efforts, the SDT will consider making that language a different defined term so that it can be used in all the places in which it needs to be referenced and avoid these issues in the future. The SDT appreciates the listing of terms that may need further clarification. In the standards drafting phase, as the SDT makes modifications to CIP-003 to meet the SAR's objectives, it will keep these in mind for the terms that are in our scope of work. The SDT has made modifications to the SAR in the 'Detailed Description' section to clarify the scope of access and communications.	
Lori Frisk - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports the comments provided by Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	Yes
Document Name	
Comment	

While we agree with the overall proposed scope, we offer the following comments as suggested improvements.

The proposed scope depends on the definition of “external routable connectivity” which is not a defined term and is not part of this SAR’s scope. Recommend this SAR’s scope expand by including what “low impact BES Cyber Systems at assets containing those systems that have external routable connectivity” means. A NERC-defined term should be capitalized. In this SAR, every instance of “external routable connectivity” is lowercase which suggests the SAR is not using a defined term. The NERC-defined term depends on ESP. Lows do not have ESPs. Lending more credibility to the conclusion this SAR is not using a defined term. This SAR’s source is the Low Impact Criteria Review Team report which includes “Electronic Access Controls” as a risk which includes “require the implementation of electronic access controls that permit only needed inbound and outbound routable protocol electronic access to the asset containing lows (and thus all individual low impact systems) from anything outside of the asset.” Most CIP-003 interpretations were for the location, not the asset. Both auditors and implementers need a consistent interpretation. What is the boundary? How does one know internal vs external?

Request one term with a definition instead of “remote” and “external.” We need clarification of remote/external to what?
Consider the impact of “demarcation of” / “asset boundary” in CIP-003
Request clarification of other terms used in CIP-003. Suggest this is an opportunity to consolidate terms and reduce industry confusion
User-initiated interactive access (CIP 3 Reference Model 5, concerning Low Impact)
Inbound and outbound electronic access (CIP 3, Section 3)
Inbound electronic access (CIP 3 Reference Model 5, concerning Low Impact)
Indirect access (CIP 3 Reference Model 6,9)
Vendor electronic remote access (proposed CIP 3)
Lower case “erc” that the SAR proposes
Does this include system-to-system? Does this include Interactive Remote Access?

Likes 0	
Dislikes 0	
Response	

See response to Hydro-Quebec above.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
N/A	
Justin Kuehne - AEP - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
N/A	
Karla Weaver - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
N/A	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
N/A	
David Jendras Sr - Ameren - Ameren Services - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
N/A	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
N/A	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	
The proposed scope depends on the definition of “external routable connectivity” which is not a defined term and is not part of this SAR’s scope. Recommend this SAR’s scope expand by including what “low impact BES Cyber Systems at assets containing those systems that have external routable connectivity” means. A NERC-defined term should be capitalized. In this SAR, every instance of “external routable connectivity” is lowercase which suggests the SAR is not using a defined term. The NERC-defined term depends on ESP. Lows do not have ESPs. Lending more credibility to the conclusion this SAR is not using a defined term. This SAR’s source is the Low Impact Criteria Review Team report which includes “Electronic Access Controls” as a risk which includes “require the implementation of electronic access controls	

that permit only needed inbound and outbound routable protocol electronic access to the asset containing lows (and thus all individual low impact systems) from anything outside of the asset." Most CIP-003 interpretations were for the location, not the asset. Both auditors and implementers need a consistent interpretation. What is the boundary? How does one know internal vs external? Request one term with a definition instead of "remote" and "external." We need clarification of remote/external to what? Consider the impact of "demarcation of" / "asset boundary" in CIP-003 Request clarification of other terms used in CIP-003. Suggest this is an opportunity to consolidate terms and reduce industry confusion User-initiated interactive access (CIP 3 Reference Model 5, concerning Low Impact) Inbound and outbound electronic access (CIP 3, Section 3) Inbound electronic access (CIP 3 Reference Model 5, concerning Low Impact) Indirect access (CIP 3 Reference Model 6,9) Vendor electronic remote access (proposed CIP 3) Lower case "erc" that the SAR proposes Does this include system-to-system? Does this include Interactive Remote Access?	
Likes 0	

Dislikes 0	

Response
See response to Hydro-Quebec above.

2. Provide any additional comments for the SAR drafting team to consider, if desired.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC	
Answer	
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
N/A	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	
Document Name	
Comment	
We would like to thank the SDT for allowing us to provide feedback.	
Likes 0	
Dislikes 0	
Response	
Thank you.	

Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	

The current scope wording could require implementation of complex, time-consuming solutions that could negatively impact reliability with minimal security benefit. Adding these specific technical requirements to CIP-003-9 may cause confusion with similar requirements currently included in CIP-005-7 and CIP-007-6. Including these detailed, technical requirements in CIP-003-9 instead of with other ESP controls in CIP-005-7 increases the likelihood of non-compliance because CIP-003-9 is intended to define security management controls at the cyber program level rather than at the detailed technical level.

In addition, we suggest clarification on the Detailed Description to Modify CIP-003-9 to include:

Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.

Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity.

Likes 0	
Dislikes 0	

Response

The SDT agrees with the issues in the Detailed Description section and has made modifications to the SAR to clarify the scope of access and communications. The SDT disagrees that the wording of the technical objectives in the SAR requires implementation of complex solutions that negatively impact reliability. The SDT notes that successful cyber attacks that have impacted reliability around the world were due in part to insufficient remote user authentication. As the SDT enters the standard drafting phase, it will consider the appropriate level of technical detail and requirements that keep it in line with the cyber security plan format of CIP-003.

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	
Document Name	
Comment	
NST suggests the following: New requirement(s) for "protection of user authentication information in transit" should specify what such protections are meant to accomplish, e.g., "confidentiality protection for user authentication information in transit." New requirement(s) for "detection of malicious communications to/between assets" containing low impact BES Cyber Systems" should be "to or from assets containing low impact BES Cyber Systems." The SAR's "Date Submitted" field appears to have a typo.	
Likes 0	
Dislikes 0	
Response	
The SDT agrees with the concerns expressed and will take them into account in the drafting phase. The SDT has made appropriate modifications to the SAR for the scoping of the detection bullet.	

Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
We agree Project 2023-04 (Modifications to CIP-003) impacts 2016-02 (Modifications to CIP Standards) and 2021-03 (CIP-002 Transmission Owner Control Centers). The industry is trying to	

resolve earlier issues from multiple SDTs simultaneously updating CIP Standards. It appears there will likely be significant overlap and possible contradiction in required CIP-002 changes between both the ongoing Project 2016-02 project and the proposed Project 2021-03 projects, we previously recommended that Project 2016-02 completes before Project 2021-03 project proceeds. We extend this recommendation to Projects 2023-04 and 2023-05 (Internal Network Security Monitoring) because CIP Requirements and definitions are deeply intertwined. Correcting one issue has caused issues elsewhere. Multiple projects updating the same Requirements and definitions cost the industry money. Entities invest in implementing the new language. Only to see that investment lost a few months later when another project changes that language – see LERC and LEAP.	
Likes 0	
Dislikes 0	
Response	
Please see response to NPCC RSC.	
Kimberly Turco - Constellation - 5,6	
Answer	
Document Name	
Comment	
Constellation has no additional comments Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	

Response
Thank you.

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	
We agree Project 2023-04 (Modifications to CIP-003) impacts 2016-02 (Modifications to CIP Standards) and 2021-03 (CIP-002 Transmission Owner Control Centers). The industry is trying to resolve earlier issues from multiple SDTs simultaneously updating CIP Standards. It appears there will likely be significant overlap and possible contradiction in required CIP-002 changes between both the ongoing Project 2016-02 project and the proposed Project 2021-03 projects, we previously recommended that Project 2016-02 completes before Project 2021-03 project proceeds. We extend this recommendation to Projects 2023-04 and 2023-05 (Internal Network Security Monitoring) because CIP Requirements and definitions are deeply intertwined. Correcting one issue has caused issues elsewhere. Multiple projects updating the same Requirements and definitions cost the industry money. Entities invest in implementing the new language. Only to see that investment lost a few months later when another project changes that language – see LERC and LEAP.	
Likes 0	
Dislikes 0	
Response	
The SDT appreciates the concern but notes it is not one within the purview of this single SDT and is a topic for NERC and the Standards Committee.	

Chantal Mazza - Hydro-Quebec (HQ) - 1 - NPCC	
Answer	
Document Name	
Comment	
We agree Project 2023-04 (Modifications to CIP-003) impacts 2016-02 (Modifications to CIP Standards) and 2021-03 (CIP-002 Transmission Owner Control Centers). The industry is trying to resolve earlier issues from multiple SDTs simultaneously updating CIP Standards. It appears there will likely be significant overlap and possible contradiction in required CIP-002 changes between both the ongoing Project 2016-02 project and the proposed Project 2021-03 projects, we previously recommended that Project 2016-02 completes before Project 2021-03 project proceeds. We extend this recommendation to Projects 2023-04 and 2023-05 (Internal Network Security Monitoring) because CIP Requirements and definitions are deeply intertwined. Correcting one issue has caused issues elsewhere. Multiple projects updating the same Requirements and definitions cost the industry money. Entities invest in implementing the new language. Only to see that investment lost a few months later when another project changes that language – see LERC and LEAP.	
Likes 0	
Dislikes 0	
Response	
See response to NPCC RSC.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter	
Answer	
Document Name	
Comment	

FirstEnergy seeks the SAR's direction to cross check all existing projects for potential encompassing of standards that may be affected.	
Likes 0	
Dislikes 0	
Response	
See response to similar concern from NPCC RSC.	
Joseph Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy supports the comments of EEI and MRO NSRF	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to those entity's comments.	
Alison MacKellar - Constellation - 5,6	
Answer	
Document Name	
Comment	

N/A Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
BPA suggests adding “Where capable” or “Where technically feasible” to these requirements. Low sites often have the most outdated technology and some of the controls recommended may not be doable at the sites.	
Likes 0	
Dislikes 0	
Response	
The SDT in its drafting phase will take this into consideration but doesn’t think such language is necessary in the SAR.	
Christine Kane - WEC Energy Group, Inc. - 3,4,5,6, Group Name WEC Energy Group	
Answer	
Document Name	
Comment	

WEC Energy Group supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
See response to MRO NSRF.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF does not have any additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Jennie Wike - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6 - WECC, Group Name Tacoma Power	
Answer	
Document Name	
Comment	

Tacoma Power recommends that when developing the CIP-003-X redlines, the SDT should provide additional clarification as to how these changes are different than the work being performed in response to the FERC Order on internal network security monitoring. As currently written in the SAR, it's not clear whether Project 2023-04 will address internal (east-west) or external (north-south) network monitoring. Additionally, the SDT should consider if there's a security benefit to monitoring encrypted communications and if there are benefits, how entities will monitor these encrypted communications.

Likes 0	
Dislikes 0	

Response
The SDT notes that at this time the FERC Order for INSM is scoped to high impact and medium impact w/ERC and should not conflict with lows. As to the North/South vs. East/West traffic question, the SDT has made modifications to the SAR to align the detection component with the already approved Attachment1, Section 3.1 descriptions. The SDT will consider the topic of encryption in the standards drafting phase as it relates to the objectives of the SAR.

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	

Comment
N/A

Likes 0	
Dislikes 0	

Response
N/A

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	
Document Name	
Comment	
ATC requests NERC consider the timing of this SAR alongside the emerging study to evaluate Internal Network Security Monitoring (INSM) for low impact, as well as the inflight effort for 2016-02 to enable for virtualization. Having multiple drafting teams focused on modifications to the same CIP Standard creates potential for confusion and reduces the ability to attain steady state for these regulations. ATC also supports EEI and NSRF comments.	
Likes 1	Tacoma Public Utilities (Tacoma, WA), 1,3,4,5,6, Wike Jennie
Dislikes 0	
Response	
See response to NPCC RSC.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	

Response
Thank you.

Jou Yang - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
The MRO NSRF has concerns with the use term “external routable connectivity” There is already a defined term External Routable Connectivity that applies to high and medium-impact BES Cyber Systems and not to low impact. The term used on this SAR has a different meaning or is applied in a different way than for the defined term. For this reason, the MRO NSRF requests that the drafting team either uses a different term or defines low impact External Routable Connectivity.	
Likes 0	
Dislikes 0	

Response
This SDT agrees and this issue is documented in the current SAR.

Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	
Document Name	
Comment	
MISO supports the comments submitted by the MRO NSRF.	
Likes 0	

Dislikes 0	
Response	
See response to MRO NSRF.	
Jonathan Robbins - AES - AES Corporation - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
N/A	

End of Report

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Coordinated cyber attack controls for low impact BES Cyber Assets		
Date Submitted:	12/20/2022 (Revised 07/25/2023)		
SAR Requester			
Name:	Howard Gugel (LICRT) (Revised by Jeffrey Sweet, Project 2023-04 SDT)		
Organization:	Project 2023-04 Modifications to CIP-003 SDT		
Telephone:	614-716-3059	Email:	jjsweet@aep.com

SAR Type (Check as many as apply)	
☐ New Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10)
☒ Revision to Existing Standard	☐ Variance development or revision
☒ Add, Modify or Retire a Glossary Term	☐ Other (Please specify)
☐ Withdraw/retire an Existing Standard	

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)	
☐ Regulatory Initiation	☐ NERC Standing Committee Identified
☒ Emerging Risk (Reliability Issues Steering Committee) Identified	☐ Enhanced Periodic Review Initiated
☐ Reliability Standard Development Plan	☒ Industry Stakeholder Identified

Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

In light of recent cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact BES Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The report may be found here.

Requested information
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
The LICRT conclusions regarding low impact BES Cyber Systems are as follows: • Individually, low impact BES Cyber Systems are truly low impact to BES reliability. This corresponds to the longstanding work of NERC and the stakeholders to design and operate the BES to withstand the loss of any of its individual assets. A medium or high impact BES Cyber System is more than an impact to a typical single BES Element/Facility. Therefore, the team does not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems. • The team recognizes that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The team recommends enhancing the existing low impact category to further mitigate the coordinated attack risk.
Project Scope (Define the parameters of the proposed project):
Modify CIP-003-9 to add controls as outlined in the Detailed Description section below.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):
Modify CIP-003-9 to add: • Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems using a routable protocol from outside the asset containing low impact BES Cyber Systems. • Requirement(s) for protection of user authentication information in transit for remote access to networks containing low impact BES Cyber Systems using a routable protocol from outside the asset containing low impact BES Cyber Systems. • Requirement(s) for detection of known or suspected malicious communications for both inbound and outbound electronic access as defined in CIP-003-9 Attachment 1, Section 3.1. To limit the scope of the requirements to only those that have external routable connectivity, the drafting team may need to create a new defined term or modify an existing defined term. For a complete technical justification and technical foundation, please refer to the Low Impact Criteria Review Report.

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impacts are unknown at this time.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
None
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator, Transmission Owner
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
The white paper was developed by industry experts and posted for industry comment prior to being presented to the Board.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
If not completed by the initiation of this SAR: 2016-02 Modifications to CIP Standards 2021-03 CIP-002 Transmission Owner Control Centers
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Reliability Principles	
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
e.g., NPCC	none

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☒ Draft SAR reviewed by NERC Staff ☒ Draft SAR presented to SC for acceptance ☒ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised

1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Coordinated cyber attack controls for low impact BES Cyber Assets		
Date Submitted:	12/20/2022 **(Revised 07/25/2023)**		
SAR Requester			
Name:	Howard Gugel (LICRT) **(Revised by Jeffrey Sweet, Project 2023-04 SDT)**		
Organization:	~~NERC~~**Project 2023-04 Modifications to CIP-003 SDT**		
Telephone:	~~404-446-9693~~**614-716-3059**	Email:	~~Howard.gugel@nerc.net~~**jjsweet@aep.com**

SAR Type (Check as many as apply)	
☐ New Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10)
☒ Revision to Existing Standard	☐ Variance development or revision
☒ Add, Modify or Retire a Glossary Term	☐ Other (Please specify)
☐ Withdraw/retire an Existing Standard	

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)	
☐ Regulatory Initiation	☐ NERC Standing Committee Identified
☒ Emerging Risk (Reliability Issues Steering Committee) Identified	☐ Enhanced Periodic Review Initiated
☐ Reliability Standard Development Plan	☒ Industry Stakeholder Identified

Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

In light of recent cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact BES Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The report may be found here.

Requested information
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
The LICRT conclusions regarding low impact BES Cyber Systems are as follows: • Individually, low impact BES Cyber Systems are truly low impact to BES reliability. This corresponds to the longstanding work of NERC and the stakeholders to design and operate the BES to withstand the loss of any of its individual assets. A medium or high impact BES Cyber System is more than an impact to a typical single BES Element/Facility. Therefore, the team does not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems. • The team recognizes that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The team recommends enhancing the existing low impact category to further mitigate the coordinated attack risk.
Project Scope (Define the parameters of the proposed project):
Modify CIP-003-9 to add controls ~~to authenticate remote users, protect the authentication information in transit, and detect malicious communications assets~~ ~~containing low impact BES Cyber Systems with external routable connectivity.~~**as outlined in the Detailed Description section below.**
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):
Modify CIP-003-9 to add: • Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems ~~at assets containing those systems that have external~~**using a** routable ~~connectivity~~**protocol from outside the asset containing low impact BES Cyber Systems**. • Requirement(s) for protection of user authentication information in transit for remote access to **networks containing** low impact BES Cyber Systems ~~at assets containing those systems that have external~~**using a** routable ~~connectivity~~**protocol from outside the asset containing low impact BES Cyber Systems**. • Requirement(s) for detection of **known or suspected** malicious communications ~~to/between assets containing low impact BES Cyber Systems with external routable connectivity~~**for both inbound and outbound electronic access as defined in CIP-003-9 Attachment 1, Section 3.1**. To limit the scope of the requirements to only those that have external routable connectivity, the

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
drafting team may need to create a new defined term or modify an existing defined term. For a complete technical justification and technical foundation, please refer to the Low Impact Criteria Review Report.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impacts are unknown at this time.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
None
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator, Transmission Owner
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
The white paper was developed by industry experts and posted for industry comment prior to being presented to the Board.
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?
If not completed by the initiation of this SAR: 2016-02 Modifications to CIP Standards 2021-03 CIP-002 Transmission Owner Control Centers
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Reliability Principles	
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
e.g., NPCC	none

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐☒ Draft SAR reviewed by NERC Staff	☐ Final SAR endorsed by the SC
☐☒ Draft SAR presented to SC for acceptance	☐ SAR assigned a Standards Project by NERC
☐☒ DRAFT SAR approved for posting by the SC	☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the first draft of the proposed standard for a formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023

Anticipated Actions	Date
45-day formal comment period with ballot	October 24 – December 7, 2023
45-day formal or informal comment period with additional ballot	February – March 2024
10-day final ballot	April 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

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

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

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

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

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

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

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

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

5. Effective Dates: See Implementation Plan for CIP-003-A.

B. Requirements and Measures

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

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

1.1.1. Personnel and training (CIP-004);

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

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

1.1.4. System security management (CIP-007);

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

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

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

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

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

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

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

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

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

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

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

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

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

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

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

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

C. Compliance

1. Compliance Monitoring Process

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

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

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

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

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

Violation Severity Levels

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2)	cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2)	cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2)	security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the seven topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR	Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls, but failed to implement one or two controls listed in Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR	implement three or more controls listed in Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR	

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)	
R3.	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from

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

Version	Date	Action	Change Tracking
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
A	TBD	Adopted by the NERC Board of Trustees.	TBD

Attachment 1

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

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

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

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

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented in Section 3.1.1, if any.

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

3.1 For connectivity that provides the ability to communicate:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

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

3.1.1 Permit only necessary inbound and outbound electronic remote access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic remote access;

3.1.3 Authenticate users when permitting each instance of electronic remote access to networks containing low impact BES Cyber Systems;

3.1.4 Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems;

3.1.5 Determine vendor electronic remote access, where vendor electronic remote access is permitted; and

3.1.6 Disable vendor electronic remote access, where vendor electronic remote access is permitted.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

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

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

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

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

4.4 Incident handling for Cyber Security Incidents;

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

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

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

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

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

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible

Entity, if any:

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

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

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

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

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Attachment 2

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

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

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

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

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

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

1. For Section 3.1.1, documentation showing routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic remote access that the Responsible Entity deems necessary, except where these communications are time-sensitive protection or control functions between Protection Systems, such as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
   - Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional

gateways); or

- Original Equipment Manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications, such as:
    - Anti-malware technologies;
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - Automated or manual log reviews;
    - Alerting; or
    - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate users when permitting each instance of electronic remote access to networks containing low impact BES Cyber Systems, such as:
    - Authentication mechanism(s) including but not limited to:
        - Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or
        - Enforcement of Multi-Factor Authentication (MFA).
    - Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters; or
    - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems, such as:
    - Protection mechanism(s) including but not limited to:
        - Implementation of an encrypted protocol or service (Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH), etc.); or
        - Implementation of an IPsec or Secure Sockets Layer (SSL) VPN.
    - Other operational, procedural, or technical controls.
5. For Section 3.1.5 documentation showing the ability to determine vendor remote access, such as:
    - Steps to preauthorize access;
    - Alerts generated by vendor log on;
    - Session monitoring;
    - Security information management logging alerts;

- Time-of-need session initiation;
- Session recording;
- System logs; or
- Other operational, procedural, or technical controls.

6. For Section 3.1.6, documentation showing the ability to disable vendor electronic remote access, such as:
    - Disabling vendor electronic remote access user or system accounts;
    - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
    - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;
    - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
    - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
    - Other operational, procedural, or technical controls.

7. For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

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

5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

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

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

   Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.
3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented

confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the first draft of the proposed standard, for a formal 45-day comment period.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023

Anticipated Actions	Date
45-day formal comment period with ballot	October 24 – December 7, 2023
45-day formal or informal comment period with additional ballot	February – March 2024
10-day final ballot	April 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

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

2. **Number:** CIP-~~003-9~~003-A

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

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

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

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

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

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

5. Effective Dates: See Implementation Plan for CIP-~~003-9~~003-A.

B. Requirements and Measures

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

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

1.1.1. Personnel and training (CIP-004);

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

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

1.1.4. System security management (CIP-007);

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

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

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

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

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

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

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

~~**1.2.6.** Vendor electronic remote access security controls; and~~

1.2.6. ~~**1.2.7.**~~ Declaring and responding to CIP Exceptional Circumstances.

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

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

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

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

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

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

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

C. Compliance

1. **Compliance Monitoring Process**

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

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

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

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

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

Violation Severity Levels

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

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-003-9)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact	as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-003-9)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented	BES Cyber Systems, but did not address two of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented	BES Cyber Systems, but did not address three of the seven topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented	four or more of the seven topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-003-9)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1.2)	the previous approval. (R1.2)
R2	~~Operations Planning~~	~~Lower~~	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2,	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2)	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-~~003-9~~A)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity implemented all electronic access controls, but failed to document ~~its cyber security plan(s) for~~the electronic access controls according to Requirement R2, Attachment 1, Section ~~3.~~ 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section ~~4.~~ 4. (R2) OR The Responsible Entity documented one or	Attachment 1, Section ~~1.~~1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section ~~2.~~2. (R2) ~~OR~~ ~~The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)~~	OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to ~~permit only necessary inbound and outbound electronic access~~implement three or more controls ~~according to~~listed in Requirement R2, Attachment 1, Section ~~3.1~~3. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber	

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-003-9)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR	OR The Responsible Entity documented its cyber security plan(s) for electronic access controls, but failed to implement ~~authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to~~one or two controls listed in Requirement R2, Attachment 1, Section ~~3.2~~3. (R2) ~~OR~~ OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for	Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its	

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

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-003-9)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Section 4. (R2) ~~OR~~ OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR	according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed ~~to document according to Requirement R2, Attachment 1, Section 5.2. (R2)~~ ~~OR~~ ~~The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed~~ to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section	

					5.3. (R2)- ~~OR~~ ~~The Responsible Entity failed to document and implement its cyber security process for vendor electronic~~	
				The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document		

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-003-9)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR ~~mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2)~~ ~~OR~~ The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement	~~remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)~~	

				the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) ~~OR~~ ~~The Responsible Entity documented its cyber security process for vendor electronic~~		

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-003-9)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)~~		
R3	~~Operations Planning~~	~~Medium~~	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	~~Operations Planning~~	~~Lower~~	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from

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

Version	Date	Action	Change Tracking
9	~~TBD~~11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
A	TBD	Adopted by the NERC Board of Trustees.	TBD

Attachment 1

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

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

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

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

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented ~~for~~in Section ~~3.1~~3.1.1, if any.

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

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

3.1 For connectivity that provides the ability to communicate:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

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

3.1.1 Permit only necessary inbound and outbound electronic remote access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic remote access;

3.1.3 Authenticate users when permitting each instance of electronic remote access to networks containing low impact BES Cyber

Systems;

3.1.4 Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems;

3.1.5 Determine vendor electronic remote access, where vendor electronic remote access is permitted; and

3.1.6 Disable vendor electronic remote access, where vendor electronic remote access is permitted.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

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

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

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

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

4.4 Incident handling for Cyber Security Incidents;

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

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

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

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

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

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

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

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;

- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

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

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

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

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

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

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

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

Attachment 2

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

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

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

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

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section ~~3.1~~3.1.1, if any.

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

1. ~~Documentation~~For Section 3.1.1, documentation showing ~~that at each asset or group of assets containing low impact BES Cyber Systems,~~ routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic remote access that the Responsible Entity deems necessary, except where ~~an entity provides rationale that communication is used for time-sensitive~~these communications are time-sensitive protection or control functions between ~~intelligent electronic devices. Examples of such documentation may include, but are not limited to representative~~ Protection Systems, such as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact

BES Cyber System(s)~~ or lists~~ ;

- Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways)~~.~~; or

- Original Equipment Manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications, such as:
   - Anti-malware technologies;
   - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
   - Automated or manual log reviews;
   - Alerting; or
   - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate users when permitting each instance of electronic remote access to networks containing low impact BES Cyber Systems, such as:
   - Authentication mechanism(s) including but not limited to:
     - Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or
     - Enforcement of Multi-Factor Authentication (MFA).
   - Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters; or
   - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems, such as:
   - Protection mechanism(s) including but not limited to:
     - Implementation of an encrypted protocol or service (Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH), etc.); or
     - Implementation of an IPsec or Secure Sockets Layer (SSL) VPN.
   - Other operational, procedural, or technical controls.
5. For Section 3.1.5 documentation showing the ability to determine vendor remote access, such as:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;
   - Security information management logging alerts;
   - Time-of-need session initiation;

- Session recording;
- System logs; or
- Other operational, procedural, or technical controls.

6. For Section 3.1.6, documentation showing the ability to disable vendor electronic remote access, such as:
    - Disabling vendor electronic remote access user or system accounts;
    - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
    - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;
    - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
    - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
    - Other operational, procedural, or technical controls.

7. ~~2. Documentation~~For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

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

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

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

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

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

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

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

~~1. For Section 6.1, documentation showing:~~

- ~~steps to preauthorize access;~~
- ~~alerts generated by vendor log on;~~
- ~~session monitoring;~~
- ~~security information management logging alerts;~~
- ~~time-of-need session initiation;~~
- ~~session recording;~~
- ~~system logs; or~~
- ~~other operational, procedural, or technical controls.~~

~~2. For Section 6.2, documentation showing:~~

- ~~disabling vendor electronic remote access user or system accounts;~~

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

~~3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:~~

- ~~Anti-malware technologies;~~
- ~~Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);~~
- ~~Automated or manual log reviews;~~
- ~~alerting; or~~
- ~~other operational, procedural, or technical controls.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-04 Modifications to CIP-003
Reliability Standard CIP-003-A

Applicable Standard(s)

- CIP-003-A – Cyber Security – Security Management Controls

Requested Retirement(s)

- CIP-003-9 – Cyber Security – Security Management Controls

Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

New/Modified/Retired Terms in the NERC Glossary of Terms

- None

Background

Project 2023-04 addresses modifications to CIP-003-9 in response to recommendations from the Low Impact Criteria Review Team (LICRT), which was formed by the NERC Board of Trustees to consider the potential threat and risk posed by a coordinated cyber-attack on low impact Bulk Electric System (BES) Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommended actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the standard authorization request (SAR) at its March

22, 2023 meeting. In response to the SAR, Project 2023-04 proposes merging Sections 3 and 6 of Attachment 1 to consolidate all electronic access, with sub-sections providing additional requirements based on the type of access (Vendor, dial-up, local, etc.).

General Considerations

This implementation plan provides entities with thirty-six (36) months to become compliant with the revised Reliability Standard. This implementation plan reflects the following considerations for entities to implement the new controls of Requirement R2, Attachment 1:

- Revise cyber security policy, plan, and procedures.
- Hire and train new staff to implement the new cyber security controls.
- Reconfigure system, network, or security architectures.
- Purchase and procurement of new technology(s).
- Install new technology(s) at all assets containing low impact BES Cyber Systems.
- The effective date of CIP-003-9 is April 1, 2026. The cyber security controls implemented with CIP-003-A do not conflict and build upon the implementation of CIP-003-9 for vendor electronic remote access.

Effective Date

Reliability Standard CIP-003-A

Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and Responsible Entities shall comply initially with those periodic requirements in CIP-003-A as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.3 on or before the effective date of CIP-003-A. Responsible Entities shall initially comply with all other periodic requirements in CIP-003-A within the periodic timeframes of their last performance under CIP-003-9.

Retirement Date

Reliability Standard CIP-003-9

Reliability Standard CIP-003-9 shall be retired immediately prior to the effective date of CIP-003-A in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard
CIP-003-9 – Low Impact BES Cyber Security Criteria Revisions

Introduction
This document is the technical rationale and justification for Reliability Standard CIP-003-A and includes the rationale for changes in the current proposed version, as well as previous versions of the standard.

It is intended to provide stakeholders and the ERO Enterprise with an understanding of the revisions, technology and technical concepts of Reliability Standard CIP-003-9. This is not a Reliability Standard and should not be considered mandatory and enforceable.

Background
In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact Bulk Electric System (BES) Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts, representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber-attack on low impact BES Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the Standard Authorization Request (SAR) at its March 22, 2023 meeting.

The LICRT conclusions regarding low impact BES Cyber Systems are as follows:

- Individually, low impact BES Cyber Systems are truly low impact to BES reliability. This corresponds to the longstanding work of NERC and the stakeholders to design and operate the BES to withstand the loss of any of its individual assets. A medium or high impact BES Cyber System is more than an impact to a typical single BES Element/Facility. Therefore, the team does not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems.
- The team recognizes that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The team recommends enhancing the existing low impact category to further mitigate the coordinated attack risk.

Those LICRT report recommendations are as follows:

- Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity.

Rationale for Attachment 1, Section 3 and Section 6

The Standard Drafting Team's (SDT's) review of the SAR and industry comment initiated a discussion of where the requirements would reside within CIP-003-9. CIP-003-9 was used as the baseline for revisions, since this version is the most recent version approved by FERC. Attachment 1, Section 3 and Attachment 1, Section 6 were identified as ideal locations to integrate the requirements due to their focus on Electronic Access Controls and Vendor Electronic Remote Access Security Controls. The SDT investigated two options:

Option A: Modify Sections 3 and 6; integrating the requirements, but keeping the sections separate
Option B: Merge Sections 3 and 6

The SDT agreed to Option B: Merge Sections 3 and 6. The following rationale was used to support the decision:

1. Merging Section 3 and Section 6 would present a single section for all electronic access with sub-sections providing additional requirements based on the type of access (Vendor, dial-up, local, etc.)
2. Section 6 has not been implemented or required by industry at this time and therefore there would be no impact to merging it with Section 3

While merging Section 3 and 6, the SDT made conforming changes to the language. The SDT uses the phrase "implement controls" to replace "implement a process" or "implement one or more method(s)". The SDT believes a "control" can include an operation, process, procedure, technology as described in the examples of Attachment 2.

Glossary Terms

The SDT also discussed the potential resurrection of the retired NERC Glossary Term: LERC, Low Impact External Routable Connectivity, or creating a new Glossary Term. The rationale for using LERC or a new Glossary Term would be to provide a shorthand way of discussing external routable connectivity when dealing with low impact assets. LERC was initially created by the Project 2014-02 SDT in response to FERC Order 791. FERC Order 822 approved the term but with a directive to address an issue within the definition of the term in 12 months. Project 2016-02 was formed to address the issue and choose to retire the term and integrate the language into Attachment 1, Section 3.1. LERC was only in use between its approval on July 1, 2016 through its retirement on December 31, 2019.

The SDT decided to retain existing CIP-003-9 Section 3.1 rather than resurrect LERC term or create a new Glossary Term. Rationale used for the decision:

1. Possible confusion with reviving LERC
2. Possible friction with stakeholders with creating/using a non-standard/new term
3. The concept of LERC is currently not used outside of CIP-003-A, Section 3

Section 3.1

The objective of Section 3.1 is to maintain the original language used in CIP-003-9, Section 3.1, Subsections (i) - (iii). There is one revision to 3.1(iii) replacing the protocol language with reference to "Protection Systems", which is a conforming change made by Project 2016-02, CIP-003-Y.

Section 3.1.1

The objective of Section 3.1.1 is to maintain the original language used in CIP-003-9, Section 3.1.

Section 3.1.2

This is an expanded cyber security control outlined in the SAR. The scope is expanded from CIP-003-9, Section 6.3 to include all communications rather than vendor specific communications. The objective of Attachment 1 Section 3.1.2 is for entities to mitigate the risk posed by malicious communications to or from low impact BES Cyber Systems. The obligation in Section 3.1.2 requires that entities implement controls to detect known or suspected inbound and outbound malicious communications between a low impact BES Cyber System and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s).

Section 3.1.3

This is a new cyber security control outlined in the SAR, which requires entities to implement controls to authenticate users when permitting (allowing) each instance of electronic remote access to networks containing low impact BES Cyber Systems. This intention of "each instance" phrase is meant to include the initial authorization and all subsequent re-connection instances of electronic remote access to the network. If there is a collection of sub-networks or Cyber Assets within the network containing low impact BES Cyber Systems, then multiple re-authentications would not be required. This control mitigates the risk of unauthenticated user access.

Section 3.1.4

This is a new cyber security control outlined in the SAR. The objective of Attachment 1, Section 3.1.4 is for entities to have the ability to protect the user authentication information (username, password, multi-factor authentication (MFA) information, session token, etc.) between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s). This protection mitigates the unintended disclosure of authentication information for remote access of low impact cyber systems.

Section 3.1.5

The objective of Section 3.1.5 is to maintain the original language used in CIP-003-9, Section 6.1. One or more method(s) can be identified as part of this electronic access control. Entities must determine vendor electronic remote access, where permitted, to their low impact BES Asset(s) and/or BES Cyber Systems.

Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access.

Section 3.1.6
The objective of Section 3.1.6 is to maintain the original language used in CIP-003-9, Section 6.2. One or more method(s) can be identified as part of this electronic access control. Entities must have the ability to disable vendor electronic remote access, where permitted, for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing low impact BES Cyber Systems.

Section 3.2
The objective of Section 3.2 is to maintain the original language used in CIP-003-9, Section 3.2.

Rationale for Attachment 2

The SDT made conforming changes to Attachment 2 merging Sections 3 and 6, and providing examples of compliance related activities.

Previous CIP-003 Versions Technical Rationale

Project 2020-03 Supply Chain Low Impact Revisions (CIP-003-9) Technical Rationale

Project 2016-02 Modifications to CIP Standards (CIP-003-Y) Technical Rationale

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2023-04 Modifications to CIP-003

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on draft one of Reliability Standard **CIP-003-A – Cyber Security – Security Management Controls** by **8 p.m. Eastern, Thursday, December 7, 2023.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Chris Larson (via email), or at 404-446-9708.

Background

In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact Bulk Electric System (BES) Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the Standard Authorization Request (SAR) at its March 22, 2023 meeting.

The LICRT report recognized that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The team recommended enhancing the existing low impact category to further mitigate the coordinated attack risk. The proposed project will revise CIP-003-9 to add electronic access controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications for assets containing low impact BES Cyber Systems with external routable connectivity.

Please provide your responses to the questions listed below, along with any detailed comments.

Questions

1. Do you agree with the language proposed in CIP-003-A Attachment 1? If you do not agree, please provide recommended language you would support and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

2. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please provide recommended language you would support and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

3. The Standard Drafting Team (SDT) proposes a three (3) year implementation plan for CIP-003-A. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.

   ☐ Yes
   ☐ No

   Comments:

4. The SDT believes the language of CIP-003-A addresses the issues outlined in the SAR in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

5. Provide any additional comments on the standard and technical rationale for the SDT to consider, if desired.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2023-04 Modifications to CIP-003

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2023-04 Modifications to CIP-003. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

Justification for VRFs and VSLs

- Requirement R1: The VRF and VSLs did not change from the previously FERC-approved CIP-003-9 Reliability Standard.
- Requirement R2: The VRF did not change from the previously FERC-approved CIP-003-9 Reliability Standard. VSL changes are outlined below.
- Requirement R3: The VRF and VSLs did not change from the previously FERC-approved CIP-003-9 Reliability Standard.
- Requirement R4: The VRF and VSLs did not change from the previously FERC-approved CIP-003-9 Reliability Standard.

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented all electronic access controls, but failed to document the electronic access	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems,	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment	but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls, but failed to implement one or two controls listed in Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2)	containing low impact BES Cyber Systems, but failed to implement three or more controls listed in Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2)	

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

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)	

VSL Justifications for CIP-003-A, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSLs for Requirement R2 are similar to the previous VSLs of CIP-003-9, with a few revisions. Created Moderate and High VSL based on the number of controls implemented. Removed mentions of Attachment 1, Section 6, since Section 6 was merged with Section 3.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Requirement R2 is not a "binary" type requirement. Violation severity levels are clear, quantitative, and non-ambiguous.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The VSL level assignments are consistent with language in Requirement R2 and Attachment 1.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The violation severity levels relate to a single violation. A failure to do multiple portions of Requirement R2, Attachment 1 is considered a single violation.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form

Project 2023-04 Modifications to CIP-003 Standard Drafting Team

Do not use this form for submitting nominations. Use the electronic form to submit nominations for **Project 2023-04 Modifications to CIP-003** Standard Drafting Team (SDT) members by **8 p.m. Eastern, Thursday, December 7, 2023**. This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form.

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Chris Larson (via email), or at 470-599-3851.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls. Previous drafting or review team experience is beneficial, but not required.

Project Information

Project Purpose

In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact BES Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the SAR at its March 22, 2023 meeting.

The LICRT report recognized that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The team recommended enhancing the existing low impact category to further mitigate the coordinated attack risk. The proposed project will revise CIP-003-9 to add controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications assets containing low impact BES Cyber Systems with external routable connectivity.

Standard(s) affected: CIP-003-9

Nominee Expertise Requested

NERC is seeking individuals who possess experience in the following areas:

- Effective communication, technical writing, negotiation, and facilitation
- Experience with CIP-003-9 and Cyber Security Management Controls
- Understanding of BES Cyber Asset Low Impact criteria
- Understanding of reliability risks associated with BES Cyber Assets and BES Cyber Systems
- Understanding of coordinated attack risks and mitigation options
- Understanding of external routable connectivity (ERC)
- Understanding of authentication for remote users
- Understanding of protection of user authentication information
- Understanding of detection of malicious communications
- Responsible entity compliance related to the areas listed above

Time Commitment Expectations

Time commitments for most projects include up to two face-to-face meetings per quarter (on average two full working days each meeting) with conference calls scheduled as needed. Team members can agree to individual or subgroup assignments, hold separate meetings, and present to the full drafting team for discussion and review. Another important component of quality reviews and drafting team efforts is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful project outcome.

Project Priority

Each project will be developed according to that project's priority status. While each standard project addresses particular industry needs, some will be identified as a higher priority. A higher priority project can include a strict timeline, which may be needed to effectively respond to a FERC Directive or other factors determined by the NERC Board of Trustees. A higher priority project may also need to increase the frequency of meetings at any time throughout the development process to account for project timeline needs. Similarly, lower priority projects may adjust to less frequent meetings to reallocate resources to high priority projects.

This project has been identified as higher priority at this time.

Name:	
Organization:	

Address:	
Telephone:	
Email:	

Please briefly describe your experience and qualifications to serve on the requested SAR Drafting Team (Bio):

If you are currently a member of any NERC drafting team, please list each team here:

☐ Not currently on any active SAR or standard drafting team.

☐ Currently a member of the following SAR or standard drafting team(s):

If you previously worked on any NERC drafting team please identify the team(s):

☐ No prior NERC SAR or standard drafting team.

☐ Prior experience on the following team(s):

Acknowledgement that the nominee has read and understands both the *NERC Participant Conduct Policy* and the *Standard Drafting Team Scope* documents, available on NERC Standards Resources.

☐ Yes, the nominee has read and understands these documents.

Select each NERC Region in which you have experience relevant to the Project for which you are volunteering:

☐ MRO ☐ NPCC ☐ RF	☐ SERC ☐ Texas RE ☐ WECC	☐ NA – Not Applicable

Select each Industry Segment that you represent:

☐	1 — Transmission Owners
☐	2 — RTOs, ISOs
☐	3 — Load-serving Entities
☐	4 — Transmission-dependent Utilities
☐	5 — Electric Generators

☐	6 — Electricity Brokers, Aggregators, and Marketers
☐	7 — Large Electricity End Users
☐	8 — Small Electricity End Users
☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
☐	10 — Regional Reliability Organizations and Regional Entities
☐	NA – Not Applicable

Select each Function[1] in which you have current or prior expertise:	
☐ Balancing Authority	☐ Transmission Operator
☐ Compliance Enforcement Authority	☐ Transmission Owner
☐ Distribution Provider	☐ Transmission Planner
☐ Generator Operator	☐ Transmission Service Provider
☐ Generator Owner	☐ Purchasing-selling Entity
☐ Interchange Authority	☐ Reliability Coordinator
☐ Load-serving Entity	☐ Reliability Assurer
☐ Market Operator	☐ Resource Planner
☐ Planning Coordinator	

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group:			
Name:		Telephone:	
Organization:		Email:	
Name:		Telephone:	
Organization:		Email:	

Provide the name and contact information of your immediate supervisor or a member of your management who can confirm your organization's willingness to support your active participation.			
Name:		Telephone:	
Title:		Email:	

[1] These functions are defined in the NERC Functional Model, which is available on the NERC web site.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-04 Modifications to CIP-003

Nomination Period Open through December 7, 2023

Now Available

Nominations are being sought for **Project 2023-04 Modifications to CIP-003** Standard Drafting Team (SDT) supplemental members through **8 p.m. Eastern, Thursday, December 7, 2023.**

Use the electronic form to submit a nomination. Contact Cindy Jackson regarding issues using the electronic form. An unofficial Word version of the nomination form is posted on the Standard Drafting Team Vacancies page and the project page.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

The time commitment for this project is expected to be up to two face-to-face meetings per quarter (on average two full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the review or drafting team sets forth. Team members may also have side projects, either individually or by subgroup, to present to the larger team for discussion and review. Lastly, an important component of the review and drafting team effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful project outcome.

NERC is seeking individuals from organizations who possess experience with CIP-003 Security Management Controls including Generator Owner/Operator, Reliability Coordinator, Balancing Authority, Transmission Owner/Operator, and Distribution Provider.

Previous drafting team experience is beneficial but not required. See the project page and nomination form for additional information.

Next Steps

The Standards Committee is expected to appoint supplemental SDT members in January 2024. Nominees will be notified shortly after they have been appointed.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Chris Larson (via email) or at 470-599-3851. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003 observer list” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-04 Modifications to CIP-003

Formal Comment Period Open through December 7, 2023
Ballot Pools Forming through November 27, 2023

Now Available

A 45-day formal comment period for draft one of **CIP-003-A – Cyber Security – Security Management Controls**, is open through **8 p.m. Eastern, Thursday, December 7, 2023.**

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Monday, November 27, 2023.** Registered Ballot Body members can join the ballot pools here.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An initial ballot for the standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **November 28 – December 7, 2023**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Chris Larson (via email) or at 404-446-9708. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003 observer list” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2023-04 Modifications to CIP-003 | Draft 1
Comment Period Start Date:	10/24/2023
Comment Period End Date:	12/7/2023
Associated Ballots:	2023-04 Modifications to CIP-003 CIP-003-A IN 1 ST 2023-04 Modifications to CIP-003 Implementation Plan IN 1 OT

There were 63 sets of responses, including comments from approximately 165 different people from approximately 104 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the language proposed in CIP-003-A Attachment 1? If you do not agree, please provide recommended language you would support and, if appropriate, technical or procedural justification.

2. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please provide recommended language you would support and, if appropriate, technical or procedural justification.

3. The Standard Drafting Team (SDT) proposes a three (3) year implementation plan for CIP-003-A. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.

4. The SDT believes the language of CIP-003-A addresses the issues outlined in the SAR in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

5. Provide any additional comments on the standard and technical rationale for the SDT to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Jaimin Patal	Saskatchewan Power Corporation (SPC)	1	MRO
					Kimberly Bentley	Western Area Power Adminstration	1,6	MRO
					Marc Gomez	Southwestern Power Administration (SWPA)	1	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO
					George Brown	Pattern Operators LP	5	MRO
					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Bryan Sherrow	Board Of Public Utilities (BPU)	1	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Michael Ayotte	ITC Holdings	1	MRO

Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC
					Nehtisha Rollis	Tennessee Valley Authority	5	SERC
Chris Carnesi	Chris Carnesi		WECC	NCPA	Marty Hostler	Northern California Power Agency	4	WECC
					Dennis Sismaet	Northern California Power Agency	6	WECC
WEC Energy Group, Inc.	Christine Kane	3		WEC Energy Group	Christine Kane	WEC Energy Group	3	RF
					Matthew Beilfuss	WEC Energy Group, Inc.	4	RF
					Clarice Zellmer	WEC Energy Group, Inc.	5	RF
					David Boeshaar	WEC Energy Group, Inc.	6	RF
Manitoba Hydro	Jay Sethi	1,3,5,6	MRO	Manitoba Hydro Group	Nazra Gladu	Manitoba Hydro	1	MRO
					Mike Smith	Manitoba Hydro	3	MRO
					Kristy-Lee Young	Manitoba Hydro	5	MRO
					Kelly Bertholet	Manitoba Hydro	6	MRO
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC

					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Nikki Carson-Marquis	Minnkota Power Cooperative, Inc.	1	MRO
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
Eversource Energy	Joshua London	1		Eversource	Joshua London	Eversource Energy	1	NPCC
					Vicki O'Leary	Eversource Energy	3	NPCC
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Alain Mukama	Hydro One Networks, Inc.	1	NPCC

Deidre Altobell	Con Edison	1	NPCC
Jeffrey Streifling	NB Power Corporation	1	NPCC
Michele Tondalo	United Illuminating Co.	1	NPCC
Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
Randy Buswell	Vermont Electric Power Company	1	NPCC
James Grant	NYISO	2	NPCC
John Pearson	ISO New England, Inc.	2	NPCC
Harishkumar Subramani Vijay Kumar	Independent Electricity System Operator	2	NPCC
Randy MacDonald	New Brunswick Power Corporation	2	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
David Burke	Orange and Rockland	3	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
David Kwan	Ontario Power Generation	4	NPCC

					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Sean Cavote	PSEG	4	NPCC
					Jason Chandler	Con Edison	5	NPCC
					Tracy MacNicoll	Utility Services	5	NPCC
					Shivaz Chopra	New York Power Authority	6	NPCC
					Vijay Puran	New York State Department of Public Service	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					Joshua London	Eversource Energy	1	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Steve Toosevich	Steve Toosevich			NIPSCO Compliance	Steven Taddeucci	NiSource - Northern Indiana Public Service Co.	3	RF

					Kathryn Tackett	NiSource - Northern Indiana Public Service Co.	5	RF
					Joseph OBrien	NiSource - Northern Indiana Public Service Co.	6	RF
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC

					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. Do you agree with the language proposed in CIP-003-A Attachment 1? If you do not agree, please provide recommended language you would support and, if appropriate, technical or procedural justification.

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	

Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting.

PNMR also supports EEI's comments pertaining to Section 3, parts 3.1.4 and 3.1.6.

Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	

Regarding the definition of 3.1's scope, the specification of "connectivity that provides the ability to communicate" is confusing and has no opposite state; connectivity in this context implies communication. The addition of "of Protection systems" to iii is also unnecessarily expansive. Language recommendation:

3.1 For routable connectivity:

I. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving a defined perimeter containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., IEC 61850, etc.)

Regarding section 3.1.2, that subsection implies deployment of Intrusion Protection Systems (IPS) at every low impact BES Cyber System for any "connection to communicate". This is technically infeasible for many communication types (e.g., RS-232, RS-485, non-IP IEC 61850, etc.). It would necessitate building routable connectivity to many systems that otherwise do not require it, do not have it, and may be difficult or expensive to build out (see cost feasibility below) simply to deploy a monitoring solution. The added communication risk combined with cost is not an effective risk-based approach to securing low impact BES.

Regarding section 3.1.4, this requirement is overly prescriptive and makes certain assumptions about how connections for communications may be authorized, secured, and used. The requirement should address a security concern topically – e.g. “ensure communications are protected appropriately given a risk-based approach”.

Regarding sections 3.1.5 and 3.1.6, we agree with the EEI comments and further assert that the undefined use of “remote access” is problematic and should be scoped to certain types of routable communications Overall, concerns with communication monitoring for low impact BES should be addressed in a risk-based and architecture-based approach rather than a BES location approach specifically because of their lower impact. For example, rather than mandating IPS monitoring and user disablement at a low impact BES, require that interactive remote access be controlled and monitored from central aggregation or choke points (or an architecturally equivalent concept) and allow the entities to determine a risk-based security partitioning and control plan based on factors within their own environment.

In addition, **FirstEnergy supports EEI’s comments** which state:

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authentical and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect BES Cyber System network authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.16 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster

Answer	No
Document Name	

Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute for question #1.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI is supportive of the approach to consolidate to the electronic access section as adding a new section to capture these revisions would be purely duplicative. I also think that the new revisions are drafted in a way that allows for utilizing solutions that may be put in place for the version 9 for these new revisions if desired but also allowing for separate solutions if needed. The only concern with the current draft language is the use of the following phrase: “to mitigate risks associated with electronic access” in the intro paragraph of Section 3. As written there is a signifigant potential to cause more scrutiny on the allowed communications that did not previously exist and was not part of the SAR, and would give total discression to auditor interpretation.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The number of Low Impact BES Cyber Systems impacted would make achieving compliance burdensome in terms of level of effort, cost, and required technology implementations.	
Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	

To accommodate those systems that do not have the capability to perform the required function, such as protecting user authentication information in transit, Tacoma Power recommends including language in Attachment 1, Section 3, such as “per system capability,” as found throughout the rest of the CIP Standards. Specifically, Tacoma Power recommends adding the “per system capability” to the lead in to Section 3 of Attachment 1.

Suggested lead in language update:

“Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, to mitigate risks associated with electronic access, the Responsible Entity shall implement controls, **per system capability**, to:”

Additionally, Tacoma Power has a concern that Attachment 1, Section 3 Part 3.1.3 can be read in multiple ways. Specifically as it relates to the (i.) and (ii.) language in the lead-in to Section 3.1 (excerpt as follows):

3.1 For connectivity that provides the ability to communicate:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

What does the phrase “**each instance** of electronic remote access to **networks** containing low impact BES Cyber Systems” mean in Part 3.1.3? We see that the TR includes the desire to allow initial authentication to the network to allow transition to sub-networks, etc. But there is no structure for this within the 3.1 (i.) and (ii.) construct. Tacoma Power is concerned that the language of 3.1.3 does not support the idea of allowed sub-network connections without additional authentication if they are to a different asset containing a low impact BCS, since this ties it back to the original (i.)

In the scenario where a relay tech logs into a central system which includes configurations to access relays at several substations, is that relay tech required to re-authenticate each time they access a relay at a different substation (i.e., at a different asset containing Low Impact BCS)? The language of the Requirement does not provide clarity to this situation.

To aid in this scenario, Tacoma Power suggests the following language for clarity of Attachment 1 Section 3 Part 3.1.3:

“3.1.3 Authenticate users when remotely accessing networks containing low impact BES Cyber Systems.”

Likes 1	LaKenya Vannorman, N/A, Vannorman LaKenya
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	

Comment
Dominion Energy supports EEI comments. Dominion Energy supports in part the proposed changes to CIP-003-A Attachment 1, but disagree with the addition of proposed 3.1.5 and 3.1.6 and the deletion of Section 6. First, the SAR only authorized the change to Section 3 and the current language in Section 6 is clearer than what is proposed. We suggest deleting 3.1.5 and 3.1.6 and restoring Section 6 to address the concerns.

Likes 0	
Dislikes 0	

Response

Joshua London - Eversource Energy - 1, Group Name Eversource

Answer	No
Document Name	

Comment
Eversource agrees with the comments of EEI.

Likes 0	
Dislikes 0	

Response

Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna

Answer	No
Document Name	

Comment
The NERC Low Impact Criteria Review Report mentions the risk of coordinated attacks on low impact BES Cyber Systems that could adversely affect the BES. However, coordinated attacks are not considered for categorization of BES Cyber Systems in CIP-002, and the proposed language in CIP-003 is placing more restrictive controls on low impact BCS than medium impact BCS without ERC. For example, in 3.1.4, protecting user authentication information all the way to the asset is more restrictive than the current requirements for high and medium impact BCS, where an Intermediate System authenticates the user who is then allowed to then access high/medium impact BCS as needed. While the risk to a coordinated attack to multiple low impact BCS is not zero, the restrictive and prescriptive controls proposed does not allow a Responsible Entity to determine the best way to protect its low impact BCS. In 3.1.3, the language “each instance” is ambiguous and should be removed to avoid confusion or misinterpretation. Also, the lack of a clear definition of remote access further adds to the ambiguity and should be clarified or defined. “Per Cyber System/Asset capability” should be added to address those cyber assets that have limitations or cannot be replaced/upgraded without significant expense.

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	

Manitoba Hydro recognizes the standard drafting team's effort to develop a draft that clearly outlines requirements meeting the objectives of the project. There appears to be a disconnect in the two requirements to authenticate access and protect this information in transit.

Requirement 3.1.3 requires that access be authenticated at the time of permitting that access to the network containing low impact BES Cyber Systems. This requirement is worded flexibly to allow a number of technical solutions to accomplish the security objective. Requirement 3.1.4 specifies that authentication information be protected in transit from the asset containing low impact BES Cyber Systems. The implementation of 3.1.3 may be configured to have a central point of authentication that is not located at the asset. The text of 3.1.4 takes away flexibility in implementation. The following text is suggested based on the currently accepted wording in CIP-005 for Medium Impact Cyber Assets:

For all instances of electronic remote access to networks containing low impact BES Cyber Systems, protect user authentication information in transit in between the remote client and the authentication system used to meet 3.1.3.

The intent of requirement 3.1.6 is clear, however as currently worded it seems to require all vendor remote access to be disabled at all times. Manitoba Hydro suggests the following wording:

Have a documented method to disable vendor electronic remote access, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

With new language there will be a large amount of Low Impact BES Cyber Systems impacted. It would be costly for utilities to meet compliance and more burdensome than medium and high impact requirements.

Likes 0	

Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
Section 3 in att 1 does not make grammatical sense nor does it flow. There is concern for auditor interpretation to vary. In addtion, SRP is in support of Tacoma Power's comment on the suggested language as it can be interpreted in multiple ways.	
Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
1. Section 3.1.2 creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers: the proposed language requires detection of known/suspected malicious communications for “inbound and outbound electronic remote access.” There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5). BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS. 2. Section 3.1.4 creates a higher compliance bar for Low BCS than for Medium BCS: in the latest Draft 5 of CIP-005-8 R2.2 - 2.3, the proposed requirements include only Interactive Remote Access, or human-initiated access. Section 3.1.4 includes all “information in transit to or from the asset containing low impact BES Cyber Systems.” BPA suggests that this requirement be aligned with the latest Draft 5 of CIP-005-8 R2.2 - 2.3: “3.1.4 Protect user authentication *of IRA communications* in transit to or from the asset containing low impact BES Cyber Systems.” 3. Section 3.1.6: While BPA appreciates the committee’s intent to “present a single section for all electronic access” (Technical Rationale, p. 2), Section 3.1.6 is nonetheless awkwardly worded. It either suggests that all vendor remote access should be disabled (rather than requiring controls that could provide an option to disable vendor remote access), or it contradicts itself in a nonsensical sentence by saying that when vendor access is permitted, it should always be disabled. BPA suggests aligning with the language used in Draft 5 of CIP-003-10, such as “Have one or more methods” for determining and disabling vendor remote access sessions.	
Likes 0	

Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC

Answer	No
Document Name	

Comment

Please clarify whether vendor electronic remote access includes cases involving protocol transition between serial and TCP/IP.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	No
Document Name	

Comment

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authentical and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **user BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.16 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt

Answer	No
Document Name	

Comment

Black Hills Corporation agrees with the comments below from EEI, FE, and PNM Resources – Public Service Company of New Mexico.

Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting.

Regarding sections 3.1.5 and 3.1.6, we agree with the EEI comments and further assert that the undefined use of “remote access” is problematic and should be scoped to certain types of routable communications. Overall, concerns with communication monitoring for low impact BES should be addressed in a risk-based and architecture-based approach rather than a BES location approach specifically because of their lower impact. For example, rather than mandating IPS monitoring and user disablement at a low impact BES, require that interactive remote access be controlled and monitored from central aggregation or choke points (or an architecturally equivalent concept) and allow the entities to determine a risk-based security partitioning and control plan based on factors within their own environment.

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authenticate and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.1.6 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response

Micah Runner - Black Hills Corporation - 1

Answer	No
Document Name	

Comment

Black Hills Corporation agrees with the comments below from EEI, FE, and PNM Resources – Public Service Company of New Mexico.

Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting.

Regarding sections 3.1.5 and 3.1.6, we agree with the EEI comments and further assert that the undefined use of “remote access” is problematic and should be scoped to certain types of routable communications Overall, concerns with communication monitoring for low impact BES should be addressed in a risk-based and architecture-based approach rather than a BES location approach specifically because of their lower impact. For example, rather than mandating IPS monitoring and user disablement at a low impact BES, require that interactive remote access be controlled and monitored from central aggregation or choke points (or an architecturally equivalent concept) and allow the entities to determine a risk-based security partitioning and control plan based on factors within their own environment.

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authenticate and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.1.6 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response

Carly Miller - Carly Miller On Behalf of: Sheila Suurmeier, Black Hills Corporation, 5, 6, 1, 3; - Carly Miller

Answer	No
Document Name	

Comment

Black Hills Corporation agrees with the comments below from EEI, FE, and PNM Resources – Public Service Company of New Mexico.

Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting.

Regarding sections 3.1.5 and 3.1.6, we agree with the EEI comments and further assert that the undefined use of “remote access” is problematic and should be scoped to certain types of routable communications. Overall, concerns with communication monitoring for low impact BES should be addressed in a risk-based and architecture-based approach rather than a BES location approach specifically because of their lower impact. For example, rather than mandating IPS monitoring and user disablement at a low impact BES, require that interactive remote access be controlled and monitored from central aggregation or choke points (or an architecturally equivalent concept) and allow the entities to determine a risk-based security partitioning and control plan based on factors within their own environment.

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authenticate and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.1.6 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response

Josh Combs - Black Hills Corporation - 3

Answer	No
Document Name	

Comment

Black Hills Corporation agrees with the comments below from EEI, FE, and PNM Resources – Public Service Company of New Mexico.

Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting.

Regarding sections 3.1.5 and 3.1.6, we agree with the EEI comments and further assert that the undefined use of “remote access” is problematic and should be scoped to certain types of routable communications. Overall, concerns with communication monitoring for low impact BES should be addressed in a risk-based and architecture-based approach rather than a BES location approach specifically because of their lower impact. For example, rather than mandating IPS monitoring and user disablement at a low impact BES, require that interactive remote access be controlled and monitored from central aggregation or choke points (or an architecturally equivalent concept) and allow the entities to determine a risk-based security partitioning and control plan based on factors within their own environment.

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authenticate and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.1.6 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response

Ben Hammer - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

Remove Requirement 2 from the standard all together, add in requirements of attachment 1 for low impact BES Cyber systems into the correct CIP standard, CIP-004, CIP-006, CIP-005, CIP-008, and CIP-010 as needed.

There is no definition for the word communicate. This needs to be defined or changed to use the correct terminology.

The language “using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and” is not clear as written. As an example, an entity can have a routable protocol that enters the low impact asset, that never communicates using a bidirectional routable protocol with any Low impact BES Cyber Assets. This creates an undue burden for Registered entities to protect assets that have no routable connectivity.

The definition of vendor needs to be defined and **should not** include long-term /fulltime contract employees that work for the Registered entity.

Likes 0	
Dislikes 0	

Response

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	No
Document Name	

Comment

As proposed, CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4 does not consider per Cyber System capability and may create an impossibility to comply within the implementation timeline without wholesale upgrades or replacements of technology and communications infrastructure.

While this newly proposed Requirement Part is consistent with the LICRT report and the subsequent approved SAR; protections from the user all the way through to the asset containing the BCS imposes a mandatory obligation for low impact that is above and beyond the current enforceable requirements set forth for high and medium impact BCS, and also precludes the use of established and current enforceable concepts used to protect user authentication information for high and medium impact like IRA through an Intermediate System.

The protections for user authentication information in transit between a user and a high or medium impact BCS are between the user and the Intermediate System, and do not extend all the way to the asset containing the high or medium impact BCS. Here, user authentication information is protected between the initiating device and the Intermediate System, and once authenticated to the Intermediate System, the Requirement language would permit the use of any protocol the entity chooses (Telnet, for example) to make the connection from the Intermediate System to the BCS. Proxied connections/new sessions established from the Intermediate System to the BCS are permitted to transverse unencrypted communication links and use unencrypted protocols (which may be the only method depending on the entity's technology). If "Telnet" is the only method that can be used, there is also no obligation to block clear test interactive protocols from going through a high or medium impact ESP if they are needed, nor to force a VPN tunnel or communication link encryption to do so.

There is no obligation to "protect user authentication information" all the way to the asset containing the BCS for high and medium impact, and to mandate this for low impact does not seem commensurate with risk. CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as written, would only permit the use of an Intermediate System if the Intermediate System were physically located within the asset containing the LBCS, instead of permitting entities to leverage existing centralized infrastructure already implemented for the purpose of protecting user authentication information for high or medium impact.

NSRF requests further SDT consideration of the addition of "per Cyber System capability" language, and the addition of options that would permit protection of user authentication information in transit between the user and an Intermediate System, or the asset containing low impact BES Cyber Systems.

The SAR only directed "protection of user authentication information in transit for **remote access to networks** containing low impact BES Cyber Systems." This would only include network access credentials which could be authenticated locally, precluding the need for these credentials to transit to the asset containing low impact BCS's. Thus, current implementations could remain compliant according to the direction of the SAR.

The proposed language of 3.1.4 expands the SAR mandate to protect all authentication information, which includes account passwords of the low impact BCS's, which requires transmitting these credentials to the BCS's. It is the expansion of the scope of the SAR regarding which credentials need to be protected that makes the proposed 3.1.4 language incompatible with current compliant practices.

If 3.1.4 were re-worded from *"Protect user authentication information"* to *"Protect network authentication information,"* this would expand compliance options to include local authentication and avoid having to send network credentials to the asset.

NSRF offers the following potential language for SDT consideration:

3.1.4 Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems if using public communication links;

3.1.4 Protect user authentication information in transit to the asset containing low impact BES Cyber Systems, unless low impact BES Cyber System remote access is already protected by going through an Intermediate System meeting the collective requirement parts of CIP-005-7 Requirement R2; if using public communication links, protect user authentication information in transit to and from the asset containing low impact BES Cyber Systems;

3.1.4 Protect user authentication information in transit:

- *to or from the asset containing low impact BES Cyber Systems if using public communication links; or*
- *to the asset containing the low impact BES Cyber Systems if using private communication links, unless low impact BES Cyber System remote access is already protected by going through an Intermediate System meeting the collective requirement parts of CIP-005-7 Requirement R2.*

3.1.4 For all instances of electronic remote access to networks containing low impact BES Cyber Systems, protect user authentication information in transit in between the remote client and the authentication system used to meet 3.1.3.

Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment

Exelon supports the comments submitted by the EEI.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon is in support of EEIs response to this question.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

LCRA seeks clarification on what “outbound electronic remote access” means. Additionally, the use of the word “remote” throughout the entirety of Section 3 seems inappropriate when discussing the various types of electronic access communications.

We are confused with the roman numerals in section 3.1 that are used to define applicability. LCRA believes that the electronic access being defines here would better be served by a NERC Glossary of Terms definition. This would enable this section to read more clearly.

Section 3.1.2 requires stronger controls than medium impact BES Cyber Systems not at Control Centers. This goes against the Brightline criteria.

Section 3.1.3 requires that authentication occurs when permitting each instance of electronic remote access. LCRA is concerned with the scoping of this requirement when managing connection over Wide Area Network (WAN). It is unclear if intermediate systems or equivalent could be used to achieve compliance.

Section 3.1.5 & 3.1.6 consider restructuring the sentences to avoid confusion. LCRA suggests the following revision:

* 3.1.5 – Implement measures to determine vendor electronic remote access

* 3.1.6 – Implement measures to disable vendor electronic remote access, where enabled

Likes 0	
Dislikes 0	

Response

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer	No
Document Name	

Comment

LCRA seeks clarification on what “outbound electronic remote access” means. Additionally, the use of the word “remote” throughout the entirety of Section 3 seems inappropriate when discussing the various types of electronic access communications.

We are confused with the roman numerals in section 3.1 that are used to define applicability. LCRA believes that the electronic access being defines here would better be served by a NERC Glossary of Terms definition. This would enable this section to read more clearly.

Section 3.1.2 requires stronger controls than medium impact BES Cyber Systems not at Control Centers. This goes against the Brightline criteria.

Section 3.1.3 requires that authentication occurs when permitting each instance of electronic remote access. LCRA is concerned with the scoping of this requirement when managing connection over Wide Area Network (WAN). It is unclear if intermediate systems or equivalent could be used to achieve compliance.

Section 3.1.5 & 3.1.6 consider restructuring the sentences to avoid confusion. LCRA suggests the following review:

- 3.1.5 – Implement measures to determine vendor electronic remote access
- 3.1.6 – Implement measures to disable vendor electronic remote access, where enabled

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

AEPC has signed on to ACES comments below:

ACES feels, “Section 3.1.4 Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems”, should read: Protect electronic remote access information in transit to or from the asset containing low impact BES Cyber Systems;”
The addition of authentication of remote users we are fine with, but the SDT chose to just scope in protection of remote user authentication information and we feel that is not the only thing that should be protected. Just like in the case of detection of vendor communication versus all communications (fixed in this version), we feel ALL electronic remote access information should be protected just as it is in CIP-005 R2 if it’s FERC/NERC’s intention of reducing overall cybersecurity risk with this change. Without fully protecting the entire remote access session, risks are only minimally reduced and this standard will have to be revised again to meet the objective.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD and BANC appreciate the Standards Drafting Team’s efforts to revise Attachment 1. Section 3.1.1 reads “Permit only necessary inbound and outbound remote electronic access as determined by the responsible entity.” Using the word “remote” in this section narrows the scope of Electronic Access Controls to only inbound and outbound electronic access that is “remote access.” The technical rationale is incorrect in that using this wording does not “maintain the original language used in CIP-003-9, Section 3.1” as CIP-003-9 is more specific.

We feel there is no need to use the word “remote” in Section 3.1.1 as it is already included when an entity “Permits only necessary inbound and outbound electronic access as determined by the Responsible Entity.” If using the word “remote” is deemed necessary, the Standards Drafting Team should provide some clarity as it is not very clear what “remote” electronic access is. We feel that “remote” is already covered by Section 3.1.1.i:

“between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);”

The same comment applies to Sections 3.1.2 and 3.1.3 as it is not clear how using the word “remote” clarifies anything.

Additionally, we believe the language in the Standards Authorization Request is proposing more strict controls/requirements for low impact BCS than the controls/requirements currently being proposed for high impact BCS and medium impact BCS in CIP-005-8 Requirements R2.1 - 2.4, and CIP-007-7 Requirement R1.1.

Likes 0	

Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	

Comment

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authentical and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.16 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	No
Document Name	

Comment

We support NPCC RSC Comments	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	No
Document Name	
Comment	
Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting. PNMR also supports EEI's comments pertaining to Section 3, parts 3.1.4 and 3.1.6.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	

AZPS does not agree with proposed language in Attachment 1 Section 3.1.4 and 3.1.6, for the other sections AZPS agrees. AZPS supports the comments and recommendations made on behalf of EEI to clarify sections 3.1.4 and 3.1.6. to ensure existing protections involving an Intermediate System meeting CIP-005-7 requirements can be utilized where applicable and protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems if using public communication links.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA

Answer	No
Document Name	

Comment

No

NCPA agrees with several other comments that the proposed language places a high level of burden on entities to protect low impact assets.

3.1.2 – Would greatly increase the demand to implement and maintain a IDS type deployment and continuously update and monitor such traffic

3.1.3 – The phrase “each instances” is not well defined and does not appear anywhere else in the standards.

3.1.4 – This language requires a higher level of security than High/Med assets

3.1.6 – Needs clarification of when to disable vendor remote access

Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CEHE) requests additional clarity from the SDT on the intent of section 3.1 iii in the Electronic Access Controls section in which the phrase “time-sensitive communications” is referenced. CEHE believes that the language, while being overtly prescriptive, is also vague and does not entirely explain which time-sensitive protocols are being referenced. CEHE would like to request a better explanation of the inferred time-sensitive protocols included in this section.

Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group supports and incorporates by reference the comments of the MRO (NSRF) Group for Question 1.	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	

Terminology used within 3.1 doesn't distinguish existing "electronic access" from the new term "electronic remote access." The use of the terminology "electronic remote access" generally refers to interactive remote access. Using the terminology "electronic remote access" for 3.1.1 and 3.1.2 will cause confusion.

Suggest changing 3.1.1 and 3.1.2 by deleting the word "remote" as follows:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic access; …

If the SDT retains the word "remote", the SDT should consider defining "electronic remote access" or alternatively revising "Interactive Remote Access" by adding the following statement to the existing definition of "Interactive Remove Access": **Interactive Remote Access includes remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s).** The revised definition would read as follows and should be used in place of "electronic remote access".

Proposed Revision of Interactive Remote Access:

User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). **Interactive Remote Access includes remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s).** Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST respectfully offers the following observations and recommendations:

We suggest revising 3.1.4 "Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems" to say, "Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems from unauthorized disclosure." Given the fact the Technical Rationale document states explicitly the purpose of this requirement is to protect the confidentiality of user authentication data, we believe the requirement itself should also make this explicit.

Regarding requirements 3.1.5 and 3.1.6 (determining and disabling vendor remote access, respectively, NST notes that although the Technical Rational states the SDT's objective is to "maintain the original language used in CIP-003-9" Sections 6.1 and 6.2, this has not been done. As a presumably unintended result, the current wording of 3.1.6 ("Disable vendor electronic remote access, where vendor electronic remote access is permitted"), if interpreted literally, would require an entity to block all vendor remote access. We recommend addressing this problem by using CIP-003-9's existing language for determining and disabling vendor remote access.

Regarding the SDT's decision to merge CIP-003-9 Sections 3 and 6, NST disagrees with the SDT's assertion, "Section 6 has not been implemented or required by industry at this time and therefore there would be no impact to merging it with Section 3." While this is presently true, Registered Entities will be obliged to address requirements in Section 6 on 4/1/2026, which we expect will be at least a year before a newer version of CIP-003 that incorporates this project's changes becomes effective. We therefore believe it would be less disruptive to only move malicious communications detection from Section 6 to Section 3, leaving the other two vendor remote access requirements unchanged.

Likes 0	

Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
To accommodate those systems that do not have the capability to perform the required function, such as protecting user authentication information in transit, Constellation recommends including language in Attachment 1, Section 3, such as "per system capability," as found throughout the rest of the CIP Standards. Specifically, Tacoma Power recommends adding the "per system capability" to the lead into Section 3 of Attachment 1. Suggested lead in language update: "Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, to mitigate risks associated with electronic access, the Responsible Entity shall implement controls, per system capability, to:" Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	

NV Energy supports the comments from MRO NSRF and EEI as they relate to 3.1.4.

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren supports EEI's comments on this question.

Likes 0	
Dislikes 0	

Response

Hillary Creurer - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

Minnesota Power supports EEI’s comments.

Likes 0	
Dislikes 0	

Response

Katrina Lyons - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

The modification to 3.1 iii is more limiting than intended. There are time-sensitive communications protocols that are unrelated to Protection Systems.

The modification to 3.1 iii could benefit from further clarification to ensure it aligns with the intended purpose and ensure industry is clear on the potential impact of this change. .

Regarding 3.1.1, it would be helpful to have a clearer explanation in the Technical Rationale (TR)for changing the language to "permitting only necessary inbound/outbound REMOTE access." The objective of the TR to “maintain the original language” could be addressed more effectively by the SDT.

Although 3.1.2 exceeds the Standards for Medium Impact and incurs substantial costs. The challenge lies in the fact these terms have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, their reuse should be restricted, and any lesser measures, such as monitoring firewall logs, should not be authorized.

The prescriptiveness of 3.1.3 seems to go beyond what is typically expected for Medium Impact.

Similarly, 3.1.4 appears to exceed the standards for Medium Impact. It would be helpful to revisit this requirement as well.

With regards to 3.1.5 and 3.1.6, the change from "have methods" to "implement controls to" introduces some ambiguity and alters the previously approved requirements. Implementing a control to determine vendor electronic remote access seems very different than having methods for determining vendor electronic remote access. The technical rationale suggests that the SDT intends to uphold the initial language, despite having, in reality, modified the language.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

The modification to 3.1 iii is more limiting than intended. There are time-sensitive communications protocols that are unrelated to Protection Systems.

The modification to 3.1 iii could benefit from further clarification to ensure it aligns with the intended purpose and ensure industry is clear on the potential impact of this change. .

Regarding 3.1.1, it would be helpful to have a clearer explanation in the Technical Rationale (TR)for changing the language to "permitting only necessary inbound/outbound REMOTE access." The objective of the TR to “maintain the original language” could be addressed more effectively by the SDT.

Although 3.1.2 exceeds the Standards for Medium Impact and incurs substantial costs. The challenge lies in the fact these terms have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, their reuse should be restricted, and any lesser measures, such as monitoring firewall logs, should not be authorized.

The prescriptiveness of 3.1.3 seems to go beyond what is typically expected for Medium Impact.

Similarly, 3.1.4 appears to exceed the standards for Medium Impact. It would be helpful to revisit this requirement as well.

With regards to 3.1.5 and 3.1.6, the change from "have methods" to "implement controls to" introduces some ambiguity and alters the previously approved requirements. Implementing a control to determine vendor electronic remote access seems very different than having methods for

determining vendor electronic remote access. The technical rationale suggests that the SDT intends to uphold the initial language, despite having, in reality, modified the language.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	No
Document Name	

Comment

ACES feels, “Section 3.1.4 Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems”, should read: Protect electronic remote access information in transit to or from the asset containing low impact BES Cyber Systems;”

The addition of authentication of remote users we are fine with, but the SDT chose to just scope in protection of remote user authentication information and we feel that is not the only thing that should be protected. Just like in the case of detection of vendor communication versus all communications (fixed in this version), we feel ALL electronic remote access information should be protected just as it is in CIP-005 R2 if it’s FERC/NERC’s intention of reducing overall cybersecurity risk with this change. Without fully protecting the entire remote access session, risks are only minimally reduced and this standard will have to be revised again to meet the objective.

Likes 0	
Dislikes 0	

Response

Alison MacKellar - Constellation - 5

Answer	No
Document Name	

Comment

To accommodate those systems that do not have the capability to perform the required function, such as protecting user authentication information in transit, Constellation recommends including language in Attachment 1, Section 3, such as "per system capability," as found throughout the rest of the CIP Standards. Specifically, Tacoma Power recommends adding the "per system capability" to the lead into Section 3 of Attachment 1. Suggested lead in language update: "Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, to mitigate risks associated with electronic access, the Responsible Entity shall implement controls, per system capability, to:"

Alison Mackellar on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	

Comment
OPG supports NPCC Regional Standards Committee’s comments. Please clarify whether vendor electronic remote access includes cases involving protocol transition between serial and TCP/IP.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	

Comment
PacifiCorp supports the comments of MRO NSRF and EEI.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	

Comment
Texas RE agrees with the proposed language in Sections 3.1.2, 3.1.3, 3.1.4, 3.1.5, and 3.1.6. Texas is concerned, however, with the term electronic remote access in Section 3.1. This phrase changes the scope of the requirement to potentially no longer include communications that are not used for remote access. For example, the proposed addition of "remote" could arguably exclude Domain Name System (DNS) and ping queries from the scope of the CIP-003 protections, potentially allowing unnecessary electronic access using these types of traffic. Such traffic has been associated with malicious attacks, including DNS cache poisoning and other activities that are not exclusively linked to remote access. As such, there is a potential reliability gap if this language is retained. Texas RE recommends removing the word “remote” in Section 3.1.1.

Likes 0	
Dislikes 0	
Response	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
The proposed language of Section 3 has lists within lists. This makes it difficult to understand how the items in each list apply to each other. The roman numerals i-iii apply to 3.1.1.-3.1.6. but this may be misinterpreted in future CMEP engagements. This also causes the standard to deviate from what is understood to be the NERC style “and/or” lists. As proposed, 3.1 and 3.2 are the list items for the Section 3 language “Responsible Entity shall implement controls to:”. Since 3.1 and 3.2 are the two items in a list, 3.1 should end with the word “and” to differentiate it from an “or” list. Propose the following changing “…the Responsible Entity shall implement controls to:” to “…the Responsible Entity shall implement the following controls.”	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed language in CIP-003-A Attachment 1.	

Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	

Response

Mark Flanary - Midwest Reliability Organization - 10

Answer	Yes
Document Name	

Comment

Although we can agree with the proposed changes, we have a suggested change to Attachment 1, Section 3.1.3 in the event another draft is necessary:

The currently proposed langage is "Authenticate users when permitting each instance of electronic remote access to networks containing low impact BES Cyber Systems;".

MRO suggests using language more similar to the definition of Interactive Remote Access (IRA). IRA is defined as “user-initiated access by a person a remote access client or other remote access technology…”. Considering that, MRO suggests inserting "user-initiated" following the word "each" on that proposed language, which would result in "Authenticate users when permitting each **user-initiated** instance of electronic remote access to networks containing low impact BES Cyber Systems;".

Without such a change, the proposed language can be interpreted as introducing system-to-system communications into the equation, which we don't believe was intended.

Likes 0	
Dislikes 0	

Response

James Keele - Entergy - 3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - Steve Toosevich, Group Name NIPSCO Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please provide recommended language you would support and, if appropriate, technical or procedural justification.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports the comments of MRO NSRF and EEI.	
Likes 0	
Dislikes 0	
Response	

Alison MacKellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation recommends changing CIP-003-A, Attachment 2, in conformance with our comments to Question 1. Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
We do not concur with the proposed language in Attachment 2 for the same reasons we do not agree with the language in Attachment 1. Please see the response to question 1 above.	
Likes 0	
Dislikes 0	

Response

Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	

Comment
We do not concur with the proposed language in Attachment 2 for the same reasons we do not agree with the language in Attachment 1. Please see the response to question 1 above.

Likes 0	
Dislikes 0	

Response

Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	

Comment
Minnesota Power supports EEI’s comments.

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	

Comment
Ameren supports EEI's comments on this question.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation recommends changing CIP-003-A, Attachment 2, in conformance with our comments to Question 1. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
As per our response to Question 1, NST recommends leaving requirements for detecting and disabling vendor remote access in Section 6, moving only malicious communications detection to Section 3.	
Likes 0	
Dislikes 0	
Response	

TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	

Terminology used within Section 3. does not distinguish existing “electronic access” from the new term “electronic remote access.” The use of the terminology “electronic remote access” generally refers to interactive remote access. Using the terminology “electronic remote access” for Section 3. Item 1 may cause confusion.

SDT should consider defining “electronic remote access” or redefining “Interactive Remote Access” as follows and using that in place of “electronic remote access.”

Continent-wide Term

Interactive Remote Access

Definition

User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Interactive Remote Access includes remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Suggest changing Section 3. Item 1 as follows:

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

1. Documentation For Section 3.1.1, documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive these communications are time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative Protection Systems, such as:

Suggest changing Section 3. Item 5 as follows for consistency:

“5. For Section 3.1.5 documentation showing the ability to determine vendor electronic remote access, such as…”

Likes 0	

Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	

Comment
WEC Energy Group supports and incorporates by reference the comments of the MRO (NSRF) Group for Question 2.

Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	

Comment
Terminology used within Section 3. does not distinguish existing “electronic access” from the new term “electronic remote access.” The use of the terminology “electronic remote access” generally refers to interactive remote access. Using the terminology “electronic remote access” for Section 3. Item 1 may cause confusion. SDT should consider defining “electronic remote access” or redefining “Interactive Remote Access” as follows and using that in place of “electronic remote access.” **Continent-wide Term** Interactive Remote Access **Definition** User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Interactive Remote Access includes remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications. Suggest changing Section 3. Item 1 as follows: Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation For Section 3.1.1, documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive these communications are time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative Protection Systems, such as:

Suggest changing Section 3. Item 5 as follows for consistency:

"5. For Section 3.1.5 documentation showing the ability to determine vendor electronic remote access, such as..."

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA

Answer	No
Document Name	

Comment

No

NCPA agrees with several other comments that the proposed language places a high level of burden on entities to protect low impact assets.

3.1.2 – Would greatly increase the demand to implement and maintain a IDS type deployment and continuously update and monitor such traffic

3.1.3 – The phrase “each instances” is not well defined and does not appear anywhere else in the standards.

3.1.4 – This language requires a higher level of security than High/Med assets

3.1.6 – Needs clarification of when to disable vendor remote access

Likes 0	
Dislikes 0	

Response

Andrew Smith - APS - Arizona Public Service Co. - 5

Answer	No
Document Name	

Comment

AZPS does not agree with the proposed language in Attachment 2. AZPS supports EEI's recommendation to add an option that would permit protection of user authentication information in transit between the user and the intermediate system, and not just the asset containing low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI does not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's comments and proposed changes as provided in our response to question 1)	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No

Document Name	
Comment	
We feel that using the words “outbound electronic remote access” in Section 3 is confusing and we do not think adding the word “remote” so that the language states “… inbound and outbound electronic “remote” access…” clarifies anything. We recommend striking the word “remote”.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
Please refer to LCRA’s concerns in question 1.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
Please refer to LCRA’s concerns in question 1.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	

Exelon is in support of EEIs response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
For CIP-003-A Requirement R2 Attachment 2, Section 3, Requirement Part 3.1.4, NSRF requests further SDT consideration of an adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the the asset containing low impact BES Cyber Systems.	
Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	

see question 1 comments, attachment 2 should be rewritten to cover the appropriate changes based off the comments on question 1.

Likes 0	
Dislikes 0	

Response

Josh Combs - Black Hills Corporation - 3

Answer	No
Document Name	

Comment

Black Hills Corporation agrees with EEI's comments: we do not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's proposed change to question 1)

Likes 0	
Dislikes 0	

Response

Carly Miller - Carly Miller On Behalf of: Sheila Suurmeier, Black Hills Corporation, 5, 6, 1, 3; - Carly Miller

Answer	No
Document Name	

Comment

Black Hills Corporation agrees with EEI's comments: we do not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's proposed change to question 1)

Likes 0	
Dislikes 0	

Response

Micah Runner - Black Hills Corporation - 1

Answer	No
Document Name	

Comment

Black Hills Corporation agrees with EEI's comments: we do not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's proposed change to question 1)

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt

Answer	No
Document Name	

Comment

Black Hills Corporation agrees with EEI's comments: we do not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's proposed change to question 1)

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	No
Document Name	

Comment

EEI does not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's proposed change to question 1)

Likes 0	
Dislikes 0	

Response

Tracy MacNicoll - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment
The examples of evidence for R3.1.1 should also include the documentation of why the communication is needed since the entity is required for low impact assets to implement the controls based on their need.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
1. Section 3.1.2 creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers: the proposed language requires detection of known/suspected malicious communications for “inbound and outbound electronic remote access.” There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5). BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS. 2. Section 3.1.4 creates a higher compliance bar for Low BCS than for Medium BCS: in the latest Draft 5 of CIP-005-8 R2.2 - 2.3, the proposed requirements include only Interactive Remote Access, or human-initiated access. Section 3.1.4 includes all “information in transit to or from the asset containing low impact BES Cyber Systems.” BPA suggests that this requirement be aligned with the latest Draft 5 of CIP-005-8 R2.2 - 2.3: “3.1.4 Protect user authentication *of IRA communications* in transit to or from the asset containing low impact BES Cyber Systems.” 3. Section 3.1.6: While BPA appreciates the committee’s intent to “present a single section for all electronic access” (Technical Rationale, p. 2), Section 3.1.6 is nonetheless awkwardly worded. It either suggests that all vendor remote access should be disabled (rather than requiring controls that could provide an option to disable vendor remote access), or it contradicts itself in a nonsensical sentence by saying that when vendor access is permitted, it should always be disabled. BPA suggests aligning with the language used in Draft 5 of CIP-003-10, such as “Have one or more methods” for determining and disabling vendor remote access sessions.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	

Comment	
SRP agrees and supports Tacoma Power's comment to incorporate the proposed changes outlined in Q1.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Per answer in question #1.	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
The language in 3.1.2 is specifying an IDS/IPS which depending on the capability of cyber assets at the low impact assets, could be infeasible or cost prohibitive to implement/replace equipment and should take into account that many cyber assets could be limited in their ability to communicate with monitoring/detection systems, communication protocols, etc. Also, in 3.1.4, the SDT should consider modifying language that focuses on mitigating risks to protect user authentication information and allow entities to determine their methods to mitigate risks that fit with their current network configuration(s). The SDT should also consider adding “per Cyber System/Asset capability” to address this reality that many cyber assets have limitations and may not be easily upgraded or replaced.	
Likes 0	
Dislikes 0	
Response	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No

Document Name	
Comment	
Eversource agrees with the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
See comments to Q1.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Tacoma Power recommends changing CIP-003-A, Attachment 2, in conformance with our comments to Question 1.	
Likes 1	LaKenya Vannorman, N/A, Vannorman LaKenya
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	

Comment	
The number of Low Impact BES Cyber Systems impacted would make achieving compliance burdensome in terms of level of effort, cost, and required technology implementations.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute for question #2.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
Based on concerns about Attachment 1 listed above this section requires adjustment.	
Likes 0	
Dislikes 0	
Response	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	Yes
Document Name	

Comment

The NAGF requests the SDT to review the proposed language in CIP-003-A Attachment 2, Section 3, Part 1 stating “except where these communications are time-sensitive protection or control functions between Protection Systems,” and compare it to the proposed language in Attachment 1, Section 3.1.iii “not used for time-sensitive communications of Protection Systems.” to ensure consistency.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mark Flanary - Midwest Reliability Organization - 10

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - Steve Toosevich, Group Name NIPSCO Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE noticed the formatting of Attachment 2, Section 3 is not consistent with Attachment 1. Texas RE recommends it contain subsections 3.1 – 3.7. Texas RE is similarly concerned with the addition of “remote” in the phrase electronic remote access as in Attachment 1. Texas RE recommends removing the term “remote” from Section 3, #1.	
Likes 0	
Dislikes 0	
Response	

3. The Standard Drafting Team (SDT) proposes a three (3) year implementation plan for CIP-003-A. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

If this standard were to be drafted as-is, large organizations would be compelled to implement substanial technological changes on a grand scale, including significant cost capital and O&M increases which would need to be accounted for on an ongoing basis as well as marshalling of significant contracted labor to execute this massive directive. Consider a tier-ed based approach based on certain risk-based factors, existing connectivity types, capabilities, etc.

FirstEnergy also supports EEI's comments which state:

The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB

Answer	No
Document Name	

Comment

The number of Low Impact BES Cyber Systems impacted would make achieving compliance burdensome in terms of level of effort, cost, and required technology implementations within the implementation timeframe.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - Steve Toosevich, Group Name NIPSCO Compliance

Answer	No

Document Name	
Comment	
Responsible entities are currently ensuring compliance with CIP-003-8 and preparation for the approved CIP-003-9. The three (3) year implementation plan of CIP-003-A would quickly follow the changes implemented in CIP-003-9 while anticipating modifications to the Standards for Project 2016-02 Modifications to CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No
Document Name	
Comment	
Eversource agrees with the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
With the restrictive and prescriptive language as currently proposed, those Responsible Entities with a significant number of low impact assets containing low impact BCS could find it impossible to implement a solution in 3 years. The SDT should consider adding “per Cyber System/Asset capability” to address the reality that many cyber assets have limitations and would require a large effort to replace and implement new cyber assets; and this does not begin to address the potential for equipment supply chain issues and delivery lead times which have not returned to normal for equipment purchases.	
Likes 0	
Dislikes 0	
Response	

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
If specific date of implementation is defined, SRP might agree. There is significant cost (equipment and resources), time for planning, and work will need to be done.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Until Questions 1 and 2 are resolved it is difficult for BPA to determine if the 3 year timeframe is appropriate.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	
Likes 0	
Dislikes 0	
Response	

Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with the comments provided by EEI. The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with the comments provided by EEI. The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	
Likes 0	
Dislikes 0	
Response	
Carly Miller - Carly Miller On Behalf of: Sheila Suurmeier, Black Hills Corporation, 5, 6, 1, 3; - Carly Miller	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with the comments provided by EEI. The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the	

proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	
Likes 0	
Dislikes 0	
Response	
Josh Combs - Black Hills Corporation - 3	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with the comments provided by EEI. The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
The absence of per Cyber System capability in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4 may create an impossibility to comply within the implementation timeline without wholesale upgrades or replacements of technology and communications infrastructure. NSRF requests further SDT consideration of the addition of "*per Cyber System capability*" language in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4.	
Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No

Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is in support of EEIs response to this question.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
LCRA believes that a 3-year implementation plan may not be sufficient due to the sheer number of Low Impact BES Cyber Systems. Additionally, there is considerable unknowns regarding the new requirements. Please see LCRA's response to question 1.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	

LCRA believes that a 3-year implementation plan may not be sufficient due to the sheer number of Low Impact BES Cyber Systems. Additionally, there is considerable unknowns regarding the new requirements. Please see LCRA's response to question 1.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.

Likes 0	
Dislikes 0	

Response

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF

Answer	No
Document Name	

Comment

ITC supports the comments submitted by EEI

Likes 0	
Dislikes 0	

Response

Andrew Smith - APS - Arizona Public Service Co. - 5

Answer	No
Document Name	

Comment

AZPS does not agree with the proposed implementation plan. AZPS agrees with EEI's comments that the 3 year implementation plan would be acceptable if there were not other industry standards projects underway that will also require changes affecting low impact BCS with differing deadlines.

Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

The pending changes for CIP-003 in other NERC projects would equate to implementing changes that would, within a relatively short time, be modified and be subject to further modifications. Additionally, CEHE supports the included EEI comments that address timing and pending NERC projects.

EEI Comment:

The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.

Likes 0	
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	No
Document Name	

Comment

WEC Energy Group supports and incorporates by reference the comments of the MRO (NSRF) Group for Question 3.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren supports EEI's comments on this question.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No

Document Name	
Comment	
We do not agree with the proposed implementation plan. Our apprehension primarily stems from the intersection of CIP-003-A and CIP-003-9, with a particular focus on the potential financial implications in Section 6.3, where additional expenditures may be necessitated to accommodate technological changes.	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
We do not agree with the proposed implementation plan. Our apprehension primarily stems from the intersection of CIP-003-A and CIP-003-9, with a particular focus on the potential financial implications in Section 6.3, where additional expentitures may be necessitated to accommodate technological changes.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports the comments of MRO NSRF and EEI.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed 3-year implementation plan.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	

Comment
Constellation has no additional comments. Alison Mackellar on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

James Keele - Entergy - 3	
Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	

Comment

Likes 0	

Dislikes 0	
Response	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 1	LaKenya Vannorman, N/A, Vannorman LaKenya
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tracy MacNicoll - Utility Services, Inc. - 4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

4. The SDT believes the language of CIP-003-A addresses the issues outlined in the SAR in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports the comments of MRO NSRF and EEI.	
Likes 0	
Dislikes 0	
Response	

Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
3.1.2 exceeds the Standards for Medium Impact and incurs substantial costs. The challenge lies in the fact these terms have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, their reuse should be restricted, and any lesser measures, such as monitoring firewall logs, should not be authorized	
Likes 0	
Dislikes 0	
Response	

Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
3.1.2 exceeds the Standards for Medium Impact and incurs substantial costs. The challenge lies in the fact these terms have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, their reuse should be restricted, and any lesser measures, such as monitoring firewall logs, should not be authorized.	
Likes 0	

Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
Further analysis is needed to determine if the benefits outweigh the cost of additional equipment needing to be purchased in order to achieve compliance.	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group supports and incorporates by reference the comments of the MRO (NSRF) Group for Question 4.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	No
Document Name	
Comment	
No NCPA agrees with several other comments that the proposed language places a high level of burden on entities to protect low impact assets.	

3.1.2 – Would greatly increase the demand to implement and maintain a IDS type deployment and continuously update and monitor such traffic

3.1.3 – The phrase “each instances” is not well defined and does not appear anywhere else in the standards.

3.1.4 – This language requires a higher level of security than High/Med assets

3.1.6 – Needs clarification of when to disable vendor remote access

Likes 0	
Dislikes 0	

Response

Andrew Smith - APS - Arizona Public Service Co. - 5

Answer	No
Document Name	

Comment

AZPS does not agree the changes are cost effective as these would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1

Answer	No
Document Name	

Comment

PNMR sees potential excessive costs in implementing 3.1.4 – particularly if the need arose to install a substation server at each LIBCS substation (as there are many field devices with varying and older protocols in place) in order to ensure the correct protocols were met.

Likes 0	
Dislikes 0	

Response

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer	No

Document Name	
Comment	
LCRA cannot determine the cost effectiveness of these proposals due to the sheer number of Low Impact BES Cyber Systems. Additionally, there is considerable unknowns regarding the new requirements. Please see LCRA's response to question 1.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
LCRA cannot determine the cost effectiveness of these proposals due to the sheer number of Low Impact BES Cyber Systems. Additionally, there is considerable unknowns regarding the new requirements. Please see LCRA's response to question 1.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	

Comment
The absence of per Cyber System capability in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4 may require premature wholesale upgrades or replacement of communications or operational technology that has not met its end of life in order to comply. NSRF requests further SDT consideration of the addition of "*per Cyber System capability*" language in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4.

Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	

Response

Ben Hammer - Western Area Power Administration - 1

Answer	No
Document Name	

Comment
The absence of per Cyber System capability in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4 may require premature wholesale upgrades or replacement of communications or operational technology that has not met its end of life in order to comply. NSRF requests further SDT consideration of the addition of "*per Cyber System capability*" language in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment
More information required. Unable to determine exact financial impact, but it is significant and needs to be allowed for in the budget.

Likes 0	
Dislikes 0	

Response

Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna

Answer	No
Document Name	
Comment	
Large entities with a large number of cyber assets could incur significant capital and O&M expenditures and labor costs that would be unrealistic if there is only a 3 year implementation plan. This could cause entities to make financial decisions that are not cost effective. The SDT is encouraged to consider the addition of “per Cyber System/Asset capability” and provide a more tiered approach for those entities with a significant number of cyber assets.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - Steve Toosevich, Group Name NIPSCO Compliance	
Answer	No
Document Name	
Comment	
Responsible Entities would potentially need to purchase new equipment to meet the proposed language of the Standard.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The number of Low Impact BES Cyber Systems impacted would make achieving compliance burdensome in terms of level of effort, cost, and required technology implementations within the implementation timeframe.	
Likes 0	
Dislikes 0	
Response	

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the MRO NSRF for question #4.	
Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
This proposal would be prohibitively expensive both to build and operate over time. To be “cost effective” implies the proposed modification to the CIP-003 standard can be absorbed with existing company staff and minor procedure adjustment. Based on the high volume of Low Impact Cyber System locations and varied configurations that we have in our service territory (approximately 10 times the level of CIP Medium Impact locations), this is not a cost-effective change but is rather a cost-prohibitive mandate. Substantial additional funding (capital and O&M), staffing, and compliance programs will be required to meet the proposed requirements.	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
PNMR sees potential excessive costs in implementing 3.1.4 – particularly if the need arose to install a substation server at each LIBCS substation (as there are many field devices with varying and older protocols in place) in order to ensure the correct protocols were met.	
Likes 0	
Dislikes 0	
Response	

Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 1	LaKenya Vannorman, N/A, Vannorman LaKenya
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren has no comments on the cost effectiveness of this project.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST is unable to assess the cost effectiveness of the proposed approaches to addressing the SAR.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	

Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Josh Combs - Black Hills Corporation - 3	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Carly Miller - Carly Miller On Behalf of: Sheila Suurmeier, Black Hills Corporation, 5, 6, 1, 3; - Carly Miller	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1	
Answer	
Document Name	
Comment	

Black Hills Corporation will not comment on cost effectiveness.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt

Answer	
Document Name	

Comment

Black Hills Corporation will not comment on cost effectiveness.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	
Document Name	

Comment

NEE does not comment on costs.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	
Document Name	

Comment

NA

Likes 0	
Dislikes 0	
Response	

5. Provide any additional comments on the standard and technical rationale for the SDT to consider, if desired.

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE

Answer	
Document Name	

Comment

While PNMR does agree that coordinated attacks present risk, it is unclear as to the realized risk associated with a coordinated attack utilizing multiple low-impact BES Cyber Systems. As it would be difficult to quantify the number of low-impact systems needed to be utilized in a potential coordinated attack and with uncertain findings as to the use of low-impact systems to conduct a coordinated attack, PNM believes the potential risk to the BES from such attacks does not sufficiently correlate with the proposed authentication and detection controls which would be a vast expansion of scope.

The NERC Low Impact Criteria Review Report references the risk of coordinated attacks on low impact BES Cyber Systems for those systems that are determined by the CIP-002 Standards. However, the CIP-002 categorization of BES Cyber Systems is not intended to take into account the effect of a coordinated attack in determining the categorization of a BES Cyber System. This language seems to attempt to change the purpose and muddy the scope of the CIP-002 Standard.

PNMR also has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.

Likes 0	
Dislikes 0	

Response

Deanna Carlson - Cowlitz County PUD - 5

Answer	
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	
Document Name	

Comment

none	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	
Comment	
Nothing further to provide at this time.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	
Document Name	
Comment	
The language as proposed fails to clearly identify the target of the compliance objective. Suggest the SDT revise the language to clarify whether the target is the network containing the Low BCS, the Low BCS, or other Cyber Assets contained in the network. The undefined term “electronic remote	

access” used throughout the proposed language lacks sufficient clarity. Suggest the SDT provide a definition to be entered into the NERC Glossary to provide consistent application.	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	
Document Name	
Comment	

SRP feels there is some concern for CIP-003 being written for low impact requirements that contain parts of all existing standards (for medium and high impact). Seems like there is an opportunity to just add low impact requirements to the existing standard(s). This will also help in keeping language consistent.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt

Answer	
Document Name	

Comment

Black Hills Corporation agrees with PNMR and has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.

Likes 0	
Dislikes 0	

Response

Micah Runner - Black Hills Corporation - 1

Answer	
Document Name	

Comment

Black Hills Corporation agrees with PNMR and has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.

Likes 0	
Dislikes 0	

Response

Carly Miller - Carly Miller On Behalf of: Sheila Suurmeier, Black Hills Corporation, 5, 6, 1, 3; - Carly Miller

Answer	
Document Name	

Comment	
Black Hills Corporation agrees with PNMR and has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.	
Likes 0	
Dislikes 0	
Response	
Josh Combs - Black Hills Corporation - 3	
Answer	
Document Name	
Comment	
Black Hills Corporation agrees with PNMR and has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
WECC suggests that the DT consider aligning the wording in Attachment 1 Sections 3.1.5 and 3.1.6 to match the working identified in Attachment 2 Section 3 items #5 and #6, specifically Section 3.1.6.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	

Comment	
The NAGF has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	
Document Name	
Comment	
None at this time.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	

Thank you for the ability to comment.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1

Answer	
Document Name	

Comment

While PNMR does agree that coordinated attacks present risk, it is unclear as to the realized risk associated with a coordinated attack utilizing multiple low-impact BES Cyber Systems. As it would be difficult to quantify the number of low-impact systems needed to be utilized in a potential coordinated attack and with uncertain findings as to the use of low-impact systems to conduct a coordinated attack, PNM believes the potential risk to the BES from such attacks does not sufficiently correlate with the proposed authentication and detection controls which would be a vast expansion of scope.

The NERC Low Impact Criteria Review Report references the risk of coordinated attacks on low impact BES Cyber Systems for those systems that are determined by the CIP-002 Standards. However, the CIP-002 categorization of BES Cyber Systems is not intended to take into account the effect of a coordinated attack in determining the categorization of a BES Cyber System. This language seems to attempt to change the purpose and muddy the scope of the CIP-002 Standard.

PNMR also has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.

Likes 0	
Dislikes 0	

Response

Andrew Smith - APS - Arizona Public Service Co. - 5

Answer	
Document Name	

Comment

AZPS has no additional comments as this time.

Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	

For this statement, there may be a discrepancy in count:

"Lower VSL

The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2)"

Should this be six instead of seven?

Likes 0	
Dislikes 0	
Response	

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	
Document Name	
Comment	

N/A

Likes 0	
Dislikes 0	
Response	

TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	
Document Name	
Comment	

Lower VSL

The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2) Should this be six topics required by R1?	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
(None)	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	

Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
In general, it seems that the SDT has expanded the requirements beyond what was recommended by the LICRT. For example, the LICRT stated there should be a requirement for the “detection of malicious communications to/between assets containing low-impact BES Cyber Systems with ERC.” This languages allows greater flexibility in determining the location of detection compared to the SDT’s specification of “for both inbound and outbound electronic remote access.” Given that access is defined by communication “outside the asset containing low-impact BES Cyber System(s),” this language inherently mandates the detection to occur at he border of the low-impact asset.	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	
Document Name	
Comment	
In general, it seems that the SDT has expanded the requirements beyond what was recommended by the LICRT. For example, the LICRT stated there should be a requirement for the “detection of malicious communications to/between assets containing low-impact BES Cyber Systems with ERC.” This languages allows greater flexibility in determining the location of detection compared to the SDT’s specification of “for both inbound and outbound electronic remote access.” Given that access is defined by communication “outside the asset containing low-impact BES Cyber System(s),” this language inherently mandates the detection to occur at he border of the low-impact asset	
Likes 0	
Dislikes 0	

Response
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators
Answer
Document Name
Comment
We would like to thank the SDT for their hard work.
Likes 0
Dislikes 0
Response
Alison MacKellar - Constellation - 5
Answer
Document Name
Comment
Constellation has no additional comments. Alison Mackellar on behalf of Constellation Segments 5 and 6
Likes 0
Dislikes 0
Response

Comments submitted by Ellese Murphy – Duke Energy

Question 1 – Yes. We support the revisions as posted but do support the alternative language recommendations from EEI for 3.1.4 and 3.1.6 for further clarity.
Question 2 – Yes
Question 3 – Yes
Question 4 – Yes
Question 5 - Duke Energy thanks the drafting team for their work.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2023-04 Modifications to CIP-003 | Draft 1
Comment Period Start Date:	10/24/2023
Comment Period End Date:	12/7/2023
Associated Ballot(s):	2023-04 Modifications to CIP-003 CIP-003-A IN 1 ST 2023-04 Modifications to CIP-003 Implementation Plan IN 1 OT

There were 63 sets of responses, including comments from approximately 165 different people from approximately 104 companies representing 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, contact Director, Standards Development Latrice Harkness (via email) or at (404) 858-8088.

Questions

1. Do you agree with the language proposed in CIP-003-A Attachment 1? If you do not agree, please provide recommended language you would support and, if appropriate, technical or procedural justification.

2. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please provide recommended language you would support and, if appropriate, technical or procedural justification.

3. The Standard Drafting Team (SDT) proposes a three (3) year implementation plan for CIP-003-A. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.

4. The SDT believes the language of CIP-003-A addresses the issues outlined in the SAR in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

5. Provide any additional comments on the standard and technical rationale for the SDT to consider, if desired.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Jaimin Patal	Saskatchewan Power Corporation (SPC)	1	MRO
					Kimberly Bentley	Western Area Power Adminstration	1,6	MRO
					Marc Gomez	Southwestern Power Administration (SWPA)	1	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO

					George Brown	Pattern Operators LP	5	MRO
					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Bryan Sherrow	Board Of Public Utilities (BPU)	1	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Michael Ayotte	ITC Holdings	1	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC

					Nehtisha Rollis	Tennessee Valley Authority	5	SERC
Chris Carnesi	Chris Carnesi		WECC	NCPA	Marty Hostler	Northern California Power Agency	4	WECC
					Dennis Sismaet	Northern California Power Agency	6	WECC
WEC Energy Group, Inc.	Christine Kane	3		WEC Energy Group	Christine Kane	WEC Energy Group	3	RF
					Matthew Beilfuss	WEC Energy Group, Inc.	4	RF
					Clarice Zellmer	WEC Energy Group, Inc.	5	RF
					David Boeshaar	WEC Energy Group, Inc.	6	RF
Manitoba Hydro	Jay Sethi	1,3,5,6	MRO	Manitoba Hydro Group	Nazra Gladu	Manitoba Hydro	1	MRO
					Mike Smith	Manitoba Hydro	3	MRO
					Kristy-Lee Young	Manitoba Hydro	5	MRO
					Kelly Bertholet	Manitoba Hydro	6	MRO
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC

					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Nikki Carson-Marquis	Minnkota Power Cooperative, Inc.	1	MRO

					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
Eversource Energy	Joshua London	1		Eversource	Joshua London	Eversource Energy	1	NPCC
					Vicki O'Leary	Eversource Energy	3	NPCC
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Alain Mukama	Hydro One Networks, Inc.	1	NPCC

Deidre Altobell	Con Edison	1	NPCC
Jeffrey Streifling	NB Power Corporation	1	NPCC
Michele Tondalo	United Illuminating Co.	1	NPCC
Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
Randy Buswell	Vermont Electric Power Company	1	NPCC
James Grant	NYISO	2	NPCC
John Pearson	ISO New England, Inc.	2	NPCC
Harishkumar Subramani Vijay Kumar	Independent Electricity System Operator	2	NPCC
Randy MacDonald	New Brunswick Power Corporation	2	NPCC
Dermot Smyth	Con Ed - Consolidated	1	NPCC

	Edison Co. of New York		
David Burke	Orange and Rockland	3	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
David Kwan	Ontario Power Generation	4	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
Glen Smith	Entergy Services	4	NPCC
Sean Cavote	PSEG	4	NPCC
Jason Chandler	Con Edison	5	NPCC
Tracy MacNicoll	Utility Services	5	NPCC

					Shivaz Chopra	New York Power Authority	6	NPCC
					Vijay Puran	New York State Department of Public Service	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					Joshua London	Eversource Energy	1	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion	5	NA - Not Applicable

						Resources, Inc.		
Steve Toosevich	Steve Toosevich			NIPSCO Compliance	Steven Taddeucci	NiSource - Northern Indiana Public Service Co.	3	RF
					Kathryn Tackett	NiSource - Northern Indiana Public Service Co.	5	RF
					Joseph OBrien	NiSource - Northern Indiana Public Service Co.	6	RF
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC

					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC

Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
Tony Gott	KAMO Electric Cooperative	3	SERC
Micah Breedlove	KAMO Electric Cooperative	1	SERC
Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC

					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. Do you agree with the language proposed in CIP-003-A Attachment 1? If you do not agree, please provide recommended language you would support and, if appropriate, technical or procedural justification.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting. PNMR also supports EEI's comments pertaining to Section 3, parts 3.1.4 and 3.1.6.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can "utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s)." The SDT changed 3.1.3 so that authentication can occur for a "network(s)" meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System). See EEI response.	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	

Regarding the definition of 3.1's scope, the specification of "connectivity that provides the ability to communicate" is confusing and has no opposite state; connectivity in this context implies communication. The addition of "of Protection systems" to iii is also unnecessarily expansive. Language recommendation:

3.1 For routable connectivity:

I. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving a defined perimeter containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., IEC 61850, etc.)

Regarding section 3.1.2, that subsection implies deployment of Intrusion Protection Systems (IPS) at every low impact BES Cyber System for any "connection to communicate". This is technically infeasible for many communication types (e.g., RS-232, RS-485, non-IP IEC 61850, etc.). It would necessitate building routable connectivity to many systems that otherwise do not require it, do not have it, and may be difficult or expensive to build out (see cost feasibility below) simply to deploy a monitoring solution. The added communication risk combined with cost is not an effective risk-based approach to securing low impact BES.

Regarding section 3.1.4, this requirement is overly prescriptive and makes certain assumptions about how connections for communications may be authorized, secured, and used. The requirement should address a security concern topically – e.g. "ensure communications are protected appropriately given a risk-based approach".

Regarding sections 3.1.5 and 3.1.6, we agree with the EEI comments and further assert that the undefined use of "remote access" is problematic and should be scoped to certain types of routable communications Overall, concerns with communication monitoring for low impact BES should be addressed in a risk-based and architecture-based approach rather than a BES location approach specifically because of their lower impact. For example, rather than mandating IPS monitoring and user disablement at a low impact BES, require that interactive remote access be controlled and monitored from central aggregation or choke points (or an architecturally equivalent

concept) and allow the entities to determine a risk-based security partitioning and control plan based on factors within their own environment.

In addition, **FirstEnergy supports EEI's comments** which state:

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authentical and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect BES Cyber System network authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.16 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	
Response	
Change made to structure. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification." See EEI response.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute for question #1.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	

Answer	No
Document Name	
Comment	
AECI is supportive of the approach to consolidate to the electronic access section as adding a new section to capture these revisions would be purely duplicative. I also think that the new revisions are drafted in a way that allows for utilizing solutions that may be put in place for the version 9 for these new revisions if desired but also allowing for separate solutions if needed. The only concern with the current draft language is the use of the following phrase: "to mitigate risks associated with electronic access" in the intro paragraph of Section 3. As written there is a signifigant potential to cause more scrutiny on the allowed communications that did not previously exist and was not part of the SAR, and would give total discression to auditor interpretation.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification."	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The number of Low Impact BES Cyber Systems impacted would make achieving compliance burdensome in terms of level of effort, cost, and required technology implementations.	

Likes 0	
Dislikes 0	

Response

The revisions to CIP-003-9 were made based on the scope of the approved SAR, and the SDT appreciates that there may be cost associated with the implementation of the new standard. The SDT has kept the requirements to a level of granularity that is either the "asset containing low impact BCS" or "networks containing low impact BCS" so that it does not go down to the level of individual BCS or device. The intent is the monitoring of traffic and authentication of users at a higher level than each system due to the large scope of lows.

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment

To accommodate those systems that do not have the capability to perform the required function, such as protecting user authentication information in transit, Tacoma Power recommends including language in Attachment 1, Section 3, such as "per system capability," as found throughout the rest of the CIP Standards. Specifically, Tacoma Power recommends adding the "per system capability" to the lead in to Section 3 of Attachment 1.

Suggested lead in language update:

"Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, to mitigate risks associated with electronic access, the Responsible Entity shall implement controls, **per system capability**, to:"

Additionally, Tacoma Power has a concern that Attachment 1, Section 3 Part 3.1.3 can be read in multiple ways. Specifically as it relates to the (i.) and (ii.) language in the lead-in to Section 3.1 (excerpt as follows):
3.1 For connectivity that provides the ability to communicate:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

What does the phrase "**each instance** of electronic remote access to **networks** containing low impact BES Cyber Systems" mean in Part 3.1.3? We see that the TR includes the desire to allow initial authentication to the network to allow transition to sub-networks, etc. But there is no structure for this within the 3.1 (i.) and (ii.) construct. Tacoma Power is concerned that the language of 3.1.3 does not support the idea of allowed sub-network connections without additional authentication if they are to a different asset containing a low impact BCS, since this ties it back to the original (i.)

In the scenario where a relay tech logs into a central system which includes configurations to access relays at several substations, is that relay tech required to re-authenticate each time they access a relay at a different substation (i.e., at a different asset containing Low Impact BCS)? The language of the Requirement does not provide clarity to this situation.

To aid in this scenario, Tacoma Power suggests the following language for clarity of Attachment 1 Section 3 Part 3.1.3:

"3.1.3 Authenticate users when remotely accessing networks containing low impact BES Cyber Systems."

Likes 1	LaKenya Vannorman, N/A, Vannorman LaKenya
Dislikes 0	

Response

1. The SDT has not included "per system capability" within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the "networks containing" or "asset containing level". The SDT also clarified the Section 3 language to also incorporate "Intermediate System" style implementations as well.
2. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can "utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s)." The SDT changed 3.1.3 so that authentication can occur for a "network(s)" meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System).

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments. Dominion Energy supports in part the proposed changes to CIP-003-A Attachment 1, but disagree with the addition of proposed 3.1.5 and 3.1.6 and the deletion of Section 6. First, the SAR only authorized the change to Section 3 and the current language in Section 6 is clearer than what is proposed. We suggest deleting 3.1.5 and 3.1.6 and restoring Section 6 to address the concerns.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Change made. The SDT has reviewed your comment and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No
Document Name	
Comment	
Eversource agrees with the comments of EEI.	

Likes 0	
Dislikes 0	
Response	
See EEI response.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
The NERC Low Impact Criteria Review Report mentions the risk of coordinated attacks on low impact BES Cyber Systems that could adversely affect the BES. However, coordinated attacks are not considered for categorization of BES Cyber Systems in CIP-002, and the proposed language in CIP-003 is placing more restrictive controls on low impact BCS than medium impact BCS without ERC. For example, in 3.1.4, protecting user authentication information all the way to the asset is more restrictive than the current requirements for high and medium impact BCS, where an Intermediate System authenticates the user who is then allowed to then access high/medium impact BCS as needed. While the risk to a coordinated attack to multiple low impact BCS is not zero, the restrictive and prescriptive controls proposed does not allow a Responsible Entity to determine the best way to protect its low impact BCS. In 3.1.3, the language “each instance” is ambiguous and should be removed to avoid confusion or misinterpretation. Also, the lack of a clear definition of remote access further adds to the ambiguity and should be clarified or defined. “Per Cyber System/Asset capability” should be added to address those cyber assets that have limitations or cannot be replaced/upgraded without significant expense.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would	

not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System).

The SDT has not included "per system capability" within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the "networks containing" or "asset containing level". The SDT also clarified the Section 3 language to also incorporate "Intermediate System" style implementations as well.

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	

Manitoba Hydro recognizes the standard drafting team's effort to develop a draft that clearly outlines requirements meeting the objectives of the project. There appears to be a disconnect in the two requirements to authenticate access and protect this information in transit.

Requirement 3.1.3 requires that access be authenticated at the time of permitting that access to the network containing low impact BES Cyber Systems. This requirement is worded flexibly to allow a number of technical solutions to accomplish the security objective. Requirement 3.1.4 specifies that authentication information be protected in transit from the asset containing low impact BES Cyber Systems. The implementation of 3.1.3 may be configured to have a central point of authentication that is not located at the asset. The text of 3.1.4 takes away flexibility in implementation. The following text is suggested based on the currently accepted wording in CIP-005 for Medium Impact Cyber Assets:

For all instances of electronic remote access to networks containing low impact BES Cyber Systems, protect user authentication information in transit in between the remote client and the authentication system used to meet 3.1.3.

The intent of requirement 3.1.6 is clear, however as currently worded it seems to require all vendor remote access to be disabled at all times. Manitoba Hydro suggests the following wording:

Have a documented method to disable vendor electronic remote access, where vendor electronic remote access is permitted.	
Likes 0	
Dislikes 0	

Response

Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can "utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s)." The SDT changed 3.1.3 so that authentication can occur for a "network(s)" meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System).

Thank you for your comment. Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	

Comment

With new language there will be a large amount of Low Impact BES Cyber Systems impacted. It would be costly for utilities to meet compliance and more burdensome than medium and high impact requirements.

Likes 0	
Dislikes 0	

Response
No change. The SDT notes that the required cyber security program for lows is not stricter than the required program for mediums w/o ERC. Medium impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems' level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The SDT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums.

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
Section 3 in att 1 does not make grammatical sense nor does it flow. There is concern for auditor interpretation to vary. In addtion, SRP is in support of Tacoma Power's comment on the suggested language as it can be interpreted in multiple ways.	
Likes 0	
Dislikes 0	

Response
Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

1. Section 3.1.2 creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers: the proposed language requires detection of known/suspected malicious communications for "inbound and outbound electronic remote access." There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5).

BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS.

2. Section 3.1.4 creates a higher compliance bar for Low BCS than for Medium BCS: in the latest Draft 5 of CIP-005-8 R2.2 - 2.3, the proposed requirements include only Interactive Remote Access, or human-initiated access. Section 3.1.4 includes all "information in transit to or from the asset containing low impact BES Cyber Systems."

BPA suggests that this requirement be aligned with the latest Draft 5 of CIP-005-8 R2.2 - 2.3: "3.1.4 Protect user authentication *of IRA communications* in transit to or from the asset containing low impact BES Cyber Systems."

3. Section 3.1.6: While BPA appreciates the committee's intent to "present a single section for all electronic access" (Technical Rationale, p. 2), Section 3.1.6 is nonetheless awkwardly worded. It either suggests that all vendor remote access should be disabled (rather than requiring controls that could provide an option to disable vendor remote access), or it contradicts itself in a nonsensical sentence by saying that when vendor access is permitted, it should always be disabled.

BPA suggests aligning with the language used in Draft 5 of CIP-003-10, such as "Have one or more methods" for determining and disabling vendor remote access sessions.

Likes 0	
Dislikes 0	

Response

1. No change. The revisions made to 3.1.2 are within the scope of the SAR.

2. Change made. Added “user-initiated instances” to the language. The DT chose not to specifically use the IRA, because of the relation with Medium/Highs and verbiage in the definition. Additionally, an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).”
3. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.”

   Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	
Please clarify whether vendor electronic remote access includes cases involving protocol transition between serial and TCP/IP.	
Likes 0	
Dislikes 0	
Response	
No change. This is specified in Section 3.1 (ii). The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and	

modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authentical and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **user BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.16 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response

See EEI response.

Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt

Answer	No
Document Name	

Comment

Black Hills Corporation agrees with the comments below from EEI, FE, and PNM Resources – Public Service Company of New Mexico.

Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting.

Regarding sections 3.1.5 and 3.1.6, we agree with the EEI comments and further assert that the undefined use of “remote access” is problematic and should be scoped to certain types of routable communications. Overall, concerns with communication monitoring for low impact BES should be addressed in a risk-based and architecture-based approach rather than a BES location approach specifically because of their lower impact. For example, rather than mandating IPS monitoring and user disablement at a low impact BES, require that interactive remote access be controlled and monitored from central aggregation or choke points (or an architecturally equivalent

concept) and allow the entities to determine a risk-based security partitioning and control plan based on factors within their own environment.

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authenticate and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.1.6 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	
Response	
See EEI, FE and PNM Resources responses.	
Micah Runner - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	

Black Hills Corporation agrees with the comments below from EEI, FE, and PNM Resources – Public Service Company of New Mexico.

Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting.

Regarding sections 3.1.5 and 3.1.6, we agree with the EEI comments and further assert that the undefined use of "remote access" is problematic and should be scoped to certain types of routable communications Overall, concerns with communication monitoring for low impact BES should be addressed in a risk-based and architecture-based approach rather than a BES location approach specifically because of their lower impact. For example, rather than mandating IPS monitoring and user disablement at a low impact BES, require that interactive remote access be controlled and monitored from central aggregation or choke points (or an architecturally equivalent concept) and allow the entities to determine a risk-based security partitioning and control plan based on factors within their own environment.

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR;

these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authenticate and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.1.6 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response
See EEI, FE and PNM Resources responses.

Carly Miller - Carly Miller On Behalf of: Sheila Suurmeier, Black Hills Corporation, 5, 6, 1, 3; - Carly Miller	
Answer	No

Document Name	
Comment	

Black Hills Corporation agrees with the comments below from EEI, FE, and PNM Resources – Public Service Company of New Mexico.

Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting.

Regarding sections 3.1.5 and 3.1.6, we agree with the EEI comments and further assert that the undefined use of "remote access" is problematic and should be scoped to certain types of routable communications. Overall, concerns with communication monitoring for low impact BES should be addressed in a risk-based and architecture-based approach rather than a BES location approach specifically because of their lower impact. For example, rather than mandating IPS monitoring and user disablement at a low impact BES, require that interactive remote access be controlled and monitored from central aggregation or choke points (or an architecturally equivalent concept) and allow the entities to determine a risk-based security partitioning and control plan based on factors within their own environment.

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authenticate and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would

only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.1.6 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response

See EEI, FE and PNM Resources responses.

Josh Combs - Black Hills Corporation - 3

Answer	No
Document Name	

Comment

Black Hills Corporation agrees with the comments below from EEI, FE, and PNM Resources – Public Service Company of New Mexico.

Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be

permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting.

Regarding sections 3.1.5 and 3.1.6, we agree with the EEI comments and further assert that the undefined use of "remote access" is problematic and should be scoped to certain types of routable communications. Overall, concerns with communication monitoring for low impact BES should be addressed in a risk-based and architecture-based approach rather than a BES location approach specifically because of their lower impact. For example, rather than mandating IPS monitoring and user disablement at a low impact BES, require that interactive remote access be controlled and monitored from central aggregation or choke points (or an architecturally equivalent concept) and allow the entities to determine a risk-based security partitioning and control plan based on factors within their own environment.

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authenticate and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.1.6 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	
Dislikes 0	

Response

See EEI, FE and PNM Resources responses.

Ben Hammer - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

Remove Requirement 2 from the standard all together, add in requirements of attachment 1 for low impact BES Cyber systems into the correct CIP standard, CIP-004, CIP-006, CIP-005, CIP-008, and CIP-010 as needed.

There is no definition for the word communicate. This needs to be defined or changed to use the correct terminology.

The language “using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and” is not clear as written. As an example, an entity can have a routable protocol that enters the low impact asset, that never communicates using a bidirectional routable protocol with any Low impact BES Cyber Assets. This creates an undue burden for Registered entities to protect assets that have no routable connectivity.

The definition of vendor needs to be defined and **should not** include long-term /fulltime contract employees that work for the Registered entity.	
Likes 0	
Dislikes 0	
Response	
1. The SDT is not authorized in the SAR to revise all of the standards listed. By having the low impact contained in CIP-002 and CIP-003, this allows "low impact only Entities" to comply with those two standards. 2. The items under 3.1 (i) (ii) and (iii) are to be read as an AND statement. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification. 3. The SDT does not intend to define the term vendor. Please see Project 2020-03 Technical Rationale.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
As proposed, CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4 does not consider per Cyber System capability and may create an impossibility to comply within the implementation timeline without wholesale upgrades or replacements of technology and communications infrastructure. While this newly proposed Requirement Part is consistent with the LICRT report and the subsequent approved SAR; protections from the user all the way through to the asset containing the BCS imposes a mandatory obligation for low impact that is above and beyond the current enforceable requirements set forth for high and medium impact BCS, and also precludes the use of established and current	

enforceable concepts used to protect user authentication information for high and medium impact like IRA through an Intermediate System.

The protections for user authentication information in transit between a user and a high or medium impact BCS are between the user and the Intermediate System, and do not extend all the way to the asset containing the high or medium impact BCS. Here, user authentication information is protected between the initiating device and the Intermediate System, and once authenticated to the Intermediate System, the Requirement language would permit the use of any protocol the entity chooses (Telnet, for example) to make the connection from the Intermediate System to the BCS. Proxied connections/new sessions established from the Intermediate System to the BCS are permitted to transverse unencrypted communication links and use unencrypted protocols (which may be the only method depending on the entity's technology). If "Telnet" is the only method that can be used, there is also no obligation to block clear test interactive protocols from going through a high or medium impact ESP if they are needed, nor to force a VPN tunnel or communication link encryption to do so.

There is no obligation to "protect user authentication information" all the way to the asset containing the BCS for high and medium impact, and to mandate this for low impact does not seem commensurate with risk. CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as written, would only permit the use of an Intermediate System if the Intermediate System were physically located within the asset containing the LBCS, instead of permitting entities to leverage existing centralized infrastructure already implemented for the purpose of protecting user authentication information for high or medium impact.

NSRF requests further SDT consideration of the addition of "per Cyber System capability" language, and the addition of options that would permit protection of user authentication information in transit between the user and an Intermediate System, or the asset containing low impact BES Cyber Systems.

The SAR only directed "protection of user authentication information in transit for **remote access to networks** containing low impact BES Cyber Systems." This would only include network access credentials which could be authenticated locally, precluding the need for these credentials to transit to the asset containing low impact BCS's. Thus, current implementations could remain compliant according to the direction of the SAR.

The proposed language of 3.1.4 expands the SAR mandate to protect all authentication information, which includes account passwords of the low impact BCS's, which requires transmitting these credentials to the BCS's. It is the expansion of the scope of the SAR regarding which credentials need to be protected that makes the proposed 3.1.4 language incompatible with current compliant practices.

If 3.1.4 were re-worded from *"Protect user authentication information"* to *"Protect network authentication information,"* this would expand compliance options to include local authentication and avoid having to send network credentials to the asset.

NSRF offers the following potential language for SDT consideration:

3.1.4 Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems if using public communication links;

3.1.4 Protect user authentication information in transit to the asset containing low impact BES Cyber Systems, unless low impact BES Cyber System remote access is already protected by going through an Intermediate System meeting the collective requirement parts of CIP-005-7 Requirement R2; if using public communication links, protect user authentication information in transit to and from the asset containing low impact BES Cyber Systems;

3.1.4 Protect user authentication information in transit:

- *BES Cyber Systems if to or from the asset containing low impact using public communication links; or*
- *to the asset containing the low impact BES Cyber Systems if using private communication links, unless low impact BES Cyber System remote access is already protected by going through an Intermediate System meeting the collective requirement parts of CIP-005-7 Requirement R2.*

3.1.4 For all instances of electronic remote access to networks containing low impact BES Cyber Systems, protect user authentication information in transit in between the remote client and the authentication system used to meet 3.1.3.

Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	

Response

1. The SDT has not included "per system capability" within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the "networks containing" or "asset containing level". The SDT also clarified the Section 3 language to also incorporate "Intermediate System" style implementations as well.
2. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can "utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact

cyber security plan(s)." The SDT changed 3.1.3 so that authentication can occur for a "network(s)" meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System).	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is in support of EEIs response to this question.	
Likes 0	
Dislikes 0	

Response	
See EEI response.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	

LCRA seeks clarification on what “outbound electronic remote access” means. Additionally, the use of the word “remote” throughout the entirety of Section 3 seems inappropriate when discussing the various types of electronic access communications.

We are confused with the roman numerals in section 3.1 that are used to define applicability. LCRA believes that the electronic access being defines here would better be served by a NERC Glossary of Terms definition. This would enable this section to read more clearly.

Section 3.1.2 requires stronger controls than medium impact BES Cyber Systems not at Control Centers. This goes against the Brightline criteria.

Section 3.1.3 requires that authentication occurs when permitting each instance of electronic remote access. LCRA is concerned with the scoping of this requirement when managing connection over Wide Area Network (WAN). It is unclear if intermediate systems or equivalent could be used to achieve compliance.

Section 3.1.5 & 3.1.6 consider restructuring the sentences to avoid confusion. LCRA suggests the following revision:

* 3.1.5 – Implement measures to determine vendor electronic remote access

* 3.1.6 – Implement measures to disable vendor electronic remote access, where enabled

Likes 0	
Dislikes 0	
Response	

1. Change made. The SDT removed the term “remote” from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1.
2. Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.
3. The SDT notes that the required cyber security program for lows is not stricter than the required program for mediums w/o ERC. Medium impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems’ level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The SDT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums.
4. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).
5. Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	

LCRA seeks clarification on what “outbound electronic remote access” means. Additionally, the use of the word “remote” throughout the entirety of Section 3 seems inappropriate when discussing the various types of electronic access communications.

We are confused with the roman numerals in section 3.1 that are used to define applicability. LCRA believes that the electronic access being defines here would better be served by a NERC Glossary of Terms definition. This would enable this section to read more clearly.

Section 3.1.2 requires stronger controls than medium impact BES Cyber Systems not at Control Centers. This goes against the Brightline criteria.

Section 3.1.3 requires that authentication occurs when permitting each instance of electronic remote access. LCRA is concerned with the scoping of this requirement when managing connection over Wide Area Network (WAN). It is unclear if intermediate systems or equivalent could be used to achieve compliance.

Section 3.1.5 & 3.1.6 consider restructuring the sentences to avoid confusion. LCRA suggests the following review:

- 3.1.5 – Implement measures to determine vendor electronic remote access
- 3.1.6 – Implement measures to disable vendor electronic remote access, where enabled

Likes 0	
Dislikes 0	

Response

See LCRA response above.

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

AEPC has signed on to ACES comments below:

ACES feels, “Section 3.1.4 Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems”, should read: Protect electronic remote access information in transit to or from the asset containing low impact BES Cyber Systems;” The addition of authentication of remote users we are fine with, but the SDT chose to just scope in protection of remote user authentication information and we feel that is not the only thing that should be protected. Just like in the case of detection of vendor communication versus all communications (fixed in this version), we feel ALL electronic remote access information should be protected just as it is in CIP-005 R2 if it’s FERC/NERC’s intention of reducing overall cybersecurity risk with this change. Without fully protecting the entire remote access session, risks are only minimally reduced and this standard will have to be revised again to meet the objective.	
Likes 0	
Dislikes 0	
Response	
See ACES response.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
SMUD and BANC appreciate the Standards Drafting Team’s efforts to revise Attachment 1. Section 3.1.1 reads “Permit only necessary inbound and outbound remote electronic access as determined by the responsible entity.” Using the word “remote” in this section narrows the scope of Electronic Access Controls to only inbound and outbound electronic access that is “remote access.” The technical rationale is incorrect in that using this wording does not “maintain the original language used in CIP-003-9, Section 3.1” as CIP-003-9 is more specific.	

We feel there is no need to use the word “remote” in Section 3.1.1 as it is already included when an entity “Permits only necessary inbound and outbound electronic access as determined by the Responsible Entity.” If using the word “remote” is deemed necessary, the Standards Drafting Team should provide some clarity as it is not very clear what “remote” electronic access is. We feel that “remote” is already covered by Section 3.1.1.i: “between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);” The same comment applies to Sections 3.1.2 and 3.1.3 as it is not clear how using the word “remote” clarifies anything. Additionally, we believe the language in the Standards Authorization Request is proposing more strict controls/requirements for low impact BCS than the controls/requirements currently being proposed for high impact BCS and medium impact BCS in CIP-005-8 Requirements R2.1 - 2.4, and CIP-007-7 Requirement R1.1.

Likes 0	
Dislikes 0	

Response
Change made. The SDT removed the term “remote” from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1. No change. The SDT notes that the required cyber security program for lows is not stricter than the required program for mediums w/o ERC. Medium impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems’ level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The SDT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums.

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No

Document Name	
Comment	

EEI supports in part the proposed changes to CIP-003-A Attachment 1, but we do not support the changes made to Section 3, parts 3.1.4 and 3.1.6. Our concerns to these two sections are described below:

Section 3, part 3.1.4, does not consider the impacts on existing CIP Cyber System potentially rendering those systems obsolete necessitating their replacement. While the proposed changes are consistent with the LICRT report and the subsequent approved SAR; these modifications would obligate entities to apply protections for user authentication and access to low impact BCS that exceed the currently enforceable requirements set forth for high and medium impact BCS. Also, these proposed changes would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS. An example of this concern would be communications through Intermediate Systems.

Further, existing requirements for user authentication information in transit between a user and a high or medium impact BCS are limited to the user and the Intermediate System, and do not extend to the asset containing the high or medium impact BCS. In contrast, a similar approach for low impact BCS would not be allowed rendering any dual use of systems used to authentical and protect user access to low impact BCS not possible. Noting that CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4, as proposed, would only permit the use of an Intermediate System if those Intermediate Systems were physically located within the asset containing the low impact BCS. Such a requirement would prevent entities from leveraging existing centralized infrastructure already in place and used to protect user authentication information for high or medium impact.

To address our concerns, we offer the following proposed edits to 3.1.4 in bold face below:

3.1.4 Protect **BES Cyber System network** authentication information in transit to or from the asset containing low impact BES Cyber Systems;

Section 3, part 3.1.6, should be clarified to ensure that entities are to have the ability to disable vendor electronic remote access when needed. To address this concern, we offer the following change to 3.16 in bold face below:

3.1.6 **Ability to** disable vendor electronic remote access, **when necessary**, where vendor electronic remote access is permitted.

Likes 0	

Dislikes 0	

Response
Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can "utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s)." The SDT changed 3.1.3 so that authentication can occur for a "network(s)" meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System). Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.

Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	No
Document Name	

Comment
We support NPCC RSC Comments

Likes 0	
Dislikes 0	

Response
See NPCC RSC response.

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1

Answer	No
Document Name	
Comment	
Section 3.1, specifically 3.1.3, is limited to the means of authentication that can be used. The standard needs to allow for a LIBCS Intermediate System equivalent. If a person could authenticate to the LIBCS Intermediate System, then remote access could be permitted from it to the Cyber Assets at the Low Impact Asset. Not all field devices support authentication, and this would help provide a means of authentication before connecting. PNMR also supports EEI's comments pertaining to Section 3, parts 3.1.4 and 3.1.6.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can "utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s)." The SDT changed 3.1.3 so that authentication can occur for a "network(s)" meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System). See EEI response.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	

ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
AZPS does not agree with proposed language in Attachment 1 Section 3.1.4 and 3.1.6, for the other sections AZPS agrees. AZPS supports the comments and recommendations made on behalf of EEI to clarify sections 3.1.4 and 3.1.6. to ensure existing protections involving an Intermediate System meeting CIP-005-7 requirements can be utilized where applicable and protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems if using public communication links.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	No

Document Name	
Comment	
No NCPA agrees with several other comments that the proposed language places a high level of burden on entities to protect low impact assets. 3.1.2 – Would greatly increase the demand to implement and maintain a IDS type deployment and continuously update and monitor such traffic 3.1.3 – The phrase “each instances” is not well defined and does not appear anywhere else in the standards. 3.1.4 – This language requires a higher level of security than High/Med assets 3.1.6 – Needs clarification of when to disable vendor remote access	
Likes 0	
Dislikes 0	
Response	
For 3.1.2, the revisions to CIP-003-9 were made based on the scope of the approved SAR, and the DT appreciates that there may be cost associated with the implementation of the new standard. Change made. Revised to “each user-initiated instance”. The SDT notes that the required cyber security program for lows is not stricter than the required program for mediums w/o ERC. Medium impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems’ level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The SDT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area	

than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums. 3.1.6. Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) requests additional clarity from the SDT on the intent of section 3.1 iii in the Electronic Access Controls section in which the phrase “time-sensitive communications” is referenced. CEHE believes that the language, while being overtly prescriptive, is also vague and does not entirely explain which time-sensitive protocols are being referenced. CEHE would like to request a better explanation of the inferred time-sensitive protocols included in this section.	
Likes 0	
Dislikes 0	
Response	
No change. Please see the definition for Protection Systems, which gives more context for time-sensitive “communications”. Also refer to CIP-003-8 Technical Rationale/GTB.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	

Comment	
WEC Energy Group supports and incorporates by reference the comments of the MRO (NSRF) Group for Question 1.	
Likes 0	
Dislikes 0	
Response	
See MRO NSRF response.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	

Terminology used within 3.1 doesn't distinguish existing "electronic access" from the new term "electronic remote access." The use of the terminology "electronic remote access" generally refers to interactive remote access. Using the terminology "electronic remote access" for 3.1.1 and 3.1.2 will cause confusion.

Suggest changing 3.1.1 and 3.1.2 by deleting the word "remote" as follows:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic access; …

If the SDT retains the word "remote", the SDT should consider defining "electronic remote access" or alternatively revising "Interactive Remote Access" by adding the following statement to the existing definition of "Interactive Remove Access": **Interactive Remote Access includes remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s).** The revised definition would read as follows and should be used in place of "electronic remote access".

Proposed Revision of Interactive Remote Access: User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). **Interactive Remote Access includes remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s).** Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT removed the term "remote" from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	

NST respectfully offers the following observations and recommendations:

We suggest revising 3.1.4 "Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems" to say, "Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems from unauthorized disclosure." Given the fact the Technical Rationale document states explicitly the purpose of this requirement is to protect the confidentiality of user authentication data, we believe the requirement itself should also make this explicit.

Regarding requirements 3.1.5 and 3.1.6 (determining and disabling vendor remote access, respectively, NST notes that although the Technical Rational states the SDT's objective is to "maintain the original language used in CIP-003-9" Sections 6.1 and 6.2, this has not been done. As a presumably unintended result, the current wording of 3.1.6 ("Disable vendor electronic remote access, where vendor electronic remote access is permitted"), if interpreted literally, would require an entity to block all vendor remote access. We recommend addressing this problem by using CIP-003-9's existing language for determining and disabling vendor remote access.

Regarding the SDT's decision to merge CIP-003-9 Sections 3 and 6, NST disagrees with the SDT's assertion, "Section 6 has not been implemented or required by industry at this time and therefore there would be no impact to merging it with Section 3." While this is presently true, Registered Entities will be obliged to address requirements in Section 6 on 4/1/2026, which we expect will be at least a year before a newer version of CIP-003 that incorporates this project's changes becomes effective. We therefore believe it would be less disruptive to only move malicious communications detection from Section 6 to Section 3, leaving the other two vendor remote access requirements unchanged.

Likes 0	
Dislikes 0	

Response

Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).

Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.

Regarding the Implementation Plan, see implementation plan section for response.

Kimberly Turco - Constellation - 6	
Answer	No
Document Name	

Comment

To accommodate those systems that do not have the capability to perform the required function, such as protecting user authentication information in transit, Constellation recommends including language in Attachment 1, Section 3, such as "per system capability," as found throughout the rest of the CIP Standards. Specifically, Tacoma Power recommends adding the "per system capability" to the lead into Section 3 of Attachment 1. Suggested lead in language update: "Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, to mitigate risks associated with electronic access, the Responsible Entity shall implement controls, per system capability, to:"

Kimberly Turco on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

The SDT has not included “per system capability” within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to also incorporate “Intermediate System” style implementations as well.

See Tacoma Power response.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
NV Energy supports the comments from MRO NSRF and EEI as they relate to 3.1.4.	
Likes 0	
Dislikes 0	
Response	
See MRO NSRF and EEI response.	

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren supports EEI's comments on this question.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No

Document Name	
Comment	

The modification to 3.1 iii is more limiting than intended. There are time-sensitive communications protocols that are unrelated to Protection Systems.

The modification to 3.1 iii could benefit from further clarification to ensure it aligns with the intended purpose and ensure industry is clear on the potential impact of this change.

Regarding 3.1.1, it would be helpful to have a clearer explanation in the Technical Rationale (TR)for changing the language to "permitting only necessary inbound/outbound REMOTE access." The objective of the TR to “maintain the original language” could be addressed more effectively by the SDT.

Although 3.1.2 exceeds the Standards for Medium Impact and incurs substantial costs. The challenge lies in the fact these terms have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, their reuse should be restricted, and any lesser measures, such as monitoring firewall logs, should not be authorized.

The prescriptiveness of 3.1.3 seems to go beyond what is typically expected for Medium Impact.

Similarly, 3.1.4 appears to exceed the standards for Medium Impact. It would be helpful to revisit this requirement as well.

With regards to 3.1.5 and 3.1.6, the change from "have methods" to "implement controls to" introduces some ambiguity and alters the previously approved requirements. Implementing a control to determine vendor electronic remote access seems very different than having methods for determining vendor electronic remote access. The technical rationale suggests that the SDT intends to uphold the initial language, despite having, in reality, modified the language.

Likes 0	
Dislikes 0	

Response

1. No change. This revision was updated based on CIP-003-10 version from Project 2016-02, which was approved by industry ballot.

2. Change made. The SDT removed the term “remote” from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1.
3. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).
4. Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.

Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	

Comment

The modification to 3.1 iii is more limiting than intended. There are time-sensitive communications protocols that are unrelated to Protection Systems.

The modification to 3.1 iii could benefit from further clarification to ensure it aligns with the intended purpose and ensure industry is clear on the potential impact of this change.

Regarding 3.1.1, it would be helpful to have a clearer explanation in the Technical Rationale (TR)for changing the language to "permitting only necessary inbound/outbound REMOTE access." The objective of the TR to “maintain the original language” could be addressed more effectively by the SDT.

Although 3.1.2 exceeds the Standards for Medium Impact and incurs substantial costs. The challenge lies in the fact these terms have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, their reuse should be restricted, and any lesser measures, such as monitoring firewall logs, should not be authorized.

The prescriptiveness of 3.1.3 seems to go beyond what is typically expected for Medium Impact. Similarly, 3.1.4 appears to exceed the standards for Medium Impact. It would be helpful to revisit this requirement as well. With regards to 3.1.5 and 3.1.6, the change from "have methods" to "implement controls to" introduces some ambiguity and alters the previously approved requirements. Implementing a control to determine vendor electronic remote access seems very different than having methods for determining vendor electronic remote access. The technical rationale suggests that the SDT intends to uphold the initial language, despite having, in reality, modified the language.	
Likes 0	
Dislikes 0	
Response	
See response above.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	
ACES feels, “Section 3.1.4 Protect user authentication information in transit to or from the asset containing low impact BES Cyber Systems”, should read: Protect electronic remote access information in transit to or from the asset containing low impact BES Cyber Systems;” The addition of authentication of remote users we are fine with, but the SDT chose to just scope in protection of remote user authentication information and we feel that is not the only thing that should be protected. Just like in the case of detection of vendor communication versus all communications (fixed in this version), we feel ALL electronic remote access information should be protected just as it is in CIP-005 R2 if it’s FERC/NERC’s intention of reducing overall cybersecurity risk with this change. Without fully protecting the entire remote access session, risks are only minimally reduced and this standard will have to be revised again to meet the objective.	
Likes 0	

Dislikes 0	

Response

No change. Thank you for the comment. The SDT intent was to stay within the scope outlined in the SAR and the LICRT Report, both of which specifically mention user authentication information.

Alison MacKellar - Constellation - 5

Answer	No
Document Name	

Comment

To accommodate those systems that do not have the capability to perform the required function, such as protecting user authentication information in transit, Constellation recommends including language in Attachment 1, Section 3, such as "per system capability," as found throughout the rest of the CIP Standards. Specifically, Tacoma Power recommends adding the "per system capability" to the lead into Section 3 of Attachment 1. Suggested lead in language update: "Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, to mitigate risks associated with electronic access, the Responsible Entity shall implement controls, per system capability, to:"

Alison Mackellar on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

The SDT has not included “per system capability” within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to also incorporate “Intermediate System” style implementations as well.

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments. Please clarify whether vendor electronic remote access includes cases involving protocol transition between serial and TCP/IP.	
Likes 0	
Dislikes 0	
Response	
See NPCC RSC response.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports the comments of MRO NSRF and EEI.	
Likes 0	
Dislikes 0	
Response	
See MRO NSRF and EEI responses.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No

Document Name	
Comment	
Texas RE agrees with the proposed language in Sections 3.1.2, 3.1.3, 3.1.4, 3.1.5, and 3.1.6. Texas is concerned, however, with the term electronic remote access in Section 3.1. This phrase changes the scope of the requirement to potentially no longer include communications that are not used for remote access. For example, the proposed addition of "remote" could arguably exclude Domain Name System (DNS) and ping queries from the scope of the CIP-003 protections, potentially allowing unnecessary electronic access using these types of traffic. Such traffic has been associated with malicious attacks, including DNS cache poisoning and other activities that are not exclusively linked to remote access. As such, there is a potential reliability gap if this language is retained. Texas RE recommends removing the word “remote” in Section 3.1.1.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT removed the term “remote” from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1. Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
The proposed language of Section 3 has lists within lists. This makes it difficult to understand how the items in each list apply to each other. The roman numerals i-iii apply to 3.1.1.-3.1.6. but this may be misinterpreted in future CMEP engagements. This also causes the standard to deviate from what is understood to be the NERC style “and/or” lists. As proposed, 3.1 and 3.2 are the list items for the Section 3 language “Responsible Entity shall implement controls to:”. Since 3.1 and 3.2 are the two items in a list, 3.1 should end with the word “and” to differentiate it from an “or” list. Propose the following changing “…the Responsible Entity shall implement controls to:” to “…the Responsible Entity shall implement the following controls.”	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.	

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed language in CIP-003-A Attachment 1.	
Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	
Response	

Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	

Although we can agree with the proposed changes, we have a suggested change to Attachment 1, Section 3.1.3 in the event another draft is necessary:

The currently proposed langage is "Authenticate users when permitting each instance of electronic remote access to networks containing low impact BES Cyber Systems;".

MRO suggests using language more similar to the definition of Interactive Remote Access (IRA). IRA is defined as “user-initiated access by a person a remote access client or other remote access technology…”. Considering that, MRO suggests inserting "user-initiated" following the word "each" on that proposed language, which would result in "Authenticate users when permitting each **user-initiated** instance of electronic remote access to networks containing low impact BES Cyber Systems;".

Without such a change, the proposed language can be interpreted as introducing system-to-system communications into the equation, which we don't believe was intended.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steve Toosevich - Steve Toosevich, Group Name NIPSCO Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy – Duke Energy	
Answer	Yes
Document Name	
Comment	
We support the revisions as posted but do support the alternative language recommendations from EEI for 3.1.4 and 3.1.6 for further clarity.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	

2. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please provide recommended language you would support and, if appropriate, technical or procedural justification.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports the comments of MRO NSRF and EEI.	
Likes 0	
Dislikes 0	
Response	
See MRO NSRF and EEI responses.	
Alison MacKellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation recommends changing CIP-003-A, Attachment 2, in conformance with our comments to Question 1. Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

See SDT response to Constellation comments in Question 1.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
We do not concur with the proposed language in Attachment 2 for the same reasons we do not agree with the language in Attachment 1. Please see the response to question 1 above.	
Likes 0	
Dislikes 0	
Response	
See SDT response to Georgia Transmission Corporation comments in Question 1. Additionally, the SDT made conforming changes to Attachment 2 based on new revisions made to Attachment 1. The intent of these revisions was to clarify what type of electronic access was in scope and add more examples of evidence that may be conducive for other network configurations, such as those where Responsible Entities use an Intermediate System(s) to facilitate user-initiated instances of electronic access to multiple BES Cyber Systems with varying impact levels.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
We do not concur with the proposed language in Attachment 2 for the same reasons we do not agree with the language in Attachment 1. Please see the response to question 1 above.	
Likes 0	
Dislikes 0	

Response	
See SDT response to Georgia System Operations Corporation comments in Question 1. Additionally, the SDT made conforming changes to Attachment 2 based on new revisions made to Attachment 1. The intent of these revisions was to clarify what type of electronic access was in scope and add more examples of evidence that may be conducive for other network configurations, such as those where Responsible Entities use an Intermediate System(s) to facilitate user-initiated instances of electronic access to multiple BES Cyber Systems with varying impact levels.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren supports EEI's comments on this question.	
Likes 0	
Dislikes 0	

Response	
See EEI response.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation recommends changing CIP-003-A, Attachment 2, in conformance with our comments to Question 1. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

See SDT's response to above Constellation comments in question 2.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
As per our response to Question 1, NST recommends leaving requirements for detecting and disabling vendor remote access in Section 6, moving only malicious communications detection to Section 3.	
Likes 0	
Dislikes 0	
Response	
See SDT response to NST comments in Question 1.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
Terminology used within Section 3. does not distinguish existing "electronic access" from the new term "electronic remote access." The use of the terminology "electronic remote access" generally refers to interactive remote access. Using the terminology "electronic remote access" for Section 3. Item 1 may cause confusion. SDT should consider defining "electronic remote access" or redefining "Interactive Remote Access" as follows and using that in place of "electronic remote access."	

Continent-wide Term

Interactive Remote Access

Definition

User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Interactive Remote Access includes remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Suggest changing Section 3. Item 1 as follows:

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

1. Documentation For Section 3.1.1, documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive these communications are time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative Protection Systems, such as:

Suggest changing Section 3. Item 5 as follows for consistency: "5. For Section 3.1.5 documentation showing the ability to determine vendor electronic remote access, such as…"	
Likes 0	
Dislikes 0	
Response	
See SDT response to Southern Indiana Gas and Electric Co. comments in Question 1.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group supports and incorporates by reference the comments of the MRO (NSRF) Group for Question 2.	
Likes 0	
Dislikes 0	
Response	
See MRO NSRF response.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

Terminology used within Section 3. does not distinguish existing “electronic access” from the new term “electronic remote access.” The use of the terminology “electronic remote access” generally refers to interactive remote access. Using the terminology “electronic remote access” for Section 3. Item 1 may cause confusion.

SDT should consider defining “electronic remote access” or redefining “Interactive Remote Access” as follows and using that in place of “electronic remote access.”

Continent-wide Term

Interactive Remote Access

Definition

User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Interactive Remote Access includes remote access between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Suggest changing Section 3. Item 1 as follows:

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

1. Documentation For Section 3.1.1, documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive these communications are time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative Protection Systems, such as:

Suggest changing Section 3. Item 5 as follows for consistency: "5. For Section 3.1.5 documentation showing the ability to determine vendor electronic remote access, such as..."	
Likes 0	
Dislikes 0	
Response	
See SDT response to CenterPoint Energy comments in Question 1.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	No
Document Name	
Comment	
No NCPA agrees with several other comments that the proposed language places a high level of burden on entities to protect low impact assets. 3.1.2 – Would greatly increase the demand to implement and maintain a IDS type deployment and continuously update and monitor such traffic 3.1.3 – The phrase “each instances” is not well defined and does not appear anywhere else in the standards. 3.1.4 – This language requires a higher level of security than High/Med assets 3.1.6 – Needs clarification of when to disable vendor remote access	

Likes 0	
Dislikes 0	
Response	
See SDT's response to NCPA comments in question 1.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
AZPS does not agree with the proposed language in Attachment 2. AZPS supports EEI's recommendation to add an option that would permit protection of user authentication information in transit between the user and the intermediate system, and not just the asset containing low impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	

Response	
See EEI response.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI does not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's comments and proposed changes as provided in our response to question 1)	
Likes 0	
Dislikes 0	
Response	
The SDT made conforming changes to Attachment 2 based on new revisions made to Attachment 1. The intent of these revisions was to clarify what type of electronic access was in scope and add more examples of evidence that may be conducive for other network configurations, such as those where Responsible Entities use an Intermediate System(s) to facilitate user-initiated electronic access to multiple BES Cyber Systems with varying impact levels.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	

We feel that using the words “outbound electronic remote access” in Section 3 is confusing and we do not think adding the word “remote” so that the language states “… inbound and outbound electronic “remote” access…” clarifies anything. We recommend striking the word “remote”.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT removed the term “remote” from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
Please refer to LCRA’s concerns in question 1.	
Likes 0	
Dislikes 0	
Response	
See SDT’s response to LCRA comments in question 1.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	

Please refer to LCRA's concerns in question 1.	
Likes 0	
Dislikes 0	
Response	
See SDT's response to LCRA comments in question 1.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is in support of EEIs response to this question.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	

Dislikes 0	
Response	
See EEI response.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
For CIP-003-A Requirement R2 Attachment 2, Section 3, Requirement Part 3.1.4, NSRF requests further SDT consideration of an adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the the asset containing low impact BES Cyber Systems.	
Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	
Response	
The SDT made conforming changes to Attachment 2 based on new revisions made to Attachment 1. The intent of these revisions was to clarify what type of electronic access was in scope and add more examples of evidence that may be conducive for other network configurations, such as those where Responsible Entities use an Intermediate System(s) to facilitate user-initiated electronic access to multiple BES Cyber Systems with varying impact levels.	
Ben Hammer - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
see question 1 comments, attachment 2 should be rewritten to cover the appropriate changes based off the comments on question 1.	

Likes 0	
Dislikes 0	
Response	
See SDT's response to WAPA comments in question 1. Additionally, the SDT made conforming changes to Attachment 2 based on new revisions made to Attachment 1.	
Josh Combs - Black Hills Corporation - 3	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with EEI's comments: we do not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's proposed change to question 1)	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Carly Miller - Carly Miller On Behalf of: Sheila Suurmeier, Black Hills Corporation, 5, 6, 1, 3; - Carly Miller	
Answer	No
Document Name	
Comment	

Black Hills Corporation agrees with EEI's comments: we do not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's proposed change to question 1)	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Micah Runner - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with EEI's comments: we do not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's proposed change to question 1)	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	No
Document Name	
Comment	

Black Hills Corporation agrees with EEI's comments: we do not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's proposed change to question 1)	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
EEI does not support the proposed language changes to Attachment 2 and propose adding an option that would permit protection of user authentication information in transit between the user and an Intermediate System, and not just the asset containing low impact BES Cyber Systems. (See EEI's proposed change to question 1)	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

The examples of evidence for R3.1.1 should also include the documentation of why the communication is needed since the entity is required for low impact assets to implement the controls based on their need.	
Likes 0	
Dislikes 0	
Response	
The SDT believes this request is outside the current SAR and is a compliance interpretation. No change has been made.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

1. Section 3.1.2 creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers: the proposed language requires detection of known/suspected malicious communications for "inbound and outbound electronic remote access." There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5).

BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS.

2. Section 3.1.4 creates a higher compliance bar for Low BCS than for Medium BCS: in the latest Draft 5 of CIP-005-8 R2.2 - 2.3, the proposed requirements include only Interactive Remote Access, or human-initiated access. Section 3.1.4 includes all "information in transit to or from the asset containing low impact BES Cyber Systems."

BPA suggests that this requirement be aligned with the latest Draft 5 of CIP-005-8 R2.2 - 2.3: "3.1.4 Protect user authentication *of IRA communications* in transit to or from the asset containing low impact BES Cyber Systems."

3. Section 3.1.6: While BPA appreciates the committee's intent to "present a single section for all electronic access" (Technical Rationale, p. 2), Section 3.1.6 is nonetheless awkwardly worded. It either suggests that all vendor remote access should be disabled

(rather than requiring controls that could provide an option to disable vendor remote access), or it contradicts itself in a nonsensical sentence by saying that when vendor access is permitted, it should always be disabled. BPA suggests aligning with the language used in Draft 5 of CIP-003-10, such as "Have one or more methods" for determining and disabling vendor remote access sessions.	
Likes 0	
Dislikes 0	
Response	
See SDT's response to BPA comments in question 1.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
SRP agrees and supports Tacoma Power's comment to incorporate the proposed changes outlined in Q1.	
Likes 0	
Dislikes 0	
Response	
See SDT's response to Tacoma Power comments in question 1.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

Per answer in question #1.	
Likes 0	
Dislikes 0	
Response	
See SDT's response to Tri-State G and T Association, Inc. comments in question 1.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
The language in 3.1.2 is specifying an IDS/IPS which depending on the capability of cyber assets at the low impact assets, could be infeasible or cost prohibitive to implement/replace equipment and should take into account that many cyber assets could be limited in their ability to communicate with monitoring/detection systems, communication protocols, etc. Also, in 3.1.4, the SDT should consider modifying language that focuses on mitigating risks to protect user authentication information and allow entities to determine their methods to mitigate risks that fit with their current network configuration(s). The SDT should also consider adding "per Cyber System/Asset capability" to address this reality that many cyber assets have limitations and may not be easily upgraded or replaced.	
Likes 0	
Dislikes 0	
Response	
For 3.1.2, the revisions were made based on the scope of the approved SAR, and the SDT appreciates that there may be cost associated with the implementation of the new standard. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System).	

The SDT has not included “per system capability” within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to also incorporate “Intermediate System” style implementations as well.	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No
Document Name	
Comment	
Eversource agrees with the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
See comments to Q1.	
Likes 0	
Dislikes 0	
Response	
See SDT’s response to Dominion comments in question 1.	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Tacoma Power recommends changing CIP-003-A, Attachment 2, in conformance with our comments to Question 1.	
Likes 1	LaKenya Vannorman, N/A, Vannorman LaKenya
Dislikes 0	
Response	
Change Made. The SDT made conforming changes to Attachment 2 based on new revisions made to Attachment 1.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The number of Low Impact BES Cyber Systems impacted would make achieving compliance burdensome in terms of level of effort, cost, and required technology implementations.	
Likes 0	
Dislikes 0	
Response	
The revisions were made based on the scope of the approved SAR, and the SDT appreciates that there may be effort and cost associated with the implementation of the new standard.	

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute for question #2.	
Likes 0	
Dislikes 0	
Response	
See EEI response.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
Based on concerns about Attachment 1 listed above this section requires adjustment.	
Likes 0	
Dislikes 0	
Response	
See SDT's response to FirstEnergy comments in question 1. Additionally, the SDT made conforming changes to Attachment 2 based on new revisions made to Attachment 1.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF requests the SDT to review the proposed language in CIP-003-A Attachment 2, Section 3, Part 1 stating “except where these communications are time-sensitive protection or control functions between Protection Systems,” and compare it to the proposed language in Attachment 1, Section 3.1.iii “not used for time-sensitive communications of Protection Systems.” to ensure consistency.	
Likes 0	
Dislikes 0	
Response	
To maintain consistency with the electronic access defined within Section 3.1 of Attachment 1, the SDT modified the language to “where electronic access meets the criteria specified in Section 3.1”.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Steve Toosevich - Steve Toosevich, Group Name NIPSCO Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE noticed the formatting of Attachment 2, Section 3 is not consistent with Attachment 1. Texas RE recommends it contain subsections 3.1 – 3.7. Texas RE is similarly concerned with the addition of "remote" in the phrase electronic remote access as in Attachment 1. Texas RE recommends removing the term "remote" from Section 3, #1.	
Likes 0	
Dislikes 0	
Response	
The SDT did not restructure Section 3 of Attachment 2, however, the SDT agrees that the way the section was structured in Section 3 of Attachment 1 modifications would be needed. The SDT believes that the adjustments made to Section 3 of Attachment 1 and the conforming changes made to Section 3 of Attachment 2, fixed the consistency aspect that was previously questionable. The SDT removed the term "remote" from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1.	
Ellese Murphy – Duke Energy	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	

3. The Standard Drafting Team (SDT) proposes a three (3) year implementation plan for CIP-003-A. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

If this standard were to be drafted as-is, large organizations would be compelled to implement substanial technological changes on a grand scale, including significant cost capital and O&M increases which would need to be accounted for on an ongoing basis as well as marshalling of significant contracted labor to execute this massive directive. Consider a tier-ed based approach based on certain risk-based factors, existing connectivity types, capabilities, etc.

FirstEnergy also supports EEI's comments which state:

The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to

Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see EEI response for question 3.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The number of Low Impact BES Cyber Systems impacted would make achieving compliance burdensome in terms of level of effort, cost, and required technology implementations within the implementation timeframe.	
Likes 0	
Dislikes 0	
Response	
No change. The revisions to CIP-003-9 were made based on the scope of the approved SAR, and the SDT appreciates that there may be cost associated with the implementation of the new standard.	
Steve Toosevich - Steve Toosevich, Group Name NIPSCO Compliance	
Answer	No
Document Name	

Comment	
Responsible entities are currently ensuring compliance with CIP-003-8 and preparation for the approved CIP-003-9. The three (3) year implementation plan of CIP-003-A would quickly follow the changes implemented in CIP-003-9 while anticipating modifications to the Standards for Project 2016-02 Modifications to CIP Standards.	
Likes 0	
Dislikes 0	
Response	
No change. The cybersecurity controls proposed for CIP-003-A do not conflict with and build upon the requirements for CIP-003-9 for vendor remote access for those with vendor access controls, while also meeting the requirements of the approved SAR for this project.	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No
Document Name	
Comment	
Eversource agrees with the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response for question 3.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No

Document Name	
Comment	
With the restrictive and prescriptive language as currently proposed, those Responsible Entities with a significant number of low impact assets containing low impact BCS could find it impossible to implement a solution in 3 years. The SDT should consider adding "per Cyber System/Asset capability" to address the reality that many cyber assets have limitations and would require a large effort to replace and implement new cyber assets; and this does not begin to address the potential for equipment supply chain issues and delivery lead times which have not returned to normal for equipment purchases.	
Likes 0	
Dislikes 0	
Response	
Please see response to Questions 1 & 2. The SDT has not included "per system capability" within Section 3 since the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the "networks containing" or "asset containing" level. The SDT clarified the Section 3 language to also incorporate "Intermediate System" style implementations as well.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
If specific date of implementation is defined, SRP might agree. There is significant cost (equipment and resources), time for planning, and work will need to be done.	
Likes 0	
Dislikes 0	

Response	
For US entities, the proposed effective date is 36 months (3 years) after FERC approval date.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Until Questions 1 and 2 are resolved it is difficult for BPA to determine if the 3 year timeframe is appropriate.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see responses to questions 1 and 2.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	

Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with the comments provided by EEI. The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Micah Runner - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	

Black Hills Corporation agrees with the comments provided by EEI. The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Carly Miller - Carly Miller On Behalf of: Sheila Suurmeier, Black Hills Corporation, 5, 6, 1, 3; - Carly Miller	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with the comments provided by EEI. The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	

Josh Combs - Black Hills Corporation - 3	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with the comments provided by EEI. The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
The absence of per Cyber System capability in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4 may create an impossibility to comply within the implementation timeline without wholesale upgrades or replacements of technology and communications infrastructure. NSRF requests further SDT consideration of the addition of "*per Cyber System capability*" language in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4.	

Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	

Response
No change. The SDT has not included “per system capability” within Section 3 since the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to incorporate “Intermediate System” style implementations as well.

Daniel Gacek - Exelon - 1	
Answer	No
Document Name	

Comment
Exelon supports the comments submitted by the EEI.

Likes 0	
Dislikes 0	

Response
Thank you for the comment, please see EEI response.

Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	

Comment
Exelon is in support of EEIs response to this question.

Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
LCRA believes that a 3-year implementation plan may not be sufficient due to the sheer number of Low Impact BES Cyber Systems. Additionally, there is considerable unknowns regarding the new requirements. Please see LCRA's response to question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment. Please see the response to LCRA Question 1 comments.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
LCRA believes that a 3-year implementation plan may not be sufficient due to the sheer number of Low Impact BES Cyber Systems. Additionally, there is considerable unknowns regarding the new requirements. Please see LCRA's response to question 1.	
Likes 0	

Dislikes 0	
Response	
Thank you for the comment. Please see the response to LCRA Question 1 comments.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. No change. The proposed implementation plan timeline is thirty-six (36) months after the effective date, which takes into account the April 1, 2026 effective date of CIP-003-9. The proposed changes to the implementation timeline of CIP-003-10 are outside the purview of this project; however, the SDT is aware of the 2016-02 revisions in CIP-003-10. The SDT notes that since 2016-02 has yet to complete final ballot, receive Board of Trustees approval, and be filed with and approved by FERC, it is not possible to know what the final effective date of CIP-003-10 will be.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	

Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
AZPS does not agree with the proposed implementation plan. AZPS agrees with EEI's comments that the 3 year implementation plan would be acceptable if there were not other industry standards projects underway that will also require changes affecting low impact BCS with differing deadlines.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	

Comment
The pending changes for CIP-003 in other NERC projects would equate to implementing changes that would, within a relatively short time, be modified and be subject to further modifications. Additionally, CEHE supports the included EEI comments that address timing and pending NERC projects. EEI Comment: The 3-year implementation plan would be acceptable if there were no other industry standard projects underway that will require entities to make changes affecting low impact BCS under different regulatory deadlines. This will result in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated. To address this concern, we ask that the proposed changes to Project 2016-02 for CIP-003 be deferred until after the industry has worked through the proposed changes under Project 2023-04 allowing entities to only make changes to the affected sites once.

Likes 0	
Dislikes 0	

Response
Thank you for the comment, please see EEI response.

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	

Comment
WEC Energy Group supports and incorporates by reference the comments of the MRO (NSRF) Group for Question 3.

Likes 0	
Dislikes 0	

Response	
Thank you for the comment, please see MRO Group response.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren supports EEI's comments on this question.	
Likes 0	
Dislikes 0	
Response	

Thank you for the comment, please see EEI response.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see EEI response.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
We do not agree with the proposed implementation plan. Our apprehension primarily stems from the intersection of CIP-003-A and CIP-003-9, with a particular focus on the potential financial implications in Section 6.3, where additional expenditures may be necessitated to accommodate technological changes.	
Likes 0	
Dislikes 0	
Response	

No change. The SDT appreciates that there may be costs associated with implementing these changes.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
We do not agree with the proposed implementation plan. Our apprehension primarily stems from the intersection of CIP-003-A and CIP-003-9, with a particular focus on the potential financial implications in Section 6.3, where additional expentitures may be necessitated to accommodate technological changes.	
Likes 0	
Dislikes 0	
Response	
No change. The SDT appreciates that there may be costs associated with implementing these changes.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports the comments of MRO NSRF and EEI.	
Likes 0	
Dislikes 0	
Response	

Thank you for the comment, please see MRO Group and EEI responses.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed 3-year implementation plan.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes

Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 1	LaKenya Vannorman, N/A, Vannorman LaKenya
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy – Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

4. The SDT believes the language of CIP-003-A addresses the issues outlined in the SAR in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports the comments of MRO NSRF and EEI.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	

3.1.2 exceeds the Standards for Medium Impact and incurs substantial costs. The challenge lies in the fact these terms have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, their reuse should be restricted, and any lesser measures, such as monitoring firewall logs, should not be authorized	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

3.1.2 exceeds the Standards for Medium Impact and incurs substantial costs. The challenge lies in the fact these terms have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, their reuse should be restricted, and any lesser measures, such as monitoring firewall logs, should not be authorized.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
Further analysis is needed to determine if the benefits outweigh the cost of additional equipment needing to be purchased in order to achieve compliance.	

Likes 0	
Dislikes 0	

Response

The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	No
Document Name	

Comment

WEC Energy Group supports and incorporates by reference the comments of the MRO (NSRF) Group for Question 4.

Likes 0	
Dislikes 0	

Response

The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi, Group Name NCPA	
Answer	No
Document Name	
Comment	
No NCPA agrees with several other comments that the proposed language places a high level of burden on entities to protect low impact assets. 3.1.2 – Would greatly increase the demand to implement and maintain a IDS type deployment and continuously update and monitor such traffic 3.1.3 – The phrase “each instances” is not well defined and does not appear anywhere else in the standards. 3.1.4 – This language requires a higher level of security than High/Med assets 3.1.6 – Needs clarification of when to disable vendor remote access	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally,	

the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. The SDT has not included “per system capability” within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to also incorporate “Intermediate System” style implementations as well. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System). 3.1.5 and 3.1.6. Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access. Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.

Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	

AZPS does not agree the changes are cost effective as these would preclude the use of established and currently enforceable concepts that are used to protect user authentication information when communicating with high and medium impact BCS.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. The SDT notes that the required cyber security program for lows is not stricter than the required program for mediums w/o ERC. Medium impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems’ level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The SDT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums.	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1	
Answer	No
Document Name	
Comment	

PNMR sees potential excessive costs in implementing 3.1.4 – particularly if the need arose to install a substation server at each LIBCS substation (as there are many field devices with varying and older protocols in place) in order to ensure the correct protocols were met.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
LCRA cannot determine the cost effectiveness of these proposals due to the sheer number of Low Impact BES Cyber Systems. Additionally, there is considerable unknowns regarding the new requirements. Please see LCRA’s response to question 1.	
Likes 0	

Dislikes 0	

Response

The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.

Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

LCRA cannot determine the cost effectiveness of these proposals due to the sheer number of Low Impact BES Cyber Systems. Additionally, there is considerable unknowns regarding the new requirements. Please see LCRA’s response to question 1.

Likes 0	
Dislikes 0	

Response

The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally,	

the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
The absence of per Cyber System capability in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4 may require premature wholesale upgrades or replacement of communications or operational technology that has not met its end of life in order to comply. NSRF requests further SDT consideration of the addition of "*per Cyber System capability*" language in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4.	
Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a "network(s)" meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. The SDT has not included "per system capability" within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the "networks containing" or "asset containing level". The SDT also clarified the Section 3 language to also incorporate "Intermediate System" style implementations as well.	
Ben Hammer - Western Area Power Administration - 1	
Answer	No

Document Name	
Comment	
The absence of per Cyber System capability in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4 may require premature wholesale upgrades or replacement of communications or operational technology that has not met its end of life in order to comply. NSRF requests further SDT consideration of the addition of "*per Cyber System capability*" language in CIP-003-A Requirement R2 Attachment 1, Section 3, Requirement Part 3.1.4	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a "network(s)" meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. The SDT has not included "per system capability" within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the "networks containing" or "asset containing level". The SDT also clarified the Section 3 language to also incorporate "Intermediate System" style implementations as well.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	

More information required. Unable to determine exact financial impact, but it is significant and needs to be allowed for in the budget.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
Large entities with a large number of cyber assets could incur significant capital and O&M expenditures and labor costs that would be unrealistic if there is only a 3 year implementation plan. This could cause entities to make financial decisions that are not cost effective. The SDT is encouraged to consider the addition of “per Cyber System/Asset capability” and provide a more tiered approach for those entities with a significant number of cyber assets.	
Likes 0	
Dislikes 0	
Response	

The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. The SDT has not included “per system capability” within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to also incorporate “Intermediate System” style implementations as well.	
Steve Toosevich - Steve Toosevich, Group Name NIPSCO Compliance	
Answer	No
Document Name	
Comment	
Responsible Entities would potentially need to purchase new equipment to meet the proposed language of the Standard.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	

Answer	No
Document Name	
Comment	
The number of Low Impact BES Cyber Systems impacted would make achieving compliance burdensome in terms of level of effort, cost, and required technology implementations within the implementation timeframe.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. The SDT has not included “per system capability” within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to also incorporate “Intermediate System” style implementations as well. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	

Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the MRO NSRF for question #4.	
Likes 1	Corn Belt Power Cooperative, 1, brusseau Larry
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
This proposal would be prohibitively expensive both to build and operate over time. To be “cost effective” implies the proposed modification to the CIP-003 standard can be absorbed with existing company staff and minor procedure adjustment. Based on the high volume of Low Impact Cyber System locations and varied configurations that we have in our service territory (approximately 10 times the level of CIP Medium Impact locations), this is not a cost-effective change but is rather a cost-prohibitive mandate. Substantial additional funding (capital and O&M), staffing, and compliance programs will be required to meet the proposed requirements.	
Likes 0	

Dislikes 0	

Response
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency. The SDT has not included “per system capability” within Section 3 due to the fact that the required controls are not specified down to the individual low impact BES Cyber System level. They are specified at either the “networks containing” or “asset containing level”. The SDT also clarified the Section 3 language to also incorporate “Intermediate System” style implementations as well. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System). Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	

PNMR sees potential excessive costs in implementing 3.1.4 – particularly if the need arose to install a substation server at each LIBCS substation (as there are many field devices with varying and older protocols in place) in order to ensure the correct protocols were met.	
Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Change made. The SDT agrees and the intent for 3.1.3 and 3.1.4 is as in the Attachment 1 header where an entity can “utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the section for the development of low impact cyber security plan(s).” The SDT changed 3.1.3 so that authentication can occur for a “network(s)” meaning one or more networks, so that a user would not be required to re-authenticate for a sub-network. The SDT has changed 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System). Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification.	
Deanna Carlson - Cowlitz County PUD - 5	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
The SDT understands that adopting the new standard may incur costs. However, costs, if any, are reasonable considering the already widely used industry tools and practices for securing network access to sensitive data; the required controls aren't detailed for individual low-impact cyber systems, they allow authentication for a “network(s)” meaning one or more networks, eliminating the need for repeated or re-authentication for sub-networks; instead specified at the "networks containing" or "asset containing" level. Additionally, the SDT clarified to include "Intermediate System" implementations providing additional permitted options. Combined these changes address the issues outlined in the SAR prioritizing cost-efficiency.	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes

Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	

Likes 1	LaKenya Vannorman, N/A, Vannorman LaKenya
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren has no comments on the cost effectiveness of this project.	

Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST is unable to assess the cost effectiveness of the proposed approaches to addressing the SAR.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Josh Combs - Black Hills Corporation - 3	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Carly Miller - Carly Miller On Behalf of: Sheila Suurmeier, Black Hills Corporation, 5, 6, 1, 3; - Carly Miller	
Answer	

Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	
Document Name	
Comment	

Black Hills Corporation will not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE does not comment on costs.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	

Dislikes 0	
Response	
Ellese Murphy – Duke Energy	
Answer	Yes
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	

5. Provide any additional comments on the standard and technical rationale for the SDT to consider, if desired.
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE
Answer
Document Name
Comment
While PNMR does agree that coordinated attacks present risk, it is unclear as to the realized risk associated with a coordinated attack utilizing multiple low-impact BES Cyber Systems. As it would be difficult to quantify the number of low-impact systems needed to be

utilized in a potential coordinated attack and with uncertain findings as to the use of low-impact systems to conduct a coordinated attack, PNM believes the potential risk to the BES from such attacks does not sufficiently correlate with the proposed authentication and detection controls which would be a vast expansion of scope. The NERC Low Impact Criteria Review Report references the risk of coordinated attacks on low impact BES Cyber Systems for those systems that are determined by the CIP-002 Standards. However, the CIP-002 categorization of BES Cyber Systems is not intended to take into account the effect of a coordinated attack in determining the categorization of a BES Cyber System. This language seems to attempt to change the purpose and muddy the scope of the CIP-002 Standard. PNMR also has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.	
Likes 0	
Dislikes 0	
Response	
The LICRT indicated they do not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems. Changes to CIP-002 are not included in the scope of the SAR for this project. The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows "low impact only Entities" to comply with those two standards.	
Deanna Carlson - Cowlitz County PUD – 5	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	

Response	
Patricia Lynch - NRG - NRG Energy, Inc. – 5	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	

Answer	
Document Name	
Comment	
Nothing further to provide at this time.	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB

Answer	
Document Name	
Comment	
The language as proposed fails to clearly identify the target of the compliance objective. Suggest the SDT revise the language to clarify whether the target is the network containing the Low BCS, the Low BCS, or other Cyber Assets contained in the network. The undefined term “electronic remote access” used throughout the proposed language lacks sufficient clarity. Suggest the SDT provide a definition to be entered into the NERC Glossary to provide consistent application.	
Likes 0	
Dislikes 0	
Response	
Change made. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also	

allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification. The SDT removed the term "remote" from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. – 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	
Document Name	
Comment	
SRP feels there is some concern for CIP-003 being written for low impact requirements that contain parts of all existing standards (for medium and high impact). Seems like there is an opportunity to just add low impact requirements to the existing standard(s). This will also help in keeping language consistent.	
Likes 0	
Dislikes 0	
Response	
The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows "low impact only Entities" to comply with those two standards.	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	
Document Name	
Comment	
Black Hills Corporation agrees with PNMR and has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.	
Likes 0	
Dislikes 0	

Response	
See PNMR response. The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows “low impact only Entities” to comply with those two standards.	
Micah Runner - Black Hills Corporation – 1	
Answer	
Document Name	
Comment	
Black Hills Corporation agrees with PNMR and has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.	
Likes 0	
Dislikes 0	
Response	
See PNMR response. The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows “low impact only Entities” to comply with those two standards.	
Carly Miller - Carly Miller On Behalf of: Sheila Suurmeier, Black Hills Corporation, 5, 6, 1, 3; - Carly Miller	
Answer	
Document Name	
Comment	
Black Hills Corporation agrees with PNMR and has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.	
Likes 0	
Dislikes 0	

Response	
See PNMR response. The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows “low impact only Entities” to comply with those two standards.	
Josh Combs - Black Hills Corporation – 3	
Answer	
Document Name	
Comment	
Black Hills Corporation agrees with PNMR and has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.	
Likes 0	
Dislikes 0	
Response	
See PNMR response. The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows “low impact only Entities” to comply with those two standards.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
WECC suggests that the DT consider aligning the wording in Attachment 1 Sections 3.1.5 and 3.1.6 to match the working identified in Attachment 2 Section 3 items #5 and #6, specifically Section 3.1.6.	
Likes 0	
Dislikes 0	

Response	
Change made. The SDT has reviewed your comments and has revised the standard structure and language to a more concise and clearer requirement. Section 3.1.5 and 3.1.6 are separated to clarify applicability specific to vendors who are permitted electronic access to the low impact assets networks. The requirement is to have the capability to determine such vendor electronic access, as well as have the capability to disable such vendor electronic access – where an entity has permitted vendor electronic access.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority – 5	
Answer	
Document Name	
Comment	
None at this time.	
Likes 0	
Dislikes 0	
Response	

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. – 1	
Answer	
Document Name	
Comment	
Thank you for the ability to comment.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico – 1	
Answer	

Document Name	
Comment	
While PNMR does agree that coordinated attacks present risk, it is unclear as to the realized risk associated with a coordinated attack utilizing multiple low-impact BES Cyber Systems. As it would be difficult to quantify the number of low-impact systems needed to be utilized in a potential coordinated attack and with uncertain findings as to the use of low-impact systems to conduct a coordinated attack, PNM believes the potential risk to the BES from such attacks does not sufficiently correlate with the proposed authentication and detection controls which would be a vast expansion of scope. The NERC Low Impact Criteria Review Report references the risk of coordinated attacks on low impact BES Cyber Systems for those systems that are determined by the CIP-002 Standards. However, the CIP-002 categorization of BES Cyber Systems is not intended to take into account the effect of a coordinated attack in determining the categorization of a BES Cyber System. This language seems to attempt to change the purpose and muddy the scope of the CIP-002 Standard. PNMR also has reservation with CIP-003 becoming a catch-all Standard for all low-impact requirements instead of designating low-impact requirements to their appropriate Standard.	
Likes 0	
Dislikes 0	
Response	
The LICRT indicated they do not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems. Changes to CIP-002 are not included in the scope of the SAR for this project. The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows “low impact only Entities” to comply with those two standards.	
Andrew Smith - APS - Arizona Public Service Co. – 5	
Answer	
Document Name	
Comment	

AZPS has no additional comments as this time.	
Likes 0	
Dislikes 0	
Response	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
For this statement, there may be a discrepancy in count: "Lower VSL *The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2)"* Should this be six instead of seven?	
Likes 0	
Dislikes 0	
Response	
Change made to all VSLs. Thank you for your comment.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	

Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 – RF	
Answer	
Document Name	
Comment	
Lower VSL *The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the seven topics required by R1. (R1.2)* Should this be six topics required by R1?	
Likes 0	
Dislikes 0	
Response	
Change made to all VSLs. Thank you for your comment.	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
(None)	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	

Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
In general, it seems that the SDT has expanded the requirements beyond what was recommended by the LICRT. For example, the LICRT stated there should be a requirement for the "detection of malicious communications to/between assets containing low-impact BES Cyber Systems with ERC." This languages allows greater flexibility in determining the location of detection compared to the SDT's specification of "for both inbound and outbound electronic remote access." Given that access is defined by communication "outside the asset containing low-impact BES Cyber System(s)," this language inherently mandates the detection to occur at he border of the low-impact asset.	
Likes 0	
Dislikes 0	
Response	
The verbiage "both inbound and outbound" and "outside the asset containing low-impact BES Cyber System(s)" is included in the currently approved CIP-003-9 Standard. The SDT has reused this verbiage to consistently address all remote access (in addition to vendor	

remote access addressed in CIP-003-9) to satisfy the revisions necessary to address the SAR. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification. The SDT removed the term "remote" from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1.	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	
Document Name	
Comment	
In general, it seems that the SDT has expanded the requirements beyond what was recommended by the LICRT. For example, the LICRT stated there should be a requirement for the "detection of malicious communications to/between assets containing low-impact BES Cyber Systems with ERC." This languages allows greater flexibility in determining the location of detection compared to the SDT's specification of "for both inbound and outbound electronic remote access." Given that access is defined by communication "outside the asset containing low-impact BES Cyber System(s)," this language inherently mandates the detection to occur at he border of the low-impact asset	
Likes 0	
Dislikes 0	
Response	
The verbiage "both inbound and outbound" and "outside the asset containing low-impact BES Cyber System(s)" is included in the currently approved CIP-003-9 Standard. The SDT has reused this verbiage to consistently address all remote access (in addition to vendor remote access addressed in CIP-003-9) to satisfy the revisions necessary to address the SAR. The SDT agrees that the way the sentence structure of Section 3 was written there was confusion on what type of electronic access was in scope and what corresponding controls would be required for that access. The SDT has taken these considerations into account and modified the structure of Section 3 by breaking up the introduction of Section 3 to each of its subsections 3.1 and 3.2. This allowed the SDT to mix and match the introduction to	

improve the sentence structure and clarify the scopes. This also allowed the SDT to change the beginnings of 3.1.1 – 3.1.6 to verbs to help with this consistency and clarification. The SDT removed the term “remote” from section 3 to avoid any confusion on how that term is defined. The scope of the electronic access is defined by Section 3.1.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	
Document Name	
Comment	
We would like to thank the SDT for their hard work.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	
Document Name	
Comment	
Constellation has no additional comments. Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reminder
Standards Announcement
Project 2023-04 Modifications to CIP-003

Initial Ballots and Non-binding Poll Open through December 7, 2023

Now Available

Initial ballots for draft one of **CIP-003-A – Cyber Security – Security Management Controls** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels are open through **8 p.m. Eastern, Thursday, December 7, 2023**.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Balloting

Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Chris Larson (via email) or at 404-446-9708. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003 observer list” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-04 Modifications to CIP-003

Formal Comment Period Open through March 14, 2024

Now Available

A 45-day formal comment period for draft two of **CIP-003-A – Cyber Security – Security Management Controls**, is open through **8 p.m. Eastern, Thursday, March 14, 2023.**

The standard drafting team's considerations of the responses received from the previous comment period are reflected in this draft of the standard.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An additional ballot for the standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **March 5 - 14, 2024**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Chris Larson (via email) or at 404-446-9708. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003 observer list” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/308)
Ballot Name: 2023-04 Modifications to CIP-003 CIP-003-A IN 1 ST
Voting Start Date: 11/28/2023 12:01:00 AM
Voting End Date: 12/7/2023 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 271
Total Ballot Pool: 292
Quorum: 92.81
Quorum Established Date: 12/7/2023 1:13:14 PM
Weighted Segment Value: 35.04

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	83	1	20	0.308	45	0.692	0	11	7
Segment: 2	6	0	0	0	0	0	0	5	1
Segment: 3	62	1	11	0.208	42	0.792	0	8	1
Segment: 4	16	1	3	0.231	10	0.769	0	1	2
Segment: 5	77	1	19	0.322	40	0.678	0	11	7
Segment: 6	40	1	13	0.394	20	0.606	0	4	3
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	5	0.5	1	0.1	0	1	0
Totals:	292	5.6	71	1.962	158	3.638	0	42	21

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Negative	Comments Submitted
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	Austin Energy	Thomas Standifur		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Micah Runner		Negative	Comments Submitted
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Corn Belt Power Cooperative	Larry brusseau		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		None	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Negative	Comments Submitted
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Negative	Comments Submitted
1	Eversource Energy	Joshua London		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	JEA	Joseph McClung		Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Third-Party Comments
1	Lakeland Electric	Larry Watt		Affirmative	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Negative	Comments Submitted
1	LS Power Transmission, LLC	Jennifer Richardson		None	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Manitoba Hydro	Nazra Gladu		Negative	Comments Submitted
1	MEAG Power	David Weekley	Rebika Yitna	Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Nikki Carson-Marquis	Negative	Third-Party Comments
1	Muscatine Power and Water	Andrew Kurriger		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Daniel Valle		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pedernales Electric Cooperative, Inc.	Bradley Collard		Abstain	N/A
1	Platte River Power Authority	Marissa Archie		Negative	Third-Party Comments
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Third-Party Comments
1	Sho-Me Power Electric Cooperative	Olivia Olson		None	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Abstain	N/A
1	Southwestern Power Administration	Angela Wheat		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Unisource - Tucson Electric Power Co.	Jessica Cordero		None	N/A
1	Western Area Power Administration	Ben Hammer		Negative	Comments Submitted
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	BC Hydro and Power Authority	Ming Jiang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Negative	Comments Submitted
3	Black Hills Corporation	Josh Combs		Negative	Comments Submitted
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Carl Spaetzel	Ryan Strom	Negative	Third-Party Comments
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Third-Party Comments
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Negative	Third-Party Comments
3	Colorado Springs Utilities	Hillary Dobson		Negative	Third-Party Comments
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Negative	Comments Submitted
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Negative	Comments Submitted
3	Eversource Energy	Vicki O'Leary		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Third-Party Comments
3	Manitoba Hydro	Mike Smith		Negative	Comments Submitted
3	MEAG Power	Roger Brand	Rebika Yitna	Negative	Comments Submitted
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Negative	Third-Party Comments
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Negative	Third-Party Comments
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NW Electric Power Cooperative, Inc.	Heath Henry		Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Negative	Comments Submitted
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Abstain	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Tri-State G and T Association, Inc.	Ryan Walter		Negative	Comments Submitted
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		None	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Negative	Third-Party Comments
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Katrina Lyons		Negative	Comments Submitted
4	Illinois Municipal Electric Agency	Mary Ann Todd		Abstain	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Negative	Third-Party Comments
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
4	Utility Services, Inc.	Tracy MacNicoll		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	AEP	Thomas Foltz		Abstain	N/A
5	AES - AES Corporation	Ruchi Shah		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	American Municipal Power	Amy Ritts		None	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Chuck Booth		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Amanda Wangler		Negative	Third-Party Comments
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		None	N/A
5	Black Hills Corporation	Sheila Suurmeier	Carly Miller	Negative	Comments Submitted
5	Bonneville Power Administration	Christopher Siewert		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Negative	Third-Party Comments
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Negative	Third-Party Comments
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Decatur Energy Center LLC	Megan Melham		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Negative	Comments Submitted
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	Negative	Third-Party Comments
5	Great River Energy	Jacalynn Bentz		Negative	Third-Party Comments
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	JEA	John Babik		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Negative	Comments Submitted
5	LS Power Development, LLC	C. A. Campbell		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Robin Berry		Negative	Third-Party Comments
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NextEra Energy	Richard Vendetti		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Reid Cashion	Scott Brame	Negative	Third-Party Comments
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		Negative	Third-Party Comments
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Abstain	N/A
5	Pattern Operators LP	George E Brown		Negative	Third-Party Comments
5	Pine Gate Renewables	Michiko Sell		None	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Negative	Third-Party Comments
5	PSEG Nuclear LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Don Cribb		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Third-Party Comments
5	Southern Company - Southern Company Generation	Leslie Burke		Abstain	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Comments Submitted
5	Tennessee Valley Authority	Darren Boehm		Negative	Comments Submitted
5	TransAlta Corporation	Ashley Scheelar		Abstain	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		None	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Black Hills Corporation	Claudine Bates		Negative	Comments Submitted
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Entergy	Julie Hall	Kristen Long	Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Kelly Bertholet		Negative	Comments Submitted
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Powerex Corporation	Raj Hundal		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Abstain	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	Tennessee Valley Authority	Armando Rodriguez		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Boeshaar		Negative	Comments Submitted
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 292 of 292 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/308)
Ballot Name: 2023-04 Modifications to CIP-003 Implementation Plan IN 1 OT
Voting Start Date: 11/28/2023 12:01:00 AM
Voting End Date: 12/7/2023 8:00:00 PM
Ballot Type: OT
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 270
Total Ballot Pool: 293
Quorum: 92.15
Quorum Established Date: 12/7/2023 1:15:26 PM
Weighted Segment Value: 40.86

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	84	1	25	0.391	39	0.609	0	12	8
Segment: 2	6	0	0	0	0	0	0	5	1
Segment: 3	63	1	20	0.37	34	0.63	0	8	1
Segment: 4	16	1	4	0.308	9	0.692	0	1	2
Segment: 5	77	1	22	0.373	37	0.627	0	10	8
Segment: 6	40	1	14	0.424	19	0.576	0	4	3
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.3	3	0.3	0	0	0	3	0
Totals:	293	5.3	88	2.166	138	3.134	0	44	23

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Negative	Comments Submitted
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Micah Runner		Negative	Comments Submitted
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Corn Belt Power Cooperative	Larry brusseau		Abstain	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		None	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Negative	Comments Submitted
1	Duke Energy	Katherine Street		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Edison International - Southern California Edison Company	Robert Blackney		Negative	Third-Party Comments
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	JEA	Joseph McClung		Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Affirmative	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Negative	Comments Submitted
1	LS Power Transmission, LLC	Jennifer Richardson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Negative	Comments Submitted
1	MEAG Power	David Weekley	Rebika Yitna	Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Nikki Carson-Marquis	Negative	Third-Party Comments
1	Muscatine Power and Water	Andrew Kurriger		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	None	N/A
1	New York Power Authority	Daniel Valle		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Pedernales Electric Cooperative, Inc.	Bradley Collard		Abstain	N/A
1	Platte River Power Authority	Marissa Archie		Negative	Third-Party Comments
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Third-Party Comments
1	Sho-Me Power Electric Cooperative	Olivia Olson		None	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Abstain	N/A
1	Southwestern Power Administration	Angela Wheat		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	David Plumb		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Unisource - Tucson Electric Power Co.	Jessica Cordero		None	N/A
1	Western Area Power Administration	Ben Hammer		Negative	Comments Submitted
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	BC Hydro and Power Authority	Ming Jiang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Negative	Comments Submitted
3	Black Hills Corporation	Josh Combs		Negative	Comments Submitted
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Carl Spaetzel	Ryan Strom	Negative	Third-Party Comments
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Negative	Third-Party Comments
3	Colorado Springs Utilities	Hillary Dobson		Negative	Third-Party Comments
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Third-Party Comments
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Mike Smith		Negative	Comments Submitted
3	MEAG Power	Roger Brand	Rebika Yitna	Negative	Comments Submitted
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Negative	Third-Party Comments
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Negative	Comments Submitted
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Abstain	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Tri-State G and T Association, Inc.	Ryan Walter		Negative	Comments Submitted
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		None	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Negative	Third-Party Comments
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Katrina Lyons		Negative	Comments Submitted
4	Illinois Municipal Electric Agency	Mary Ann Todd		Abstain	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Affirmative	N/A
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
4	Utility Services, Inc.	Tracy MacNicoll		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	AEP	Thomas Foltz		Abstain	N/A
5	AES - AES Corporation	Ruchi Shah		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	American Municipal Power	Amy Ritts		None	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Amanda Wangler		Negative	Third-Party Comments
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		None	N/A
5	Black Hills Corporation	Sheila Suurmeier	Carly Miller	Negative	Comments Submitted
5	Bonneville Power Administration	Christopher Siewert		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Negative	Third-Party Comments
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Negative	Third-Party Comments
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Decatur Energy Center LLC	Megan Melham		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Negative	Comments Submitted
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	Negative	Third-Party Comments
5	Great River Energy	Jacalynn Bentz		Negative	Third-Party Comments
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	JEA	John Babik		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Negative	Comments Submitted
5	LS Power Development, LLC	C. A. Campbell		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Robin Berry		Negative	Third-Party Comments
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NextEra Energy	Richard Vendetti		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Reid Cashion	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		Negative	Third-Party Comments
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Abstain	N/A
5	Pattern Operators LP	George E Brown		Negative	Third-Party Comments
5	Pine Gate Renewables	Michiko Sell		None	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Negative	Third-Party Comments
5	PSEG Nuclear LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Don Cribb		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Third-Party Comments
5	Southern Company - Southern Company Generation	Leslie Burke		Abstain	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Comments Submitted
5	Tennessee Valley Authority	Darren Boehm		Negative	Comments Submitted
5	TransAlta Corporation	Ashley Scheelar		Abstain	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		None	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Black Hills Corporation	Claudine Bates		Negative	Comments Submitted
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Entergy	Julie Hall	Kristen Long	Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Kelly Bertholet		Negative	Comments Submitted
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Powerex Corporation	Raj Hundal		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Abstain	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	Tennessee Valley Authority	Armando Rodriguez		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Boeshaar		Negative	Comments Submitted
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 293 of 293 entries

BALLOT RESULTS

Ballot Name: 2023-04 Modifications to CIP-003 CIP-003-A | Non-binding Poll IN 1 NB
Voting Start Date: 11/28/2023 12:01:00 AM
Voting End Date: 12/7/2023 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 255
Total Ballot Pool: 280
Quorum: 91.07
Quorum Established Date: 12/7/2023 1:57:18 PM
Weighted Segment Value: 32.11

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	16	0.296	38	0.704	20	6
Segment: 2	6	0	0	0	0	0	5	1
Segment: 3	59	1	11	0.239	35	0.761	11	2
Segment: 4	16	1	5	0.385	8	0.615	1	2
Segment: 5	74	1	16	0.327	33	0.673	17	8
Segment: 6	38	1	10	0.4	15	0.6	7	6
Segment: 7	1	0	0	0	0	0	1	0
Segment: 8	0	0	0	0	0	0	0	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	6	0.3	3	0.3	0	0	3	0
Totals:	280	5.3	61	1.947	129	3.353	65	25

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Micah Runner		Negative	Comments Submitted
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Corn Belt Power Cooperative	Larry brusseau		Abstain	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		None	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Negative	Comments Submitted
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Negative	Comments Submitted
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Joshua London		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	JEA	Joseph McClung		Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		Affirmative	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Negative	Comments Submitted
1	LS Power Transmission, LLC	Jennifer Richardson		None	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Comments Submitted
1	MEAG Power	David Weekley	Rebika Yitna	Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Nikki Carson-Marquis	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		Negative	Comments Submitted
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Daniel Valle		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Pedernales Electric Cooperative, Inc.	Bradley Collard		Abstain	N/A
1	Platte River Power Authority	Marissa Archie		Negative	Comments Submitted
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Abstain	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Sho-Me Power Electric Cooperative	Olivia Olson		None	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Abstain	N/A
1	Southwestern Power Administration	Angela Wheat		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Unisource - Tucson Electric Power Co.	Jessica Cordero		None	N/A
1	Western Area Power Administration	Ben Hammer		Negative	Comments Submitted
2	California ISO	Darcy O'Connell		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	BC Hydro and Power Authority	Ming Jiang		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Negative	Comments Submitted
3	Black Hills Corporation	Josh Combs		Negative	Comments Submitted
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Carl Spaetzel	Ryan Strom	Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Colorado Springs Utilities	Hillary Dobson		Negative	Comments Submitted
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	MEAG Power	Roger Brand	Rebika Yitna	Negative	Comments Submitted
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Negative	Comments Submitted
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Abstain	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Ryan Walter		Negative	Comments Submitted
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Comments Submitted
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		None	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Katrina Lyons		Negative	Comments Submitted
4	Illinois Municipal Electric Agency	Mary Ann Todd		Abstain	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Affirmative	N/A
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
4	Utility Services, Inc.	Tracy MacNicoll		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	AEP	Thomas Foltz		Abstain	N/A
5	AES - AES Corporation	Ruchi Shah		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Chuck Booth		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Amanda Wangler		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		None	N/A
5	Black Hills Corporation	Sheila Suurmeier	Carly Miller	Negative	Comments Submitted
5	Bonneville Power Administration	Christopher Siewert		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Negative	Comments Submitted
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
5	Decatur Energy Center LLC	Megan Melham		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Evergy	Jeremy Harris	Alan Kloster	Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Negative	Comments Submitted
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	Negative	Comments Submitted
5	Great River Energy	Jacalynn Bentz		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	JEA	John Babik		Abstain	N/A
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Negative	Comments Submitted
5	LS Power Development, LLC	C. A. Campbell		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	National Grid USA	Robin Berry		Negative	Comments Submitted
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NextEra Energy	Richard Vendetti		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Reid Cashion	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Negative	Comments Submitted
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Abstain	N/A
5	Pattern Operators LP	George E Brown		Negative	Comments Submitted
5	Pine Gate Renewables	Michiko Sell		None	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG Nuclear LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Don Cribb		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments Submitted
5	Southern Company - Southern Company Generation	Leslie Burke		Abstain	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Comments Submitted
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	TransAlta Corporation	Ashley Scheelar		Abstain	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		None	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Black Hills Corporation	Claudine Bates		Negative	Comments Submitted
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Entergy	Julie Hall	Kristen Long	Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Shelly Dineen		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	Powerex Corporation	Raj Hundal		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Abstain	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Abstain	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Negative	Comments Submitted
7	Amazon Web Services	Kristine Martz		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 280 of 280 entries

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard for a 45-day formal comment period with additional ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023
45-day formal comment period with initial ballot	October 24 – December 7, 2023

Anticipated Actions	Date
45-day formal comment period with additional ballot	January 30 – March 14, 2024
10-day final ballot	April 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

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

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

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

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

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

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

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

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

5. Effective Dates: See Implementation Plan for CIP-003-A.

B. Requirements and Measures

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

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

1.1.1. Personnel and training (CIP-004);

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

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

1.1.4. System security management (CIP-007);

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

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

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

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

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

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

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

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

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

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

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

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

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

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

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

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

C. Compliance

1. Compliance Monitoring Process

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

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

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

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

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

Violation Severity Levels

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the six topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2)	cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the six topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2)	cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the six topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2)	security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the six topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR	Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls, but failed to implement one or two controls listed in Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR	implement three or more controls listed in Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR	

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)	
R3.	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from

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

Version	Date	Action	Change Tracking
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
A	TBD	Adopted by the NERC Board of Trustees.	TBD

Attachment 1

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

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

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

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

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented in Section 3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, where electronic access is:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

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

the Responsible Entity shall implement a control(s) that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic access;

3.1.3 Authenticate users when permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems;

3.1.4 Protect user authentication information for each user-initiated

instance of electronic access while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BES Cyber System(s);

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a control(s) that authenticates all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

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

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

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

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

4.4 Incident handling for Cyber Security Incidents;

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

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

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

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

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

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

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

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

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

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

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Attachment 2

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

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

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

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

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

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

1. For Section 3.1.1, documentation showing the permittance of only inbound and outbound electronic access, where electronic access meets the criteria specified in Section 3.1, that the Responsible Entity deems necessary, such as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
   - Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways); or
   - Original Equipment Manufacturer (OEM) specification sheets that

provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets the criteria specified in Section 3.1, such as:
    - Anti-malware technologies;
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - Automated or manual log reviews;
    - Alerting; or
    - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate users when permitting each user-initiated instance of electronic access, where electronic access meets the criteria specified in Section 3.1, to a network(s) containing low impact BES Cyber Systems, such as:
    - Authentication mechanism(s) including but not limited to:
        - Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or
        - Enforcement of Multi-Factor Authentication (MFA).
    - Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
    - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BES Cyber System; or
    - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for each user-initiated instance of electronic access, where electronic access meets the criteria specified in Section 3.1, while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and
    - the authentication system used to meet Section 3.1.3, or
    - the asset containing low impact BES Cyber System(s),

    such as:
    - Protection mechanism(s) including but not limited to:
        - Implementation of an encrypted protocol or service (Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH), etc.); or
        - Implementation of an IPsec or Secure Sockets Layer (SSL) VPN.

- Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets the criteria specified in Section 3.1, such as:
    - Steps to preauthorize access;
    - Alerts generated by vendor log on;
    - Session monitoring;
    - Security information management logging alerts;
    - Time-of-need session initiation;
    - Session recording;
    - System logs; or
    - Other operational, procedural, or technical controls.
6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets the criteria specified in Section 3.1, such as:
    - Disabling vendor electronic access user or system accounts;
    - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic access;
    - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
    - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
    - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or
    - Other operational, procedural, or technical controls.
7. For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security

Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);

2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

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

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

   Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is

necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

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

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~first~~second draft of the proposed standard for a ~~formal~~ 45-day formal comment period with additional ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023

Anticipated Actions	Date
45-day formal comment period with initial ballot	October ~~25~~24 – December ~~8~~7, 2023
45-day formal ~~or informal~~ comment period with additional ballot	February 25 – March 11, 2024
10-day final ballot	April 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

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

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

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

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

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

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

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

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

5. Effective Dates: See Implementation Plan for CIP-003-A.

6.

B. Requirements and Measures

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

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

1.1.1. Personnel and training (CIP-004);

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

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

1.1.4. System security management (CIP-007);

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

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

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

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

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

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

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

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

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

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

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

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

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

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

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

C. Compliance

1. **Compliance Monitoring Process**

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with ~~the NERC~~mandatory and enforceable Reliability Standards in their respective jurisdictions.

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

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

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

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

Violation Severity Levels

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the ~~seven~~six topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2)	cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the ~~seven~~six topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2)	cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the ~~seven~~six topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2)	security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the ~~seven~~six topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR	Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls, but failed to implement one or two controls listed in Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR	implement three or more controls listed in Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR	

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)	
R3.	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)

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

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from

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

Version	Date	Action	Change Tracking
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
A	TBD	Adopted by the NERC Board of Trustees.	TBD

Attachment 1

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

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

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

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

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented in Section 3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, ~~to mitigate risks associated with~~where electronic access~~, the Responsible Entity shall implement controls to~~ is:

~~**3.1** For connectivity that provides the ability to communicate:~~

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

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

the Responsible Entity shall implement a control(s) that:

3.1.1 Permit only necessary inbound and outbound electronic ~~remote~~ access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic ~~remote~~ access;

3.1.3 Authenticate users when permitting each user-initiated instance of electronic ~~remote~~ access to ~~networks~~a network(s)

containing low impact BES Cyber Systems;

3.1.4 Protect user authentication information for each user-initiated instance of electronic access while in transit ~~to or from~~ between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

- the authentication system used to meet Section 3.1.3, or
- ~~**3.1.4**~~ the asset containing low impact BES Cyber ~~Systems~~System(s);

3.1.5 ~~Determine~~Include one or more method(s) for determining vendor electronic ~~remote~~ access, where vendor electronic ~~remote~~ access is permitted; and

3.1.6 ~~Disable~~Include one or more method(s) for disabling vendor electronic ~~remote~~ access, where vendor electronic ~~remote~~ access is permitted.

3.2 ~~Authenticate~~ For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a control(s) that authenticates all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

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

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

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

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

4.4 Incident handling for Cyber Security Incidents;

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

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

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

Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

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

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

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

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

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

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

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

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Attachment 2

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

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

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

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

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

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

1. For Section 3.1.1, documentation showing ~~routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit~~the permittance of only inbound and outbound electronic ~~remote~~ access, where electronic access meets the criteria specified in Section 3.1, that the Responsible Entity deems necessary, ~~except where these communications are time-sensitive protection or control functions between Protection Systems,~~ such as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
   - Lists of implemented electronic access controls (e.g., access control lists

restricting IP addresses, ports, or services; implementing unidirectional gateways); or

- Original Equipment Manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets the criteria specified in Section 3.1, such as:
    - Anti-malware technologies;
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - Automated or manual log reviews;
    - Alerting; or
    - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate users when permitting each user-initiated instance of electronic ~~remote access to networks~~access, where electronic access meets the criteria specified in Section 3.1, to a network(s) containing low impact BES Cyber Systems, such as:
    - Authentication mechanism(s) including but not limited to:
        - ~~•~~ Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or
        - ~~•~~ Enforcement of Multi-Factor Authentication (MFA).
    - Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters; ~~or~~
    - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BES Cyber System; or
    - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information ~~in transit to or from~~for each user-initiated instance of electronic access, where electronic access meets the criteria specified in Section 3.1, while in transit between the Cyber Asset outside the asset containing low impact BES Cyber ~~Systems, such as:~~System(s) and
    - the authentication system used to meet Section 3.1.3, or
    - the asset containing low impact BES Cyber System(s),

    such as:
    - Protection mechanism(s) including but not limited to:

- Implementation of an encrypted protocol or service (Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH), etc.); or
- Implementation of an IPsec or Secure Sockets Layer (SSL) VPN.
- Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing ~~the ability to determine vendor remote access,~~one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets the criteria specified in Section 3.1, such as:
    - Steps to preauthorize access;
    - Alerts generated by vendor log on;
    - Session monitoring;
    - Security information management logging alerts;
    - Time-of-need session initiation;
    - Session recording;
    - System logs; or
    - Other operational, procedural, or technical controls.
6. For Section 3.1.6, documentation showing ~~the ability to disable~~one or more methods for disabling vendor electronic ~~remote~~ access, where vendor electronic access is permitted and electronic access meets the criteria specified in Section 3.1, such as:
    - Disabling vendor electronic ~~remote~~ access user or system accounts;
    - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic ~~remote~~ access;
    - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic ~~remote~~ access;
    - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
    - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic ~~remote~~ access; or
    - Other operational, procedural, or technical controls.
7. For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control

room, or access control on the BES Cyber System).

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

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

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

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

the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

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

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

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard for a 45-day formal comment period with additional ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023

Anticipated Actions	Date
45-day formal comment period with initial ballot	October 24 – December 7, 2023
45-day formal comment period with additional ballot	February 25 – March 11, 2024
10-day final ballot	April 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

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

2. **Number:** CIP-~~003-9~~003-A

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

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

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

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

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

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

5. Effective Dates: See Implementation Plan for CIP-~~003-9~~003-A.

6.

B. Requirements and Measures

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

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

1.1.1. Personnel and training (CIP-004);

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

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

1.1.4. System security management (CIP-007);

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

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

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

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

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

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

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

~~**1.2.6.** Vendor electronic remote access security controls; and~~

1.2.6. ~~**1.2.7.**~~ Declaring and responding to CIP Exceptional Circumstances.

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

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

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

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

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

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

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

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

C. Compliance

1. **Compliance Monitoring Process**

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with ~~the NERC~~mandatory and enforceable Reliability Standards in their respective jurisdictions.

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

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

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

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

Violation Severity Levels

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the ~~seven~~six topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less	policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the ~~seven~~six topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous	policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the ~~seven~~six topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2)	the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address four or more of the ~~seven~~six topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity implemented all electronic access controls, but failed to document ~~its cyber security plan(s) for~~ the electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to ~~authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to~~ document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) ~~3.2~~ OR The Responsible Entity documented its cyber security plan(s) for electronic access controls, but failed to ~~authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to~~ implement one or two controls listed in Requirement R2, Attachment 1, Section 3. (R2)	The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but failed to ~~permit only necessary inbound and outbound electronic access~~ implement three or more controls listed in Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) OR	OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity	Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote accesssecurity controls according to Requirement R2, Attachment 1, Section 6. (R2)~~	Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2) OR ~~mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2)~~ ~~OR~~ The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for	Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed ~~to documentaccording to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed~~ to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2) ~~OR~~ ~~The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote accesssecurity controls according to Requirement R2, Attachment 1, Section 6. (R2)~~	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2) ~~OR The Responsible Entity documented its cyber security process for vendor electronic remote accesssecurity controls, but failed to implement vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)~~		

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4.	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from

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

Version	Date	Action	~~Action~~Change Tracking	~~Change Tracking~~
9	~~TBD~~11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report	
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.		
9	3/22/2023	Effective Date	April 1, 2026	
A	TBD	Adopted by the NERC Board of Trustees.	TBD	

Attachment 1

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

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

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

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

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented ~~for~~in Section ~~3.1~~3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, ~~the Responsible Entity shall implement~~where electronic access ~~controls to~~is:

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

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

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

the Responsible Entity shall implement a control(s) that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both

inbound and outbound electronic access;

3.1.3 Authenticate users when permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems;

3.1.4 Protect user authentication information for each user-initiated instance of electronic access while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BES Cyber System(s);

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 ~~Authenticate~~ For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a control(s) that authenticates all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

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

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

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

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

4.4 Incident handling for Cyber Security Incidents;

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

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

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

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

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

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

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

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;

- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

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

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

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

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

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

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

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

Attachment 2

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

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

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

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

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section ~~3.1~~3.1.1, if any.

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

1. ~~Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit~~For Section 3.1.1, documentation showing the permittance of only inbound and outbound electronic access, where electronic access meets the criteria specified in Section 3.1, that the Responsible Entity deems necessary, ~~except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative~~ such as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber

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

- Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways) ~~.~~; or

- Original Equipment Manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets the criteria specified in Section 3.1, such as:
   - Anti-malware technologies;
   - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
   - Automated or manual log reviews;
   - Alerting; or
   - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate users when permitting each user-initiated instance of electronic access, where electronic access meets the criteria specified in Section 3.1, to a network(s) containing low impact BES Cyber Systems, such as:
   - Authentication mechanism(s) including but not limited to:
     - Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or
     - Enforcement of Multi-Factor Authentication (MFA).
   - Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
   - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BES Cyber System; or
   - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for each user-initiated instance of electronic access, where electronic access meets the criteria specified in Section 3.1, while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and
   - the authentication system used to meet Section 3.1.3, or
   - the asset containing low impact BES Cyber System(s),

   such as:
   - Protection mechanism(s) including but not limited to:
     - Implementation of an encrypted protocol or service (Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH), etc.); or

- Implementation of an IPsec or Secure Sockets Layer (SSL) VPN.
- Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets the criteria specified in Section 3.1, such as:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;
   - Security information management logging alerts;
   - Time-of-need session initiation;
   - Session recording;
   - System logs; or
   - Other operational, procedural, or technical controls.
6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets the criteria specified in Section 3.1, such as:
   - Disabling vendor electronic access user or system accounts;
   - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or
   - Other operational, procedural, or technical controls.

7. ~~2. Documentation~~For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

1. to identify, classify, and respond to Cyber Security Incidents; to determine

whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);

2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

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

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

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

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

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

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

~~1. For Section 6.1, documentation showing:~~

- ~~steps to preauthorize access;~~
- ~~alerts generated by vendor log on;~~
- ~~session monitoring;~~
- ~~security information management logging alerts;~~
- ~~time-of-need session initiation;~~
- ~~session recording;~~
- ~~system logs; or~~
- ~~other operational, procedural, or technical controls.~~

~~2. For Section 6.2, documentation showing:~~

- ~~disabling vendor electronic remote access user or system accounts;~~

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

~~3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:~~

- ~~Anti-malware technologies;~~
- ~~Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);~~
- ~~Automated or manual log reviews;~~
- ~~alerting; or~~
- ~~other operational, procedural, or technical controls.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-04 Modifications to CIP-003
Reliability Standard CIP-003-A

Applicable Standard(s)

- CIP-003-A – Cyber Security – Security Management Controls

Requested Retirement(s)

- CIP-003-9 – Cyber Security – Security Management Controls[1]

Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

New/Modified/Retired Terms in the NERC Glossary of Terms

- None

Background

Project 2023-04 addresses modifications to CIP-003-9 in response to recommendations from the Low Impact Criteria Review Team (LICRT), which was formed by the NERC Board of Trustees to consider the potential threat and risk posed by a coordinated cyber-attack on low impact Bulk Electric System (BES) Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommended actions to address those risks. The Board accepted the

[1] If Reliability Standard CIP-003-9 has been superseded by another version, this standard will replace the currently effective version of CIP-003.

LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the standard authorization request (SAR) at its March 22, 2023 meeting. In response to the SAR, Project 2023-04 proposes merging Sections 3 and 6 of CIP-003-9, Attachment 1 and 2 to consolidate all electronic access requirements.

General Considerations

This implementation plan provides entities with thirty-six (36) months to become compliant with the revised Reliability Standard. This implementation plan reflects the following considerations for entities to implement the new controls of Requirement R2, Attachment 1:

- Revise cyber security policy, plan, and procedures.
- Hire and train new staff to implement the new cyber security controls.
- Reconfigure system, network, or security architectures.
- Purchase, procure, and install new technology(s).
- The effective date of CIP-003-9 is April 1, 2026. The cyber security controls implemented with CIP-003-A do not conflict and build upon the implementation of CIP-003-9 for vendor electronic remote access. The DT revisions are based on CIP-003-9, since it is FERC approved, but not yet effective. Registered Entities are in the process of complying with CIP-003-9, though the standard is not yet mandatory and enforceable.

Effective Date

Reliability Standard CIP-003-A

Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and Responsible Entities shall comply initially with those periodic requirements in CIP-003-A as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.3 on or before the effective date of CIP-003-A. Responsible Entities shall initially comply with all other periodic requirements in CIP-003-A within the periodic timeframes of their last performance under CIP-003-9.

Retirement Date

Reliability Standard CIP-003-9

Reliability Standard CIP-003-9 shall be retired immediately prior to the effective date of CIP-003-A in the jurisdiction in which the revised standard is becoming effective. If CIP-003-9 has been superseded by another version of Reliability Standard CIP-003, the currently effective version will be retired.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale

Project 2023-04 Modifications to CIP-003

Reliability Standard CIP-003-A – Low Impact BES Cyber Security Criteria Revisions | January 2024

Introduction

This document is the technical rationale and justification for Reliability Standard CIP-003-A and includes the rationale for changes in the current proposed version, as well as previous versions of the standard.

It is intended to provide stakeholders and the ERO Enterprise with an understanding of the revisions, technology and technical concepts of Reliability Standard CIP-003-A. This is not a Reliability Standard and should not be considered mandatory and enforceable.

Background

In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact Bulk Electric System (BES) Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts, representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber-attack on low impact BES Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the Standard Authorization Request (SAR) at its March 22, 2023 meeting.

The LICRT conclusions regarding low impact BES Cyber Systems (LIBCS) are as follows:

- Individually, low impact BES Cyber Systems are truly low impact to BES reliability. This corresponds to the longstanding work of NERC and the stakeholders to design and operate the BES to withstand the loss of any of its individual assets. A medium or high impact BES Cyber System is more than an impact to a typical single BES Element/Facility. Therefore, the team does not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems.
- The team recognizes that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The team recommends enhancing the existing low impact category to further mitigate the coordinated attack risk.

Those LICRT report recommendations are as follows:

- Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity.

Rationale for Attachment 1, Section 3 and Section 6

The Standard Drafting Team's (SDT's) review of the SAR and industry comments initiated a discussion of where the requirements would reside within CIP-003-A. CIP-003-9 was used as the baseline for revisions, since this version is the most recent version approved by the Federal Energy Regulatory Commission (FERC). Attachment 1, Section 3 and Attachment 1, Section 6 were identified as ideal locations to integrate the requirements due to their focus on Electronic Access Controls and Vendor Electronic Remote Access Security Controls. The SDT considered two options:

Option A: Modify Sections 3 and 6, integrating the requirements, but keeping the sections separate.
Option B: Merge Sections 3 and 6.

The SDT agreed to Option B: Merge Sections 3 and 6. The following rationale was used to support the decision:

1. Merging Section 3 and Section 6 would present a single section for all electronic access with sub-sections providing additional requirements based on the type of access (Vendor, dial-up, local, etc.).
2. Section 6 has not been implemented or required by industry at this time and therefore there would be no impact to merging it with Section 3.

While merging Section 3 and 6, the SDT made conforming changes to the language. The SDT uses the phrase "implement controls" to replace "implement a process" or "implement one or more method(s)". The SDT believes a "control" can include an operation, process, procedure, or technology as described in the examples of Attachment 2.

Glossary Terms

The SDT also discussed potentially reintroducing, with modification, the retired NERC Glossary term: LERC, Low Impact External Routable Connectivity, or creating a new NERC Glossary term. The rationale for using LERC or potentially defining a new term would be to provide a shorthand way of discussing external routable connectivity when dealing with assets containing low impact BES Cyber Systems. LERC was initially created by the Project 2014-02 SDT in response to FERC Order No. 791. In Order No. 822, FERC approved the LERC definition subject to modifications. Project 2016-02 was formed to address Order 822 and, rather than modify the definition, that SDT chose to retire the term and integrate the language into Attachment 1, Section 3.1. The term was only in use from July 1, 2016 through December 31, 2019.

The SDT agreed to keep the language from the previous CIP-003-9 Section 3.1 intact rather than reintroducing the retired LERC term or create a new glossary term. Rationale used for the decision:

1. Possible confusion with reintroducing the term LERC.
2. Possible friction with industry stakeholders with using a new term.
3. Actual requirement for LERC or a new term beyond Section 3.

Section 3.1

The objective of Section 3.1 is to maintain the original language used in CIP-003-9, Section 3.1, Subsections (i) - (iii). There is one revision to 3.1(iii) replacing the protocol language with reference to

"Protection Systems", which is a conforming change made by Project 2016-02, CIP-003-Y. Figure 1 provides a graphical representation of Section 3.1, Subsections (i)-(iii).

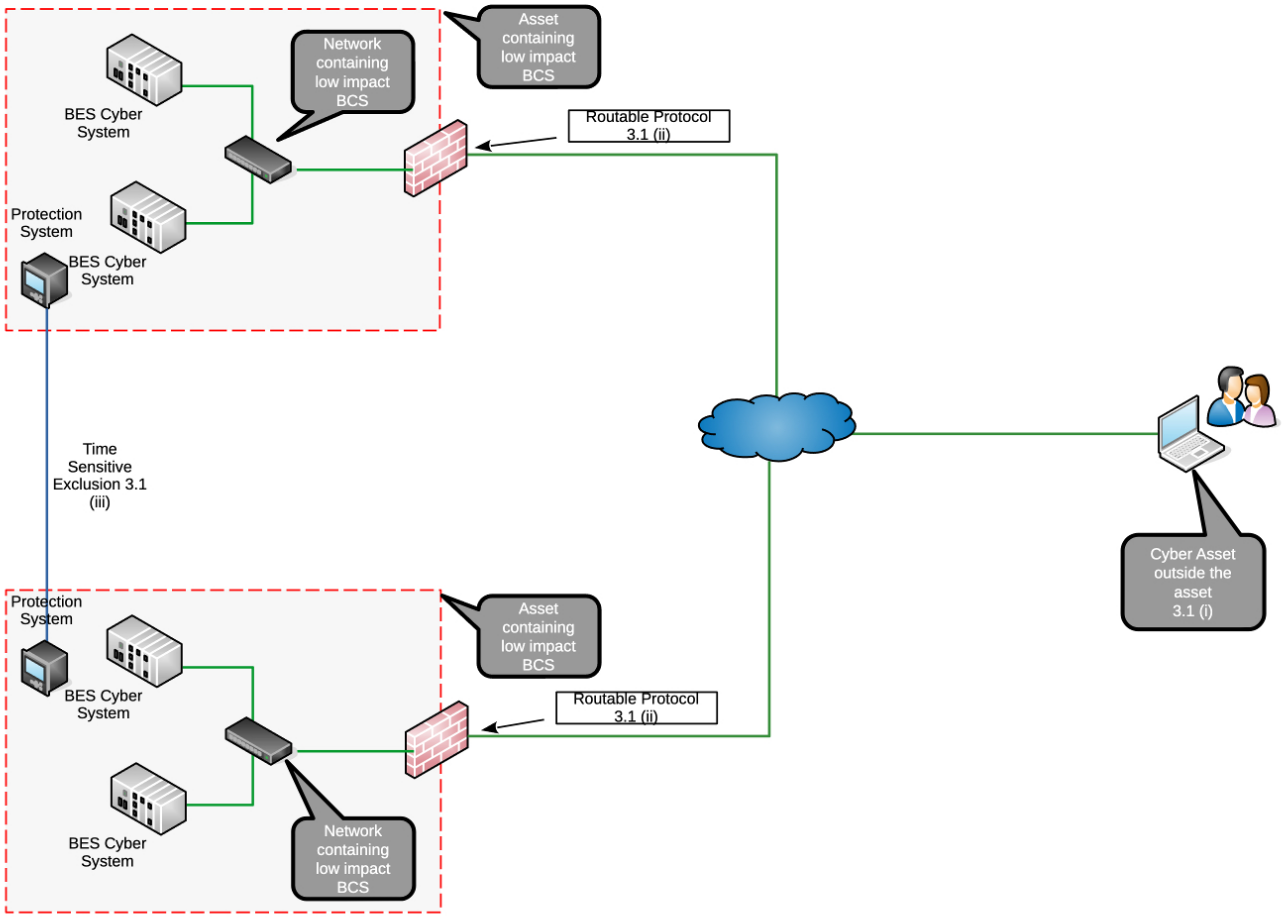


Figure 1

Section 3.1.1

The objective of Section 3.1.1 is to maintain the original language used in CIP-003-9, Section 3.1.

Section 3.1.2

This is an expanded cyber security control outlined in the SAR. The scope is expanded from CIP-003-9, Section 6.3 to include all communications rather than vendor specific communications. The objective of Attachment 1 Section 3.1.2 is for entities to mitigate the risk posed by malicious communications to or from low impact BES Cyber Systems. The detection of known or suspected malicious communications can be accomplished in several ways. For example, Figure 2 depicts implementing the control (e.g., Intrusion Detection System (IDS) in a centralized location (e.g., at a corporate hub site) rather than at every distributed "asset containing LIBCS" such as substations in this example "hub and spoke" model. The

obligation in Section 3.1.2 requires that entities implement controls to detect known or suspected inbound and outbound malicious communications between a LIBCS and a Cyber Asset(s) outside the asset containing LIBCS (s) thus allowing entity flexibility in where the control is implemented based on their architecture.

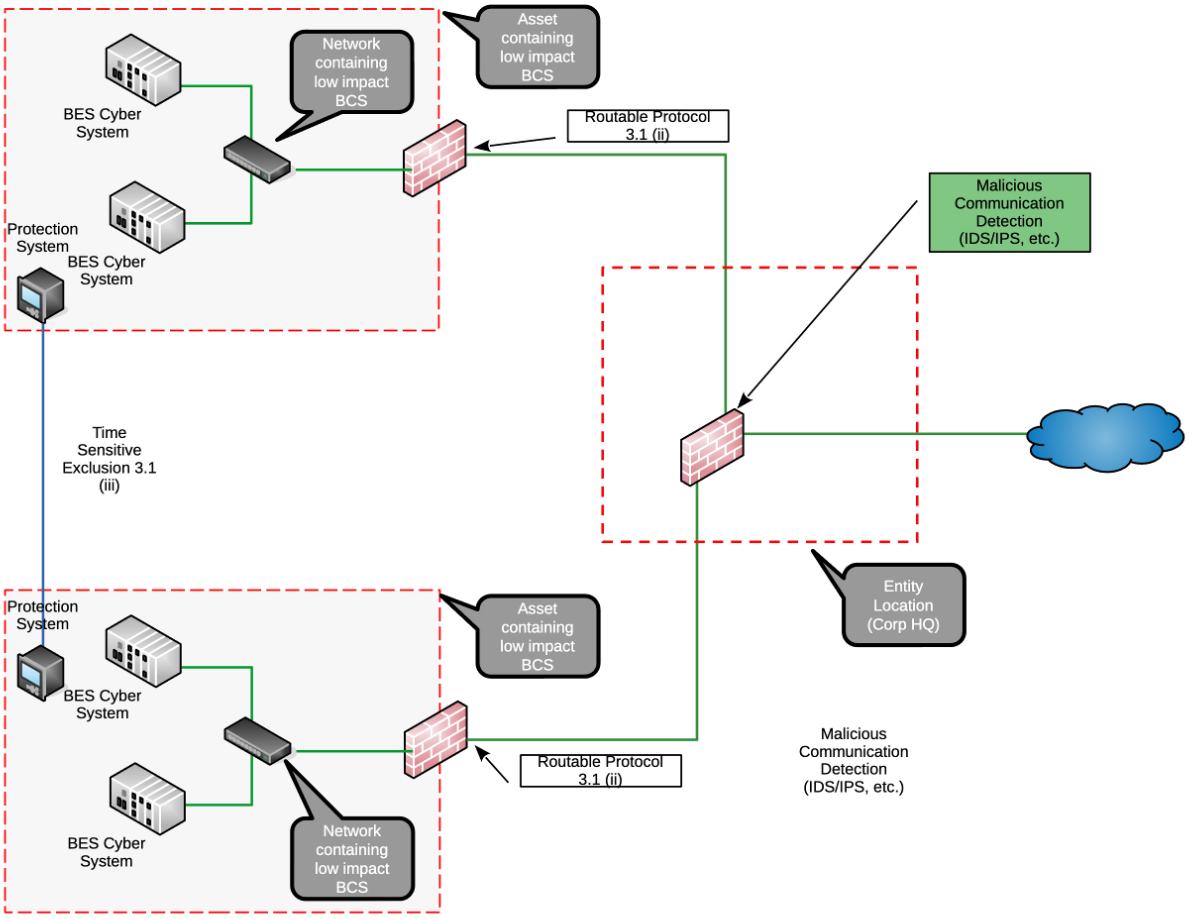


Figure 2

Section 3.1.3

This is a new cyber security control outlined in the SAR, which requires entities to implement controls to authenticate users when permitting (allowing) each instance of electronic remote access to networks containing low impact BES Cyber Systems. The intent is at the time any access to the "network containing low impact BES Cyber Systems" is being permitted, the remote user is already authenticated. Figure 3 below depicts a situation where the authentication of the remote user is occurring after the user already has access to the "network containing LIBCS" as the authentication servers are on the same network with the LIBCS. The firewall in this scenario allows the user through to the network on which the LIBCS reside before the user is authenticated.

The intention of “each instance” phrase is meant to include the initial authorization and all subsequent re-connection instances of electronic remote access to the network. If there is a collection of sub-networks or Cyber Assets within the network containing LIBCS, then multiple re-authentications at those levels would not be required. This control mitigates the risk of unauthenticated user access to networks on which LIBCS reside.

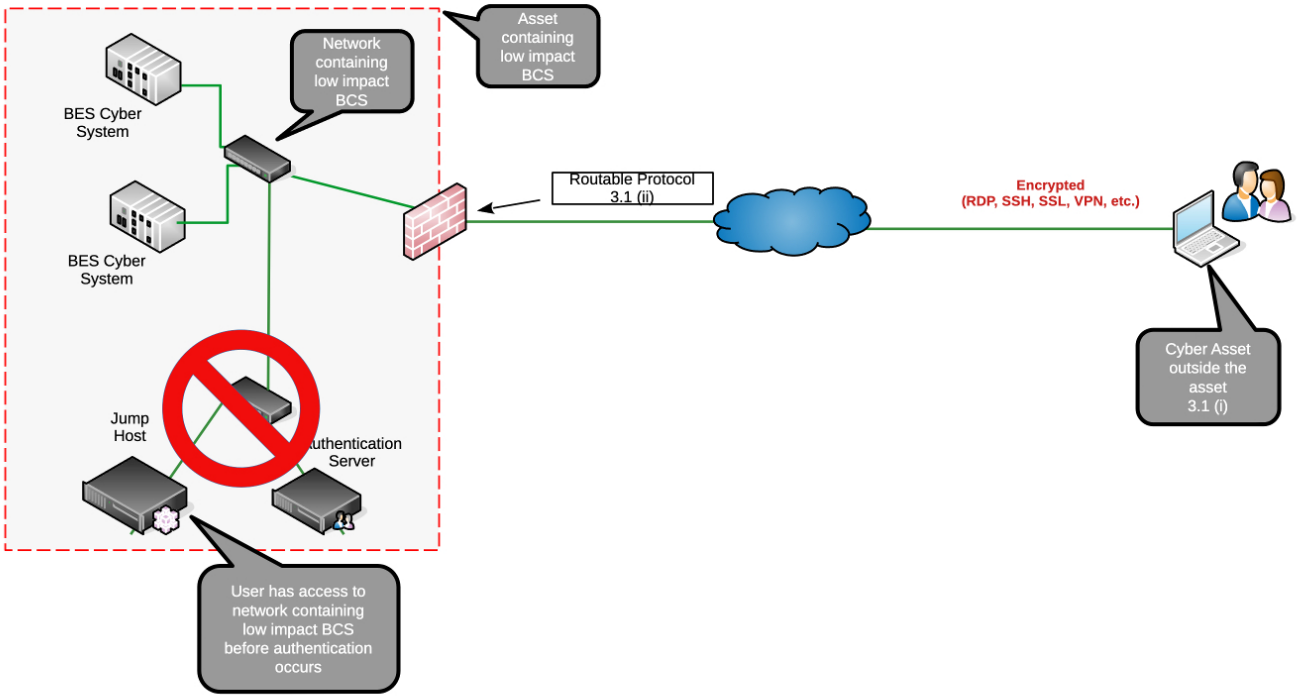


Figure 3

Section 3.1.4

This is a new cyber security control outlined in the SAR. The objective of Attachment 1, Section 3.1.4 is for entities to protect the user authentication information (e.g., username, password, multi-factor authentication (MFA) information, session token, etc.) while in transit between the remote user’s Cyber Asset and either the asset containing the LIBCS or the entity’s authentication system used to meet Section 3.1.3. The intent is not to specify authentication directly to a particular device, but to allow for entities that desire to use an existing compliant CIP-005 Requirement R2 Intermediate System or similar

architecture for access to networks containing LIBCS as well. For example, Figure 4 below depicts authentication at the boundary of the asset containing a LIBCS. In this example, the authentication server and jump host are on a different network than the "network containing LIBCS", making it uniquely different from Figure 3 above.

Figure 4 depicts an example of protected authentication at a central intermediate system before accessing a network containing a LIBCS. This protection mitigates the unintended disclosure of authentication information for remote access of LIBCS.

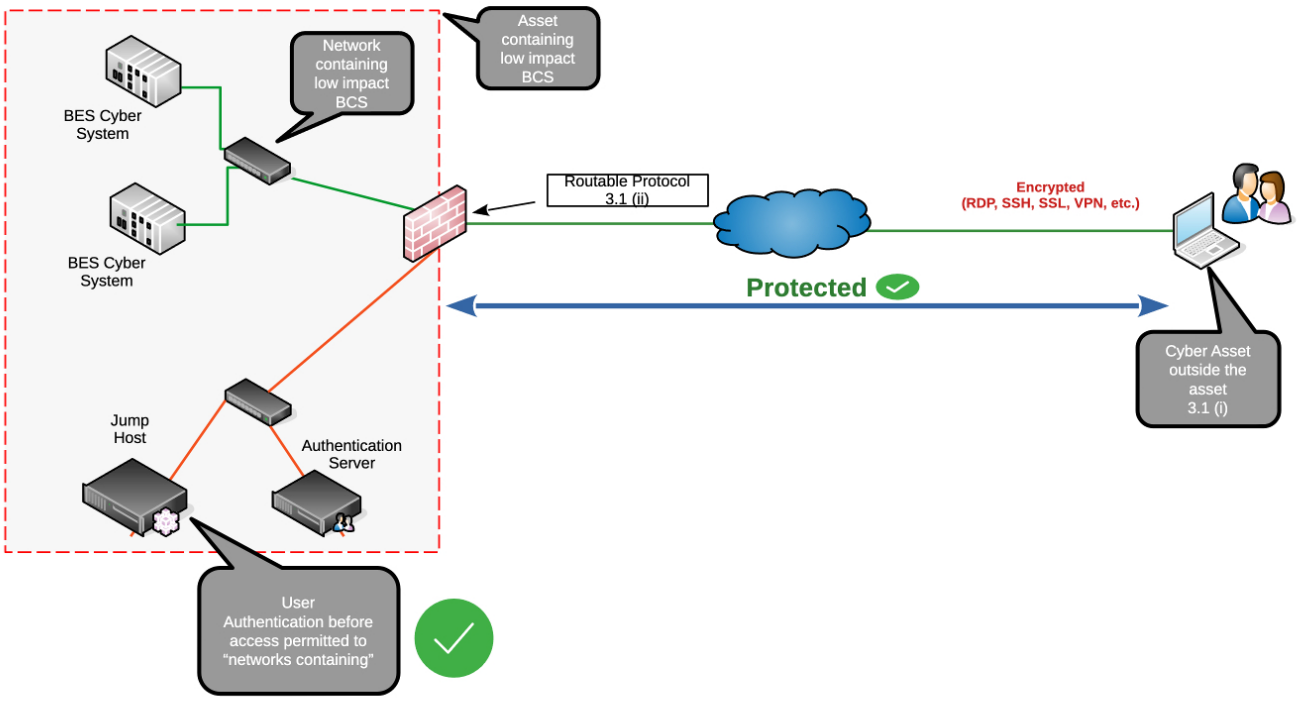


Figure 4

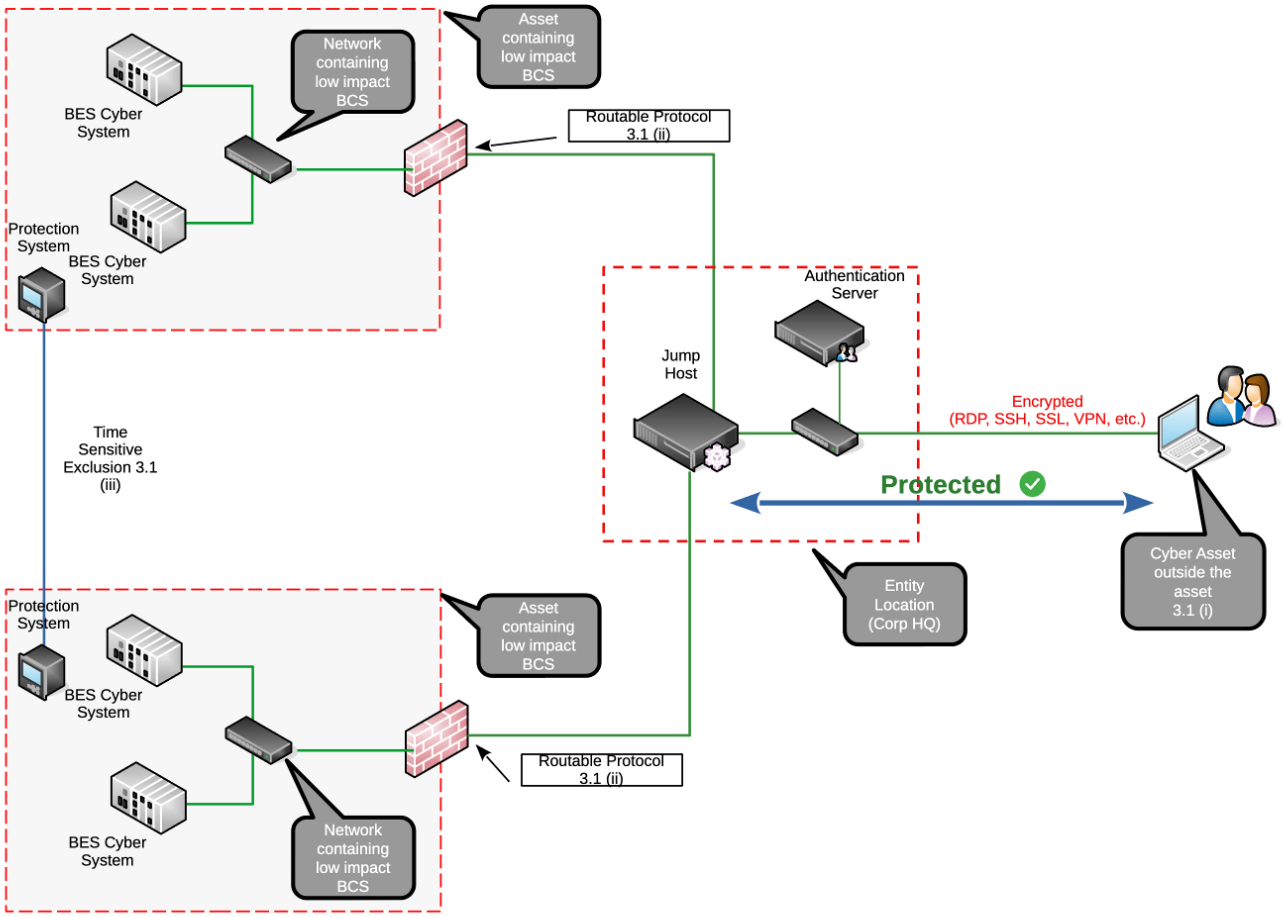


Figure 5

Section 3.1.5

The objective of Section 3.1.5 is to maintain the original language used in CIP-003-9, Section 6.1, as much as possible. One or more method(s) can be identified as part of this electronic access control. Entities must determine vendor electronic remote access, where permitted, to their low impact BES Asset(s) and/or LIBCS. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access.

Section 3.1.6

The objective of Section 3.1.6 is to maintain the original language used in CIP-003-9, Section 6.2, as much as possible. One or more method(s) can be identified as part of this electronic access control. Entities must have the ability to disable vendor electronic remote access, where permitted, for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing LIBCS.

Section 3.2

The objective of Section 3.2 is to maintain the original language used in CIP-003-9, Section 3.2, as much as possible.

Rationale for Attachment 2

The SDT made conforming changes to Attachment 2 merging Sections 3 and 6, and providing examples of compliance related activities.

Previous CIP-003 Versions Technical Rationale

Project 2020-03 Supply Chain Low Impact Revisions (CIP-003-9) Technical Rationale

Project 2016-02 Modifications to CIP Standards (CIP-003-Y) Technical Rationale

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2023-04 Modifications to CIP-003

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on draft two of Reliability Standard **CIP-003-A – Cyber Security – Security Management Controls** by **8 p.m. Eastern, Thursday, March 14, 2024.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Chris Larson (via email), or at 404-446-9708.

Background

In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact Bulk Electric System (BES) Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts who were representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the Standard Authorization Request (SAR) at its March 22, 2023 meeting.

The LICRT report recognized that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The LICRT recommended enhancing the existing low impact category to further mitigate the coordinated attack risk. The proposed project will revise CIP-003-9 to add electronic access controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications for assets containing low impact BES Cyber Systems with external routable connectivity.

Please provide your responses to the questions listed below, along with any detailed comments.

Questions

1. Do you agree with the language proposed in CIP-003-A Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

2. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

3. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-A. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.

   ☐ Yes
   ☐ No

   Comments:

4. The DT believes the language of CIP-003-A addresses the issues outlined in the SAR in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

5. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2023-04 Modifications to CIP-003

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2023-04 Modifications to CIP-003. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

Justification for VRFs and VSLs

- Requirement R1: The VRF and VSLs did not change from the previously FERC-approved CIP-003-9 Reliability Standard.
- Requirement R2: The VRF did not change from the previously FERC-approved CIP-003-9 Reliability Standard. VSL changes are outlined below.
- Requirement R3: The VRF and VSLs did not change from the previously FERC-approved CIP-003-9 Reliability Standard.
- Requirement R4: The VRF and VSLs did not change from the previously FERC-approved CIP-003-9 Reliability Standard.

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity implemented all electronic access controls, but failed to document the electronic access	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems,	The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment	but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls, but failed to implement one or two controls listed in Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2)	containing low impact BES Cyber Systems, but failed to implement three or more controls listed in Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2)	

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

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)	documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)	

VSL Justifications for CIP-003-A, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSLs for Requirement R2 are similar to the previous VSLs of CIP-003-9, with a few revisions. Created Moderate and High VSL based on the number of controls implemented. Removed mentions of Attachment 1, Section 6, since Section 6 was merged with Section 3.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Requirement R2 is not a "binary" type requirement. Violation severity levels are clear, quantitative, and non-ambiguous.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The VSL level assignments are consistent with language in Requirement R2 and Attachment 1.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The violation severity levels relate to a single violation. A failure to do multiple portions of Requirement R2, Attachment 1 is considered a single violation.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-04 Modifications to CIP-003

Formal Comment Period Open through March 14, 2024

Now Available

A 45-day formal comment period for draft two of **CIP-003-A – Cyber Security – Security Management Controls**, is open through **8 p.m. Eastern, Thursday, March 14, 2023.**

The standard drafting team's considerations of the responses received from the previous comment period are reflected in this draft of the standard.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An additional ballot for the standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **March 5 - 14, 2024**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Chris Larson (via email) or at 404-446-9708. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003 observer list” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2023-04 Modifications to CIP-003 | Draft 2
Comment Period Start Date:	1/30/2024
Comment Period End Date:	3/14/2024
Associated Ballots:	2023-04 Modifications to CIP-003 CIP-003-A AB 2 ST 2023-04 Modifications to CIP-003 Implementation Plan AB 2 OT

There were 71 sets of responses, including comments from approximately 169 different people from approximately 111 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the language proposed in CIP-003-A Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

2. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

3. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-A. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.

4. The DT believes the language of CIP-003-A addresses the issues outlined in the SAR in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical, or procedural justification.

5. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Husam Al-Hadidi	Manitoba Hydro (System Preformance)	1,3,5,6	MRO
					Kimberly Bentley	Western Area Power Adminstration	1,6	MRO
					Jaimin Patal	Saskatchewan Power Coporation (SPC)	1	MRO
					George Brown	Pattern Operators LP	5	MRO
					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Dane Rogers	Oklahoma Gas and Electric (OG&E)	1,3,5,6	MRO

					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Ayotte	ITC Holdings	1	MRO
					Andrew Coffelt	Board of Public Utilities-Kansas (BPU)	1,3,5,6	MRO
					Peter Brown	Invenergy	5,6	MRO
					Angela Wheat	Southwestern Power Administration	1	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC
					Nehtisha Rollis	Tennessee Valley Authority	5	SERC
Manitoba Hydro	Jay Sethi	1,3,5,6	MRO	Manitoba Hydro Group	Nazra Gladu	Manitoba Hydro	1	MRO
					Mike Smith	Manitoba Hydro	3	MRO
					Kristy-Lee Young	Manitoba Hydro	5	MRO
					Kelly Bertholet	Manitoba Hydro	6	MRO
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC

					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
Southern Company - Southern Company Services, Inc.	Jennifer Tidwell	1,3,5,6	SERC	Southern Company	Leslie Burke	Southern Company - Southern Company Generation	5	SERC
					Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Nick Fogleman	Prairie Power, Inc.	1,3	SERC
					Cooper Cash	North Carolina Electric Membership Corporation	3,4,5	SERC
Public Utility District No. 2 of Grant County, Washington	Karla Weaver	4		GCPD Group	Karla Weaver	Grant County PUD	4	WECC
					Nikkee Hebdon	Public Utility District No. 2 of Grant County, Washington	5	WECC
					Joanne Anderson	Public Utility District No. 2 of Grant County, Washington	1	WECC

					Mike Stussy	Public Utility District No. 2 of Grant County, Washington	6	WECC
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy- FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
Black Hills Corporation	Rachel Schuldt	6		Black Hills Corporation - All Segments	Micah Runner	Black Hills Corporation	1	WECC
					Josh Combs	Black Hills Corporation	3	WECC
					Rachel Schuldt	Black Hills Corporation	6	WECC
					Carly Miller	Black Hills Corporation	5	WECC
					Sheila Suurmeier	Black Hills Corporation	5	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Alain Mukama	Hydro One Networks, Inc.	1	NPCC
					Deidre Altobell	Con Edison	1	NPCC
					Jeffrey Streifling	NB Power Corporation	1	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC

Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
Randy Buswell	Vermont Electric Power Company	1	NPCC
James Grant	NYISO	2	NPCC
John Pearson	ISO New England, Inc.	2	NPCC
Harishkumar Subramani Vijay Kumar	Independent Electricity System Operator	2	NPCC
Randy MacDonald	New Brunswick Power Corporation	2	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
David Burke	Orange and Rockland	3	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
David Kwan	Ontario Power Generation	4	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
Glen Smith	Entergy Services	4	NPCC
Sean Cavote	PSEG	4	NPCC
Jason Chandler	Con Edison	5	NPCC
Tracy MacNicoll	Utility Services	5	NPCC

					Shivaz Chopra	New York Power Authority	6	NPCC
					Vijay Puran	New York State Department of Public Service	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					Joshua London	Eversource Energy	1	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC

					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
Santee Cooper	Vicky Budreau	3		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC

1. Do you agree with the language proposed in CIP-003-A Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD does not agree with the wording of Attachment 1, Section 3.1.3 which states:

“Authenticate users when permitting **each user-initiated instance** of electronic access to a network(s) containing low impact BES Cyber Systems;”

It is not feasible to authenticate each user-initiated instance of electronic access since doing so limits the technical solutions for implementing such a control. For example – if a registered entity were to implement a jump host solution, a user may be able to authenticate to the jump host and be permitted to access the low impact BES Cyber System based on successfully authenticating to the jump host. If the user established multiple connections from the jump host into multiple low impact BES Cyber Systems at different low impact assets, the proposed language may be interpreted as requiring additional authentication for each connection to other low impact BES Cyber Systems.

Section 3.1.3 as currently written is stricter than the high or medium impact Interactive Remote Access (IRA) requirements where “each user-initiated instance” of IRA ***DOES NOT*** require additional authentication for each connection.

SMUD recommends the Standards Drafting Team change the language in Section 3.1.3 to read:

“3.1.3 Authenticate users prior to permitting user-initiated electronic access to a network(s) containing low impact BES Cyber Systems;”

This suggested wording aligns better with the SAR, whereas the existing wording does not indicate that users must be authenticated ***before*** access is granted to networks containing low impact BES Cyber Systems. The way in which Section 3.1.3 is currently written, it is as if the connection requires the authentication rather than the user being authenticated.

SMUD also recommends the Standards Drafting Team make the following conforming changes to the language in Section 3.1.4 to read:

“3.1.4 Protect user authentication information for user-initiated electronic access while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

• the authentication system used to meet Section 3.1.3, or

• the asset containing low impact BES Cyber System(s);”

Likes 2	Orlando Utilities Commission, 5, Colon Dania; American Municipal Power, 5, Ritts Amy
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 5,6

Answer	No
Document Name	
Comment	

NRG disagrees with the removal of the term “remote” when referencing “electronic remote access” throughout Attachment 1. Not only does this significantly expand the scope of the requirements with respect to any type of non-remote electronic access, but it also moves away from the original intent of the three recommendations initially proposed by the LICRT. NRG recommends expanding the definition of the current term “interactive remote access” to include Low Impact BES Cyber Systems and using that newly defined terminology throughout this requirement.

Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	

James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	

Section 3.2 states the Responsible Entity shall implement a control(s) that authenticates all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 3.2 should be removed, and Dial-up connectivity should be excluded from CIP-003-A regulations for LOW impact BES Cyber Systems.

Likes 0	
Dislikes 0	
Response	

Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	

NRG disagrees with the removal of the term “remote” when referencing “electronic remote access” throughout Attachment 1. Not only does this significantly expand the scope of the requirements with respect to any type of non-remote electronic access, but it also moves away from the original intent of the three recommendations initially proposed by the LICRT. NRG recommends expanding the definition of the current term “interactive remote access” to include Low Impact BES Cyber Systems and using that newly defined terminology throughout this requirement.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment

It appears that the Attachment 1 Section 3, Part 3.1.3 language is not restricted to the initial user authentication to a central management system that controls the access to multiple low impact BCS, as was intended by the SDT. Additionally, the lead-in statement in Section 3.1 (and i-iii) defines what type of access to control, and it appears that the access described in the current Section 3.1.3 would not be in-scope of the electronic access defined in Section 3.1, and therefore would not create a required control. This is due to Section 3.1 (i) defining access as “between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing…”, not “between a network containing a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing…”.

Tacoma Power suggests the following language for Section 3.1.3:

“Authenticate user-initiated electronic access to a network(s) containing low impact BES Cyber Systems prior to establishing access applicable to Section 3.1;”

Note this change may be better as a new section in Attachment 1, for example, Section 3.3.

The above change would also lead to conforming changes in Section 3.1.4, as follows:

“Protect user authentication information for user-initiated electronic access while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and:

• the authentication system used to meet Section 3.1.3, or

• the asset containing low impact BES Cyber System(s);”

Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	

Response

Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna

Answer	No
Document Name	

Comment

The wording in 3.1.3 as written could be read as requiring authentication each time a user accesses a network containing a Low Impact BES Cyber System, which would be stricter than the allowed jump host for medium and high impact requirements. Possible suggested wording to 3.1.3 are as follows:

“Authenticate users prior to user-initiated electronic access to a network(s) containing low impact BES Cyber Systems.”

Or

“Authenticate users prior to user-initiated electronic access to a network(s) containing low impact BES Cyber Systems (multiple re-authentications are not required when accessing multiple sub networks within a larger network)”

The wording for 3.1.4 should be updated as well to match the suggested wording in 3.1.3:

“Protect authenticated information for user-initiated electronic access while in transit between ….”

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

Section 3.2 states the Responsible Entity shall implement a control(s) that authenticates all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 3.2 should be removed, and Dial-up connectivity should be excluded from CIP-003-A regulations for LOW impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Although section 3.1.2 is within the scope of the SAR, BPA still believes it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. The proposed language requires detection of known/suspected malicious communications

for “inbound and outbound electronic remote access.” There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5).

BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS or the applicability be changed to bring it in-line with other requirements.

Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Matthew Jaramilla, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

Salt River Project agrees and supports comments from SMUD and Tacoma Power.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB

Answer	No
Document Name	

Comment

Requirement 3.1.4 is not clear regarding what protection of the user authentication information is required. Please work to consolidate 3.1.3 and 3.1.4. The objectives are unclear. While substantial clarity was provided in the explanatory Webex, the proposed language lacks that clarity.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment
SMUD does not agree with the wording of Attachment 1, Section 3.1.3 which states: “Authenticate users when permitting **each user-initiated instance** of electronic access to a network(s) containing low impact BES Cyber Systems;” It is not feasible to authenticate each user-initiated instance of electronic access since doing so limits the technical solutions for implementing such a control. For example – if a registered entity were to implement a jump host solution, a user may be able to authenticate to the jump host and be permitted to access the low impact BES Cyber System based on successfully authenticating to the jump host. If the user established multiple connections from the jump host into multiple low impact BES Cyber Systems at different low impact assets, the proposed language may be interpreted as requiring additional authentication for each connection to other low impact BES Cyber Systems. Section 3.1.3 as currently written is stricter than the high or medium impact Interactive Remote Access (IRA) requirements where “each user-initiated instance” of IRA ***DOES NOT*** require additional authentication for each connection. SMUD recommends the Standards Drafting Team change the language in Section 3.1.3 to read: “3.1.3 Authenticate users prior to permitting user-initiated electronic access to a network(s) containing low impact BES Cyber Systems;” This suggested wording aligns better with the SAR, whereas the existing wording does not indicate that users must be authenticated ***before*** access is granted to networks containing low impact BES Cyber Systems. The way in which Section 3.1.3 is currently written, it is as if the connection requires the authentication rather than the user being authenticated. SMUD also recommends the Standards Drafting Team make the following conforming changes to the language in Section 3.1.4 to read: “3.1.4 Protect user authentication information for user-initiated electronic access while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and • the authentication system used to meet Section 3.1.3, or • the asset containing low impact BES Cyber System(s);”

Likes 0	
Dislikes 0	

Response

TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	

Comment
Southern Indiana Gas and Electric (SIGE) appreciate the work of the drafting team to address previous feedback provided for CIP-003-A Attachment 1. SIGE suggests the following changes in bold in order to qualify the type of access that is being addressed by this standard. The use of the verbiage “user-initiated instance of electronic access” could easily be interpreted as any user log-in. The act of a user logging into a local HMI at a substation is technically a “user-initiated instance of electronic access .“ The suggested changes are intended to mimic the Interactive Remote Access term as defined in the NERC Glossary of terms, while not making any reference to an ESP.

3.1.3 Authenticate users when permitting each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, to a network(s) containing low impact BES Cyber Systems;

3.1.4 Protect user authentication information for each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

• the authentication system used to meet Section 3.1.3, or

• the asset containing low impact BES Cyber System(s);

3.1.5 Include one or more method(s) for determining vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment

Tri-State agrees with SMUD's comments below:

SMUD does not agree with the wording of Attachment 1, Section 3.1.3 which states:

“Authenticate users when permitting **each user-initiated instance** of electronic access to a network(s) containing low impact BES Cyber Systems;”

It is not feasible to authenticate each user-initiated instance of electronic access since doing so limits the technical solutions for implementing such a control. For example – if a registered entity were to implement a jump host solution, a user may be able to authenticate to the jump host and be permitted to access the low impact BES Cyber System based on successfully authenticating to the jump host. If the user established multiple connections from the jump host into multiple low impact BES Cyber Systems at different low impact assets, the proposed language may be interpreted as requiring additional authentication for each connection to other low impact BES Cyber Systems.

Section 3.1.3 as currently written is stricter than the high or medium impact Interactive Remote Access (IRA) requirements where “each user-initiated instance” of IRA ***DOES NOT*** require additional authentication for each connection.

SMUD recommends the Standards Drafting Team change the language in Section 3.1.3 to read:

“3.1.3 Authenticate users prior to permitting user-initiated electronic access to a network(s) containing low impact BES Cyber Systems;”

This suggested wording aligns better with the SAR, whereas the existing wording does not indicate that users must be authenticated ***before*** access is granted to networks containing low impact BES Cyber Systems. The way in which Section 3.1.3 is currently written, it is as if the connection requires the authentication rather than the user being authenticated.

SMUD also recommends the Standards Drafting Team make the following conforming changes to the language in Section 3.1.4 to read:

“3.1.4 Protect user authentication information for user-initiated electronic access while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

• the authentication system used to meet Section 3.1.3, or

• the asset containing low impact BES Cyber System(s);”

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	No
Document Name	

Comment

Reclamation recommends aligning language with CIP-005-7 language or first focusing on modifying CIP-005-7 language prior to adjusting language for CIP-003-A.

Likes 0	
Dislikes 0	

Response

Carver Powers - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

The verbiage scoping required controls to the identified communication paths is eliminated in the proposed drafted language. Recommend clearly scoping the controls from 3.1.1 through 3.1.6 to the communications identified in 3.1 i-iii. Without this clarification:

1. There is no determination of the boundary for inbound and outbound in 3.1.1 and 3.1.2

2. 3.1.3 would require authentication for all user logins, including local logins.

3. 3.1.5 and 3.1.6 would apply to vendors using TCAs.

The information in Attachment 2 states "electronic access meets the criteria specified in Section 3.1" for 3.1.1 through 3.1.6, this language should be included in Attachment 1.

The phrase “User initiated instance electronic access” should align more closely with the first sentence of the Interactive Remote Access definition to provide consistency and clarity. Without this clarity the language could include system to system communications.

Recommending using a more consolidated term than “inbound and outbound electronic access”. If meaning bi-directional, then the standard should state that versus drawing a distinction between inbound and outbound.

Likes 0	
Dislikes 0	

Response

Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Santee Cooper does not agree with the wording of Attachment 1, Section 3.1.3 which states: "Authenticate users when permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems;"

It would be difficult to authenticate each user-initiated instance of electronic access. For example, if a user established multiple connections from the jump host into multiple low impact assets, the proposed language may be interpreted as requiring additional authentication for each connection to other low impact assets. This would make the CIP-003 Attachment 1, Section 3.1.3 requirement stricter than the high or medium impact Interactive Remote Access (IRA) requirement that doesn’t require additional authentication for each connection.

In addition, the existing wording does not indicate that users must be authenticated before access is granted to a network(s) containing low impact assets. The way 3.1.3 is currently written, it is as if the connection requires the authentication rather than the user being authenticated.

Likes 0	
Dislikes 0	

Response

Alain Mukama - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

For both sub-requirements 3.1.5 and 3.1.6 in Attachment 1, clarification is required on whether it includes both Interactive Remote Access and system-to-system remote access.

Likes 0	
Dislikes 0	

Response

Mark Flanary - Midwest Reliability Organization - 10	
Answer	No
Document Name	

Comment
MRO interprets the draft Requirement language in Section 3.1.3 such that authentication is required each time a user initiates electronic access to any network(s) containing low impact BCSs. This interpretation of the language does not support the single authentication asserted by the SDT during the Project 2023-04 Webinar, relating to the jumphost in Figure 5 in the Technical Rationale. MRO recommends the Requirement language in Section 3.1.3 be changed to support the SDT's assertions. Any changes to the Requirement language needs to ensure that any electronic access directly from a network containing low impact BES Cyber Asset to a different network(s) containing low impact BES Cyber Systems, when not using a centralized electronic access system (e.g. jumphost), still requires authentication. Recommended language change: **Authenticate users prior to permitting user-initiated instances of electronic access to a network(s) containing low impact BES Cyber Systems**

Likes 0	
Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	No
Document Name	

Comment
Attachment 1 appears to have exceeded the CIP-003 R2 (documented cybersecurity plan) due to the amount of technical controls that have now been added. Recommendation: if the SDT intends to keep expanding controls beyond the documented plans they should consider creating a new requirement. Why is this phrase used "User initiated instance electronic access". Recommending using a more consolidated term than "inbound and outbound electronic access". If meaning bi-directional, then the standard should state that versus drawing a distinction between inbound and outbound. Sub requirement 3.15, request clarification on whether the sub requirement applies to both system to system and user-initiated access by a vendor.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA supports comments made by SMUD and Tacoma Power.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI appreciates the work of the drafting team to address previous feedback provided for CIP-003-A Attachment 1, but proposes the following modifications to Section 3, Part 3.1.3: “Authenticate users **prior to** permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems **(multiple re-authentications to sub-networks within a larger network are not required)**;**”** We also suggest including clear language in the implementation guidance describing the change from use of the term remote access to electronic access including the relationship between the term electronic access and scoping language used in Section 3, Part 3.1, i-iii.	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	No
Document Name	
Comment	
The term “user-initiated instance” needs to be further clarified. We require more clarification on how much weight the technical rationale will have in interpreting compliance with Sections 3.1.3 and 3.1.4 with regulators when completing compliance monitoring activities. We believe the removal of the word “remote” from Section 3.1.3 in permitting user-initiated instances can create confusion on when a user is required to authenticate.	

Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	

NEE's initial interpretation of CIP-003 Attachment 1 Section 3.1 was that the SDT's goal for inbound and outbound malicious communications protection was tied to firewalls or routers at each low BES Asset. However, the current language does not provide flexibility for managing inbound and outbound malicious communication security controls centrally, as illustrated in the Technical Rationale for Section 3.1.2.

The standard language appears to imply medium impact Electronic Security Perimeter (ESP) and Electronic Access Point (EAP) protections at each low impact BES Asset without explicitly stating this. Section 3.1.4's authentication communication protection implies encryption at each remote cyber asset, exceeding medium impact requirements with Intermediate Systems.

The Low Impact Criteria Review Team's (LICRT) intent was to address risk reduction for coordinated attacks on low BES Assets. Management of low impact security controls for authentication and malware mitigation, either locally or centrally, should be accommodated in Section 3.1 language. Implying controls are mandated at each low BES Asset goes beyond the LICRT's effort.

While the Technical Rationale illustration for Section 3.1.2 provides for central aggregation, it does not address Section 3.1.4 if encrypted authentication communications pass through a central malware mitigation system for inbound and outbound traffic. The SDT should consider adjusting the language to allow both centralized and local security control options and clarify what options are available.

Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	

The language used should prioritize risk-based assessment with a focus on operational impact.

Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric (CEHE) appreciates the work of the drafting team to address previous feedback provided for CIP-003-A Attachment 1. CEHE suggests the following changes in bold in order to qualify the type of access that is being addressed by this standard. The use of the verbiage “user-initiated instance of electronic access” could easily be interpreted as any user log-in. The act of a user logging into a local HMI at a substation is technically a “user-initiated instance of electronic access .“ The suggested changes are intended to mimic the Interactive Remote Access term as defined in the NERC Glossary of terms, while not making any reference to an ESP.

3.1.3 Authenticate users when permitting each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, to a network(s) containing low impact BES Cyber Systems;

3.1.4 Protect user authentication information for each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

• the authentication system used to meet Section 3.1.3, or

• the asset containing low impact BES Cyber System(s);

3.1.5 Include one or more method(s) for determining vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please explain why, and provide recommended language you would support and, if appropriate, technical, or procedural justification.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
It is NST's understanding, based on the Technical Rationale document and the SDT's March 6, 2024 project webinar, that once a remote user has been authenticated in accordance with proposed requirement 3.1.3 and allowed to access a network containing low impact BCS, a Responsible Entity could, if it was so inclined, allow that user to connect to multiple BCS within that network, without re-authentication, for the duration of any given instance of remote electronic access. We believe that 3.1.3 should be modified to make this clear.	
Likes 1	LS Power Development, LLC, 5, Campbell C. A.
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	No
Document Name	
Comment	
LS Power Development agrees with comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	

Answer	No
Document Name	
Comment	
Seminole Electric votes negative because the standard drafting team has failed to justify within their technical rationale the need and the basis for all of the additional requirements for low impact sites	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC

Answer	No
Document Name	
Comment	
Attachment 1 appears to have exceeded the CIP-003 R2 (documented cybersecurity plan) due to the amount of technical controls that have now been added. Recommendation: if the SDT intends to keep expanding controls beyond the documented plans they should consider creating a new requirement. Why is this phrase used “User initiated instance electronic access”. Recommending using a more consolidated term than “inbound and outbound electronic access”. If meaning bi-directional, then the standard should state that versus drawing a distinction between inbound and outbound. Sub requirement 3.15, request clarification on whether the sub requirement applies to both system to system and user-initiated access by a vendor.	
Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	

Response

Karla Weaver - Public Utility District No. 2 of Grant County, Washington - 4, Group Name GCPD Group	
Answer	No
Document Name	
Comment	
GCPD agrees and supports comments from SMUD and Tacoma Power about Appendix A section 3.13. This wording is more restrictive than IRAs utilized for Medium and High Impact access.	
Likes 0	
Dislikes 0	

Response

Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
The modification to 3.1 iii is more limiting than intended. There are time-sensitive communications protocols that are unrelated to Protection Systems. The challenge for 3.1.2 lies in the fact these terms used have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, using these same words with different examples in the measures creates ambiguity in the expectations for compliance. The prescriptiveness of 3.1.3 and 3.1.4 seems to go beyond what is typically expected for Medium Impact.	
Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the proposed langauge but also supports EEI's alternative language for added clarity.	

Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	Yes
Document Name	

Comment

Alliant Energy supports comments submitted by MRO NSRF.

Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	

Response

Karen Artola - CPS Energy - 1,3,5 - Texas RE

Answer	Yes
Document Name	

Comment

Time-sensitive communications of Protection Systems needs to be clearly defined.

Likes 0	
Dislikes 0	

Response

Amy Wilke - American Transmission Company, LLC - 1

Answer	Yes
Document Name	

Comment

Thank you for considering and addressing the concerns by changing 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the “asset containing” or the authentication source used in 3.1.3 (such as an Intermediate System).

Likes 0	
Dislikes 0	

Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
For Section 3.1.3, the NSRF recommends changing “when” to “prior to” in order to clarify that the remote user be authenticated prior to access, as explained in the Technical Rationale. Additionally, the currently proposed language does not contain the clarification stated in the Technical Rationale that would allow a single authentication for user-initiated access to low impact BCS that reside in a sub-network contained within a larger network. The NSRF recommends adding a parenthetical to Section 3.1.3 to align with that intent. Example: 3.1.3 Authenticate users **prior to** permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems **(multiple re-authentications to sub-networks within a larger network are not required)**; MRO NSRF is of the belief that both of these suggested changes would be non-substantive and could be implemented prior to final ballot, if this ballot is successful.	
Likes 2	Orlando Utilities Commission, 5, Colon Dania; American Municipal Power, 5, Ritts Amy
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	

For Section 3.1.3, Manitoba Hydro recommends changing “when” to “prior to” in order to clarify that the remote user be authenticated prior to access, as explained in the Technical Rationale.

Additionally, the currently proposed language does not contain the clarification stated in the Technical Rationale that would allow a single authentication for user-initiated access to low impact BCS that reside in a sub-network contained within a larger network. Manitoba Hydro recommends adding a parenthetical to Section 3.1.3 to align with that intent.

Example: 3.1.3 Authenticate users **prior to** when permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems **(multiple re-authentications to sub-networks within a larger network are not required)**;

Manitoba Hydro is of the belief that both of these suggested changes would be non-substantive and could be implemented prior to final ballot, if this ballot is successful.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker

Answer	Yes
Document Name	

Comment

Cleco agrees with EEI comments.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer	Yes
Document Name	

Comment

Black Hills Corporation agrees with EEI’s proposal for the following modifications to Section 3, Part 3.1.3:

"Authenticate users **prior to** (*remove:* when) permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems **(multiple re-authentications to sub-networks within a larger network are not required);"** We also suggest including clear language in the implementation guidance describing the change from use of the term remote access to electronic access including the relationship between the term electronic access and scoping language used in Section 3, Part 3.1, i-iii.	
Likes 0	
Dislikes 0	
Response	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company is in agreement with EEI comments.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Jamie Monette On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Jamie Monette	
Answer	Yes
Document Name	
Comment	

The term user-initiated access creates ambiguity.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	Yes
Document Name	

Comment

The NAGF requests clarification regarding the language in section 3.1.3 for initial user-initiated access being adequate to move between low impact systems without additional authentication.

Likes 0	
Dislikes 0	

Response

Ben Hammer - Western Area Power Administration - 1

Answer	Yes
Document Name	

Comment

Recomended changes are in **bold**:

3.1.3 Authenticate users **prior to** permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems **(multiple re-authentications to sub-networks within a larger network are not required)**;

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster

Answer	Yes
Document Name	

Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the MRO NSRF for questions #1.	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
PNMR agrees with the language proposed in CIP-003-A Attachment 1. However, PNMR does agree with EEI in their suggestion to include clear language in the implementation guidance describing the change from the use of the term remote access to electronic access including the relationship between the term electronic access and scoping language used in Section 3, part 3.1, i-iii.	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Minnesota Power supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	Yes
Document Name	

Comment

Exelon is responding in alignment with the comments from the EEI.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	Yes
Document Name	

Comment

Exelon is responding in alignment with the comments from the EEI.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	Yes
Document Name	

Comment

ACES approves of the proposed changes, but at some point, to make the standards clearer, we should consider distinguishing between "electronic access" a logical network connection and an individual's "electronic access" ie the ability to use credentials to log into a Cyber Asset.

Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See EEI Comments	
Likes 0	
Dislikes 0	
Response	
Kristina Marriott - Miller Bros. Solar, LLC - 5 - MRO,WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	

Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Patricia Ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
We do not concur with the proposed language in Attachment 2 for the same reasons we do not agree with the language in Attachment 1. Please see the response to question 1 above.	
Likes 0	
Dislikes 0	
Response	

Karla Weaver - Public Utility District No. 2 of Grant County, Washington - 4, Group Name GCPD Group	
Answer	No
Document Name	
Comment	
Item 3 is the measure for section 3.1.3 which is too restrictive.	
Likes 0	
Dislikes 0	
Response	

Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
Seminole Electric votes negative and does not agree because the standard drafting team has failed to justify within their technical rationale the need and the basis for all of the additional requirements for low impact sites	
Likes 0	
Dislikes 0	

Response

C. A. Campbell - LS Power Development, LLC - 5	
Answer	No
Document Name	
Comment	
LS Power Development agrees with comments submitted by EEI.	
Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

CEHE does not support the language proposed in CIP-003-A Attachment 2.

SIGE suggests the following changes in bold in order to qualify the type of access that is being addressed by this standard. The use of the verbiage “user-initiated instance of electronic access” could easily be interpreted as any user log-in. The act of a user logging into a local HMI at a substation is technically a “user-initiated instance of electronic access.” The suggested changes are intended to mimic the Interactive Remote Access term as defined in the NERC Glossary of terms, while not making any reference to an ESP.

Attachment 2, Section 3:

3. For Section 3.1.3, documentation showing the ability to authenticate users when permitting each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, where **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, to a network(s) containing low impact BES Cyber Systems, such as:

• Authentication mechanism(s) including but not limited to:

{C}§ Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or

{C}§ Enforcement of Multi-Factor Authentication (MFA).

• Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;

• Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BES Cyber System; or

• Other operational, procedural, or technical controls.

4. For Section 3.1.4, documentation showing the ability to protect user authentication information for each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, where electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

• the authentication system used to meet Section 3.1.3, or

• the asset containing low impact BES Cyber System(s),

such as:

• Protection mechanism(s) including but not limited to:

{C}§ Implementation of an encrypted protocol or service (Hypertext Transfer Protocol

Secure (HTTPS), Secure Shell (SSH), etc.); or

{C}§ Implementation of an IPsec or Secure Sockets Layer (SSL) VPN.

{C}§ Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic remote access, where vendor electronic **remote** access, **not including system-to-system process communication**s, is permitted and electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, such as:

• Steps to preauthorize access;

• Alerts generated by vendor log on;

• Session monitoring;

• Security information management logging alerts;

• Time-of-need session initiation;

• Session recording;

• System logs; or

• Other operational, procedural, or technical controls.

6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted and electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, such as:

• Disabling vendor electronic **remote** access, **not including system-to-system process communications accounts**;

• Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic **remote** access, **not including system-to-system process communications**;

• Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic **remote** access, **not including system-to-system process communications**;

• Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);

• Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic **remote** access, **not including system-to-system process communications**; or

• Other operational, procedural, or technical controls.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	

Comment

The language used should prioritize risk-based assessment with a focus on operational impact.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	No

Document Name	
Comment	
Please updated Attachment 2 to include the updated Attachment 1 Section 3 controls requested in question 1.	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	No
Document Name	
Comment	
The additional discrete requirements and expansion to all inbound and outbound electronic access is a significant incremental increase in the requirements for low-impact assets. Pending on an organizations current cybersecurity maturity level, meeting and maintaining these requirements will take significant effort and cost. It is anticipated this will require entities to hire multiple additional full-time staff to maintain and partake in lengthy contract negotiations with OEMs and other remote access vendors to ensure the additional discrete details included in the language can be met. Although section 3.1.2 is within the scope of the SAR, we still believe it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. The proposed language requires detection of known/suspected malicious communications for “inbound and outbound electronic remote access.” There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5). We suggest that this requirement be removed for better consistency with the requirements for Medium BCS or the applicability be changed to bring it in-line with other requirements.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI proposes the following revisions to align with the proposal provided in response to Question 1. “For Section 3.1.3, documentation showing the ability to authenticate users **prior to** permitting each user-initiated instance of electronic access, where electronic access meets the criteria specified in Section 3.1, to a network(s) containing low impact BES Cyber Systems, such as…”	

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA supports comments made by SMUD and Tacoma Power.

Likes 0	
Dislikes 0	

Response

Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper

Answer	No
Document Name	

Comment

In Attachment 2, Section 3, Example 2, in the list of examples the "Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)" is the only one of the bulleted list that meets the security objective of the SAR.

For example:

· "Anti malware technologies" are at the host level and are not a great option for detecting "malicious communications at the network level". The controls should be network based and not host based.

· "Automated or manual log reviews" are too ambiguous, it would be best to specify what types of logs that would meet the security objective. Simply reviewing electronic access logs, for example, is not sufficient.

· "Alerting" and "Other operational, procedural, or technical controls" should be removed since they provide no real guidance.

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Attachment 1 - Ameren would like clarity in section 3.1.3. Is the Responsible Entity capable of relying on services/support vendors for user accounts and authentication? Attachment 2 - For section 3.1.5, Ameren would like clarity around the phrase "Security information management logging alerts." In CIP-007, this is described as "Security event monitoring."	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends aligning language with CIP-005-7 language or first focusing on modifying CIP-005-7 language prior to adjusting language for CIP-003-A.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Please see response to question #1. Attachment 2 language would need to be updated based on the proposed changes in Attachment 1.	
Likes 0	
Dislikes 0	

Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	

SIGE suggests the following changes in bold in order to qualify the type of access that is being addressed by this standard. The use of the verbiage “user-initiated instance of electronic access” could easily be interpreted as any user log-in. The act of a user logging into a local HMI at a substation is technically a “user-initiated instance of electronic access.” The suggested changes are intended to mimic the Interactive Remote Access term as defined in the NERC Glossary of terms, while not making any reference to an ESP.

Attachment 2, Section 3:

3. For Section 3.1.3, documentation showing the ability to authenticate users when permitting each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, where **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, to a network(s) containing low impact BES Cyber Systems, such as:

• Authentication mechanism(s) including but not limited to:

{C}§ Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or

{C}§ Enforcement of Multi-Factor Authentication (MFA).

• Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;

• Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BES Cyber System; or

• Other operational, procedural, or technical controls.

4. For Section 3.1.4, documentation showing the ability to protect user authentication information for each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, where electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

• the authentication system used to meet Section 3.1.3, or

• the asset containing low impact BES Cyber System(s),

such as:

• Protection mechanism(s) including but not limited to:

{C}§ Implementation of an encrypted protocol or service (Hypertext Transfer Protocol

Secure (HTTPS), Secure Shell (SSH), etc.); or

{C}§ Implementation of an IPsec or Secure Sockets Layer (SSL) VPN.

{C}§ Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic remote access, where vendor electronic **remote** access, **not including system-to-system process communication**s, is permitted and electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, such as:

• Steps to preauthorize access;

• Alerts generated by vendor log on;

• Session monitoring;

• Security information management logging alerts;

• Time-of-need session initiation;

• Session recording;

• System logs; or

• Other operational, procedural, or technical controls.

6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted and electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, such as:

• Disabling vendor electronic **remote** access, **not including system-to-system process communications accounts**;

• Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic **remote** access, **not including system-to-system process communications**;

• Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic **remote** access, **not including system-to-system process communications**;

• Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);

• Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic **remote** access, **not including system-to-system process communications**; or

• Other operational, procedural, or technical controls.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

In Attachment 2, Section 3, Example 2, there is only one bullet in the list of examples provided that meet the security objective of the SAR. That example is “Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)”.

The other bullets are not good examples for the following reasons:

“Anti-malware technologies” are at the host level and is not a great control for detecting “malicious communications at the network level;” malicious code - YES, malicious communications - NO. The controls should be network based and not host based.

“Automated or manual log reviews” depending on how they are done, is not a great control. It would be best to specify what types of logs that would meet the security objective (e.g. Security Incident and Event Management logs, Netflow, Jflow etc.). Simply reviewing electronic access logs, for example, is not sufficient.

“Alerting” and “Other operational, procedural, or technical controls” do not add any value to the list of examples since they provide no real guidance.

SMUD recommends the Standards Drafting Team consider the following changes to Attachment 2, Section 3, Example 2:

“2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets the criteria specified in Section 3.1, such as:

• Anti-malware technologies; **[Delete]**

• Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)

- Monitor or alert for changes to communication baselines; [**Add]**
- Logging and alerting configuration for Security Incident and Event Management (SIEM) systems or other event correlation systems; [**Add]**

• Automated or manual log reviews; **[Delete]**

• Alerting; or **[Delete]**

• Other operational, procedural, or technical controls**. [Delete]**

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB

Answer	No
Document Name	

Comment

Attachment 2, Section 3: All the Authentication Mechanisms identified represent some form of centralized account management. Due to economies of scale, reliability, this may not represent the best option. Additionally, it precludes usage of password vault tools that may provide effective security for managing credentials. Please re-word to allow flexibility of approach based on risk and technologies.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Matthew Jaramilla, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

Salt River Project supports SMUD comments and also suggest deleting "automated or manual log reviews" and "alterting"

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Although section 3.1.2 is within the scope of the SAR, BPA still believes it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. The proposed language requires detection of known/suspected malicious communications for “inbound and outbound electronic remote access.” There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5).

BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS or the applicability be changed to bring it in-line with other requirements.

Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Tacoma Power recommends updating the Attachment 2 language based on the proposed changes to Attachment 1, Section 3.1.3 (see response to Comment 1). Tacoma Power also endorses the comments provided by SMUD.	
Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Please reference the comments in response to Question 1 above.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
NRG disagrees with the removal of the term “remote” when referencing “electronic remote access” throughout Attachment 1. Not only does this significantly expand the scope of the requirements with respect to any type of non-remote electronic access, but it also moves away from the original intent of the three recommendations initially proposed by the LICRT. NRG recommends expanding the definition of the current term “interactive remote access” to include Low Impact BES Cyber Systems and using that newly defined terminology throughout this requirement.	

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

In Attachment 2, Section 3, Example 2, there is only one bullet in the list of examples provided that meet the security objective of the SAR. That example is “Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)”.

The other bullets are not good examples for the following reasons:

“Anti malware technologies” are at the host level and is not a great control for detecting “malicious communications at the network level;” malicious code - YES, malicious communications - NO. The controls should be network based and not host based.

“Automated or manual log reviews” depending on how they are done, is not a great control. It would be best to specify what types of logs that would meet the security objective (e.g. Security Incident and Event Management logs, Netflow, Jflow etc.). Simply reviewing electronic access logs, for example, is not sufficient.

“Alerting” and “Other operational, procedural, or technical controls” do not add any value to the list of examples since they provide no real guidance.

SMUD recommends the Standards Drafting Team consider the following changes to Attachment 2, Section 3, Example 2:

“2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets the criteria specified in Section 3.1, such as:

• Anti-malware technologies; [Delete]

• Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);

- Monitor or alert for changes to communication baselines; [Add]
- Logging and alerting configuration for Security Incident and Event Management (SIEM) systems or other event correlation systems; [Add]

• Automated or manual log reviews; [Delete]

• Alerting; or [Delete]

• Other operational, procedural, or technical controls. [Delete]

Likes 2	Orlando Utilities Commission, 5, Colon Dania; American Municipal Power, 5, Ritts Amy
Dislikes 0	

Response

Kristina Marriott - Miller Bros. Solar, LLC - 5 - MRO,WECC,Texas RE	
Answer	No
Document Name	
Comment	
Language throughout that states "such as" then listing multiple bullet points should be reworded to state: "one or more of the following". The “such as” verbiage may lead auditors to mark each item as being applicable.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See EEI Comments	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	

Answer	Yes
Document Name	
Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	

Comment	
See comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the MRO NSRF for questions #2.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF requests clarification for section 3.1.3 to understand if the Responsible Entity can rely on services/support vendors for their user accounts and authentication.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Jamie Monette On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Jamie Monette	
Answer	Yes
Document Name	
Comment	

NA	
Likes 0	
Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Recommend modifying the language in Attachment 1 to align with the language in Attachment 2.	
Likes 0	
Dislikes 0	
Response	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company is in agreement with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI’s proposal for the following revisions to align with the proposal provided in response to Question 1.	

“For Section 3.1.3, documentation showing the ability to authenticate users **prior to (*remove:* when)** permitting each user-initiated instance of electronic access, where electronic access meets the criteria specified in Section 3.1, to a network(s) containing low impact BES Cyber Systems, such as…”	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Revise Section 3.1.3 based on Attachment 1 revisions recommended above.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments.	

Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
The language in CIP-003A Attachment 2 is acceptable as long as the wording for 3.1.3 and 3.1.4 are modified/updated as suggested	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Revise Section 3.1.3 based on Attachment 1 revisions recommended above.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by MRO NSRF	
Likes 0	
Dislikes 0	

Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the proposed langauge but also supports EEI's alternative language for added clarity.	
Likes 0	
Dislikes 0	
Response	
Patricia Ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

3. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-A. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.

James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
As Long as Dial-up is not in scope 3 years is agreeable. IF Dial-up is NOT removed, 3 years is not long enough.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
AZPS agrees with EEI's proposal to align the implementation plans for CIP-003 changes resulting from Project 2016-02 and Project 2023-04 to avoid separate versions and implementation plans which will require entities to make changes affecting low impact BCS under different regulatory deadlines resulting in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Until Tacoma Power's concern on the language in Attachment 1 Section 3.1.3 is resolved to include only the initial authentication, this implementation plan is not achievable. However, if these concerns are addressed, then 36 months is reasonable timeframe.	
Likes 1	American Municipal Power, 5, Ritts Amy

Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	
Comment	
As Long as Dial-up is not in scope 3 years is agreeable. IF Dial-up is NOT removed, 3 years is not long enough.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Until Questions 1 and 2 are resolved it is difficult for BPA to determine if the 3 year timeframe is appropriate.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Matthew Jaramilla, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
Salt River Project agrees and supports comments from AZPS and EEI. In addition, SRP would like to have a specific date of implementation as there is significant cost associated with this project (equipment and resources), time for planning, and work that would need to be done.	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE supports the comments as submitted by Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends that the CIP-003-A implementation plan consider the CIP-003-10 implementation plan to allow the effective use of resources.	
Likes 0	
Dislikes 0	
Response	

Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company is in agreement with EEI comments.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The NAGF recommends that the CIP-003-A implementation plan consider the CIP-003-10 implementation plan to allow the effective use of resources.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	No

Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #3.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NEE supports EEI's comments: "EEI proposes the alignment of the implementation plan for CIP-003 in Project 2016-02 with the 3-year implementation plan proposed in Project 2023-04 allowing entities to only make changes to the affected sites once. We further suggest combining the revisions to CIP-003 resulting from Project 2023-04 and 2016-02 into one version for NERC Board approval after passing ballot if they will be presented to the Board at the same meeting. Separate versions and implementation plans will require entities to make changes affecting low impact BCS under different regulatory deadlines resulting in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated."	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The undertaking will demand significant effort, substantial capital investment and additional staffing.	
Likes 0	
Dislikes 0	
Response	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	

Answer	No
Document Name	
Comment	

Comments: CEHE does not agree with the proposed implementation plan because of the pending changes in Project 2016-02. CEHE agrees with EEI's comment on the implementation plan.

EEI Comments:

EEI proposes the alignment of the implementation plan for CIP-003 in Project 2016-02 with the 3-year implementation plan proposed in Project 2023-04 allowing entities to only make changes to the affected sites once. We further suggest combining the revisions to CIP-003 resulting from Project 2023-04 and 2016-02 into one version for NERC Board approval after passing ballot if they will be presented to the Board at the same meeting. Separate versions and implementation plans will require entities to make changes affecting low impact BCS under different regulatory deadlines resulting in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated.

Likes 0	
Dislikes 0	
Response	

Robert Blackney - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	
Comment	

See comments submitted by EEI.

Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	
Comment	

Dominion Energy supports EEI comments

Likes 0	
Dislikes 0	

Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	No
Document Name	
Comment	
As a parent company to a fleet of over 25 Low Impact Generation Facilities, along with affiliates with equally sizeable fleets, 36 months will not be enough time for owners with multiple Low Impact generation facilities to onboard these controls. Recommend a provision for owners with multiple Low Impact facilities allowing up to 5 years.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
We do not agree with the proposed implementation plan. Our apprehension primarily stems from the intersection of CIP-003-A and CIP-003-9, with a particular focus on the potential financial implications in Section 6.3, where additional expenditures may be necessitated to accommodate technological changes.	
Likes 0	
Dislikes 0	

Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
SMUD agrees with a three-year implementation plan and believes it is the necessary amount of time for supply chains to support the changes registered entities will need to implement.	
Likes 0	
Dislikes 0	
Response	

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the implementation plan, but also supports EEI's recommendation to align the implementation of the LICRT CIP-003 revisions with the implementation of the CIP-003 revisions from the 2016-02 Project.	
Likes 0	
Dislikes 1	Orlando Utilities Commission, 5, Colon Dania
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by MRO NSRF	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
The 3 year implementation plan is sufficient unless there is a supply chain issue with the manufacturers of the equipment needed to implement this solution.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	

Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
OUC agrees with a three-year implementation plan and believes it is the necessary amount of time for supply chains to support the changes registered entities will need to implement.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
If concerns are addressed in Attachment 1 then a 3 year implementation time is sufficient.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Jamie Monette On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Jamie Monette	
Answer	Yes
Document Name	

Comment	
Additional time should be considered to architect and implement authentication methods.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI proposes the alignment of the implementation plan for CIP-003 in Project 2016-02 with the 3-year implementation plan proposed in Project 2023-04 allowing entities to only make changes to the affected sites once. We further suggest combining the revisions to CIP-003 resulting from Project 2023-04 and 2016-02 into one version for NERC Board approval after passing ballot if they will be presented to the Board at the same meeting. Separate versions and implementation plans will require entities to make changes affecting low impact BCS under different regulatory deadlines resulting in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated.	
Likes 1	Sempra - San Diego Gas and Electric, 5, Wright Jennifer
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See EEI Comments	
Likes 0	
Dislikes 0	
Response	
Mohamed Derbas - Sempra - San Diego Gas and Electric - 1	
Answer	Yes
Document Name	

Comment	
SDG&E supports EEI's commnets on this item.	
Likes 0	
Dislikes 0	
Response	
Kristina Marriott - Miller Bros. Solar, LLC - 5 - MRO,WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karla Weaver - Public Utility District No. 2 of Grant County, Washington - 4, Group Name GCPD Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
WECC leaves comments on the implemtation plan to the applicable entities.	

Likes 0	
Dislikes 0	
Response	

4. The DT believes the language of CIP-003-A addresses the issues outlined in the SAR in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical, or procedural justification.

Katrina Lyons - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

3.1.2 exceeds the Standards for Medium Impact and incurs substantial costs. The challenge lies in the fact these terms have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, using these same words with different examples in the measures creates ambiguity in the expectations for compliance.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	No
Document Name	

Comment

Some entities implemented electronic access controls not expecting these added controls. The added malicious communication detection(s) may require a complete redesign to properly implement this control making it costly.

Likes 0	
Dislikes 0	

Response

C. A. Campbell - LS Power Development, LLC - 5

Answer	No
Document Name	

Comment

Since there is no cost recovery mechanism for generation facilities, from a business perspective, these technical controls and compliance processes have the potential to significantly impact the cost structure of support at each site. It would be accurate to say that we have the framework in place to support these technologies, but the concern would be the human-capital required to support the recurring maintenance of such processes. Because of how Low Impact Generation Facilities are setup, the objectives outlined in the proposed controls would require effort from IT/OT support providers,

O&Ms, and OEMs. Needless to say, 36 months will not be enough time for owners with multiple Low Impact generation facilities to implement these requirements.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The undertaking will demand significant effort, substantial capital investment and additional staffing.	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	No
Document Name	
Comment	
The additional discrete requirements and expansion to all inbound and outbound electronic access is a significant incremental increase in the requirements for low-impact assets. Pending on an organization's current cybersecurity maturity level, meeting and maintaining these requirements will take significant effort and cost. It is anticipated this will require entities to hire multiple additional full-time staff to maintain and partake in lengthy contract negotiations with OEMs and other remote access vendors to ensure the additional discrete details included in the language can be met.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	

Comment	
NCPA supports comments made by SMUD and Tacoma Power.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends minimizing churn among standard versions and clearly identify the scope; Reclamation also recommends the DT take additional time to coordinate the modifications with other existing drafting teams for related standards. This will help minimize the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. Reclamation will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	

Comment	
Tri-State would need to have more details before costs could be accurately determined.	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
NIPSCO has not determined whether this will be cost effective. The procurement process for a tool(s) and resources will be initiated should the requirement language remain as is.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
For small Entities implementation of the controls outlined in the proposed standard could be financially burdensome. Entities with a large number of Low stations may have difficulty meeting the 36 months implementation timeframe.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	

For small Entities implementation of the controls outlined in the proposed standard could be financially burdensome. Entities with a large number of Low stations may have difficulty meeting the 36 months implementation timeframe.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Matthew Jaramilla, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

Salt River Project agrees and supports Tacoma's comment. In addition, SRP believes that more information required as it is difficult to determine the exact financial impact, even though we are expecting a significant cost that would need to be budgeted.

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

As Long as Dial-up is not in scope the project can be performed in a cost-effective manner. IF Dial-up is not removed, the project will not be cost-effective.

Likes 0	
Dislikes 0	

Response

Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna

Answer	No
Document Name	

Comment

It cannot be determined at this time if the SAR addresses the issues in a cost effective manner.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment

Until Tacoma Power's concern on the language in Attachment 1 Section 3.1.3 is resolved to include only the initial authentication, this is not a cost effective requirement, both in terms of upfront cost of implementing significant additional tooling, as well as ongoing stakeholder time to update and perform work practices in a compliant manner.

Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

Irrespective of cost effectiveness, NRG does not believe that the proposed changes address the original issues outlined in the SAR. Please reference comments in response to Question 1 above for additional detail.

Likes 0	
Dislikes 0	

Response

James Keele - Entergy - 3

Answer	No
Document Name	

Comment	
As Long as Dial-up is not in scope the project can be performed in a cost-effective manner. IF Dial-up is not removed, the project will not be cost-effective.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
Irrespective of cost effectiveness, NRG does not believe that the proposed changes address the original issues outlined in the SAR. Please reference comments in response to Question 1 above for additional detail.	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
SMUD views the changes as neither cost effective nor cost ineffective.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See EEI Comments	
Likes 0	

Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by MRO NSRF	
Likes 0	
Dislikes 0	
Response	
Patricia Ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karla Weaver - Public Utility District No. 2 of Grant County, Washington - 4, Group Name GCPD Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kristina Marriott - Miller Bros. Solar, LLC - 5 - MRO,WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	
Document Name	
Comment	
ITC does not respond to cost questions	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	

NST lacks the information necessary to comment on this question.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	
Document Name	

Comment

NEE does not comment on costs.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Jamie Monette On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Jamie Monette

Answer	
Document Name	

Comment

NA

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 3

Answer	
Document Name	

Comment

Ameren has no comment on the cost effectiveness of the project.

Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost-effectiveness.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
WECC leaves comments on the cost-effectiveness to the applicable entities.	
Likes 0	
Dislikes 0	
Response	

5. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	
Document Name	

Comment

In the revised Technical Rationale document on page 7, the paragraph directly above Figure 4 references “Figure 4” but is actually referencing Figure 5. If confirmed and appropriate, the paragraph should be moved below Figure 4 and the text changed to say:

“***Figure 5*** depicts an example of protected authentication at a central intermediate system before accessing a network containing a LIBCS. This protection mitigates the unintended disclosure of authentication information for remote access of LIBCS.”

Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	
Document Name	

Comment

Duke Energy supports EEI's comments and thanks the Drafting Team for their work.

Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	
Document Name	

Comment

Alliant Energy supports comments submitted by MRO NSRF

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	
Document Name	
Comment	
As Long as Dial-up is not in scope the new requirements for CIP-003-A can be implemented.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	
Document Name	
Comment	
Tacoma Power supports SMUD’s comments on the technical rationale changes.	
Likes 1	American Municipal Power, 5, Ritts Amy

Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	
Document Name	2023-04 Unofficial Comment Form Additional Ballot_NSRF FINAL_20240306.docx
Comment	
The High VSL column for R2 regarding electronic access (Section 3) contains a typo at the end of the second paragraph. “Section 2” should read “Section 3”.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	
Document Name	
Comment	
As Long as Dial-up is not in scope the new requirements for CIP-003-A can be implemented.	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE recommends revising Requirement Part 3.1 from “shall implement a control(s) that” to “shall implement one or more controls that.”	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Matthew Jaramilla, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	

Answer	
Document Name	
Comment	

Salt River Project still has concerns on how CIP-003 is written for low impact requirements to contain parts of all existing standards (for medium and high impact). Seems like there is an opportunity to just add low impact requirements to the existing standard(s). This will also help in keeping language consistent.

Likes 0	
Dislikes 0	
Response	

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	
Document Name	
Comment	

BC Hydro appreciates the drafting team's efforts and the opportunity to comment, and offers the following suggestion.

BC Hydro suggests included in the Technical Rationale more pertinent use cases and examples to clarify the language used in the revised standards. Specifically the use of 'operational, procedural or technical' methods mentioned in the revised CIP-003 standard Attachment 2 Section 3.5 and 3.6.

Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB

Answer	
Document Name	
Comment	

TVA does not agree with the inappropriate scaling of Medium and High controls to BCAs at Low assets. If additional requirement are scaled to Low BCAs, TVA recommends NERC identify Low BCS in the applicability of the CIP-004 - CIP-013 requirements instead of extending CIP-003 R2 to apply the same requirements to Lows.

Likes 0	
Dislikes 0	
Response	

Dania Colon - Orlando Utilities Commission - 5	
Answer	
Document Name	
Comment	

TVA does not agree with the inappropriate scaling of Medium and High controls to BCAs at Low assets. If additional requirements are scaled to Low BCAs, TVA recommends NERC identify Low BCS in the applicability of the CIP-004 - CIP-013 requirements instead of extending CIP-003 R2 to apply the same requirements to Lows.

Likes 0	
Dislikes 0	
Response	

TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	
Document Name	
Comment	

SIGE appreciates the work of the drafting team to address previous feedback provided for CIP-003-A Technical Rationale. SIGE suggests the following changes in order to qualify the type of access that is being addressed by this standard. The use of the verbiage “user-initiated instance of electronic access” could easily be interpreted as any user log-in. The act of a user logging into a local HMI at a substation is technically a “user-initiated instance of electronic access “. The suggested changes are intended to mimic the Interactive Remote Access term as defined in the NERC Glossary of terms, while not making any reference to an ESP.

Section 3.1.3

This is a new cyber security control outlined in the SAR, which requires entities to implement controls to authenticate users when permitting (allowing) each instance of **user-initiated instance of** electronic remote access, **not including system-to-system process communications,** to networks containing low impact BES Cyber Systems. The intent is at the time any access to the “network containing low impact BES Cyber Systems” is being permitted, the remote user is already authenticated. Figure 3 below depicts a situation where the authentication of the remote user is occurring after the user already has access to the “network containing LIBCS” as the authentication servers are on the same network with the LIBCS. The firewall in this scenario allows the user through to the network on which the LIBCS reside before the user is authenticated.

The intention of “each instance” phrase is meant to include the initial authorization and all subsequent re-connection instances of **user-initiated instance of electronic remote access, not including system-to-system process communications,** to the network. If there is a collection of sub-networks or Cyber Assets within the network containing LIBCS, then multiple re-authentications at those levels would not be required. This control mitigates the risk of unauthenticated user access to networks on which LIBCS reside.

Section 3.1.4 contains an incorrect reference to Figure 4. The correct reference should be Figure 5.

Section 3.1.4

This is a new cyber security control outlined in the SAR. The objective of Attachment 1, Section 3.1.4 is for entities to protect the user authentication information (e.g., username, password, multi-factor authentication (MFA) information, session token, etc.) while in transit between the remote user's Cyber Asset and either the asset containing the LIBCS or the entity's authentication system used to meet Section 3.1.3. The intent is not to specify authentication directly to a particular device, but to allow for entities that desire to use an existing compliant CIP-005 Requirement R2 Intermediate System or similar architecture for access to networks containing LIBCS as well. For example, Figure 4 below depicts authentication at the boundary of the asset containing a LIBCS. In this example, the authentication server and jump host are on a different network than the "network containing LIBCS", making it uniquely different from Figure 3 above.

Figure 5 depicts an example of protected authentication at a central intermediate system before accessing a network containing a LIBCS. This protection mitigates the unintended disclosure of authentication information for remote access of LIBCS.

Section 3.1.5

The objective of Section 3.1.5 is to maintain the original language used in CIP-003-9, Section 6.1, as much as possible. One or more method(s) can be identified as part of this electronic access control. Entities must determine **user-initiated instances of vendor electronic remote access, not including system-to-system process communications**, where permitted, to their low impact BES Asset(s) and/or LIBCS. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular **user-initiated instance of vendor electronic remote access, not including system-to-system process**.

Section 3.1.6

The objective of Section 3.1.6 is to maintain the original language used in CIP-003-9, Section 6.2, as much as possible. One or more method(s) can be identified as part of this electronic access control. Entities must have the ability to disable **user-initiated instances of vendor electronic remote access, not including system-to-system process communications**, where permitted, for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing LIBCS.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer	
Document Name	

Comment

Black Hills Corporation agrees with EEI's comments which request clarification around VPN tunnels and 3rd party authentication. (EEI comments included below)

EEI proposes clarification in the Technical Rationale regarding the use of VPN tunnels as a permanent connection between OEMS and/or continuous monitoring vendors who use an HMI to remotely connect to an entity SCADA system to remotely maintain in-scope sites in the context of compliance with Attachment 1, R3, Part 3.1.3.

As an example, wind farms can be maintained remotely by the OEM and/or have a continuous monitoring vendor (third-party) using HMIs remotely connected to the SCADA system via VPN tunnel. The VPN tunnel is typically established between a switch or firewall at the wind farm and a similar

device at the third-party location. An HMI is set up at the third-party location. VPN tunnels are generally configured to connect automatically using pre-established authentication mechanisms. Once a VPN tunnel is formed it is a connection between the OEM and/or continuous monitoring vendor and the SCADA system for the vendor to manage the turbines.

In this scenario, discussion in the Technical Rationale about an entity's ability to comply with Attachment 1, R3, Part 3.1.3. would be beneficial because third-party authentication would take place at the HMI and/or SCADA system devices, and the entity would not be in control of each user-initiated instance of electronic access because they occur on the third-party vendor's side of the VPN tunnel.

Clarification could include discussion of this scenario in the context of Interactive Remote Access (IRA), and/or what is meant by "user-initiated instance of access to a network containing."

EEI believes this change to the Technical Rationale document could be made without a substantive change requiring another ballot.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	
Document Name	

Comment

NA

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	
Document Name	

Comment

Reclamation recommends when adjusting CIP-003 that changes first be made to Medium and High impact standards. CIP-003 should mirror higher impact requirements but at an equal to or less restrictive level.

Likes 0	
Dislikes 0	

Response

Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
Southern Company is in agreement with EEI comments.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	
Provide guidance on how a system similar to an Intermediate System could be used to meet 3.1.3 and 3.1.4. Technical guidance diagrams. The information in figure 4 should be included in the diagram for figure 1 and figure 2. Figure 4 provides confusion because it does not meet the criteria listed in 3.1.1 and 3.1.2. Figure 5 is not referenced in any of the guidance and is unclear if there is user authentication information between the jump host and the BES Cyber System. Several projects were/are modifying CIP-003 in parallel (2016-02, 2020-03 and 2023-04) and a different approach is used in dealing with the previous Technical Rationale content. For example, in Project 2023-04, hyperlinks to the previous TRs are added in the document, whereas in 2016-02, information from the previous TRs is kept and information was added related to the 2016-02 changes. Furthermore, the recently approved CIP-003-9 TR filed with the 2020-03 project contained only 8 pages from the initial 32 pages. These 8 pages consisted only the changes regarding the -9 version. In summary, three different projects modifying the CIP-003 and its TR with three different approaches. As a general comment, it would be helpful to the	

industry for the NERC SDTs to choose a way going forward that is applied across all NERC projects. In the case of the TR in this project, we suggest keeping one TR that includes the previous versions of the TR, as was done in the 2016-02 project.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Jamie Monette On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Jamie Monette	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	
Document Name	
Comment	
Jump Server comment. Technical guidance diagrams.	

Within the Technical Guidance diagrams there is a concern on Figure 3 and Figure 4 concerning if both diagrams are approved configurations or if figure 3 is an incorrect configuration and Figure 4 is an appropriate configuration. Additionally, in Figure 4 there needs to be a key for the line colors and a DMZ designation.

Several projects were/are modifying CIP-003 in parallel (2016-02, 2020-03 and 2023-04) and a different approach is used in dealing with the previous Technical Rationale content. For example, in Project 2023-04, hyperlinks to the previous TRs are added in the document, whereas in 2016-02, information from the previous TRs is kept and information was added related to the 2016-02 changes. Furthermore, the recently approved CIP-003-9 TR filed with the 2020-03 project contained only 8 pages from the initial 32 pages. These 8 pages consisted only the changes regarding the -9 version. In summary, three different projects modifying the CIP-003 and its TR with three different approaches. As a general comment, it would be helpful to the industry for the NERC SDTs to choose a way going forward that is applied across all NERC projects. In the case of the TR in this project, we suggest keeping one TR that includes the previous versions of the TR, as was done in the 2016-02 project.

We note that according to the proposed texts and considering the current version of CIP-005 for Medium Impact Systems, the level of security required for remote access of Low Impact systems is higher than for that of Medium Impact systems without Control Center. We assume that the future revision of CIP-005 will correct this apparent inconsistency.ma

Likes 0	
Dislikes 0	

Response

Ben Hammer - Western Area Power Administration - 1

Answer	
Document Name	

Comment

The High VSL column for R2 regarding electronic access (Section 3) contains a typo at the end of the second paragraph. “Section 2” should read “Section 3”.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster

Answer	
Document Name	

Comment

Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the MRO NSRF for questions #5.

Likes 0	
Dislikes 0	

Response

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	

Comment

EEI proposes clarification in the Technical Rationale regarding the use of VPN tunnels as a permanent connection between OEMS and/or continuous monitoring vendors who use an HMI to remotely connect to an entity SCADA system to remotely maintain in-scope sites in the context of compliance with Attachment 1, R3, Part 3.1.3.

As an example, wind farms can be maintained remotely by the OEM and/or have a continuous monitoring vendor (third-party) using HMIs remotely connected to the SCADA system via VPN tunnel. The VPN tunnel is typically established between a switch or firewall at the wind farm and a similar device at the third-party location. An HMI is set up at the third-party location. VPN tunnels are generally configured to connect automatically using pre-established authentication mechanisms. Once a VPN tunnel is formed it is a connection between the OEM and/or continuous monitoring vendor and the SCADA system for the vendor to manage the turbines.

In this scenario, discussion in the Technical Rationale about an entity's ability to comply with Attachment 1, R3, Part 3.1.3. would be beneficial because third-party authentication would take place at the HMI and/or SCADA system devices, and the entity would not be in control of each user-initiated instance of electronic access because they occur on the third-party vendor's side of the VPN tunnel.

Clarification could include discussion of this scenario in the context of Interactive Remote Access (IRA), and/or what is meant by "user-initiated instance of access to a network containing."

EEI believes this change to the Technical Rationale document could be made without a substantive change requiring another ballot.

Likes 1	Sempra - San Diego Gas and Electric, 5, Wright Jennifer
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	
Document Name	

Comment

We operate within a geographical region characterized by limited access of local academic enrichment opportunities for young professionals in cybersecurity. Moreover, this project will require significant technical effort, substantial capital investment, and the augmentation of staffing resources.

Likes 0	

Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	
Document Name	
Comment	
Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
(None)	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	

C. A. Campbell - LS Power Development, LLC - 5	
Answer	
Document Name	
Comment	
LS Power Development agrees with comments submitted by EEL. Thank you for the opportunity to comment.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	
Jump Server comment. Technical guidance diagrams. Within the Technical Guidance diagrams there is a concern on Figure 3 and Figure 4 concerning if both diagrams are approved configurations or if figure 3 is an incorrect configuration and Figure 4 is an appropriate configuration. Additionally, in Figure 4 there needs to be a key for the line colors and a DMZ designation. Several projects were/are modifying CIP-003 in parallel (2016-02, 2020-03 and 2023-04) and a different approach is used in dealing with the previous Technical Rationale content. For example, in Project 2023-04, hyperlinks to the previous TRs are added in the document, whereas in 2016-02, information from the previous TRs is kept and information was added related to the 2016-02 changes. Furthermore, the recently approved CIP-003-9 TR filed with the 2020-03 project contained only 8 pages from the initial 32 pages. These 8 pages consisted only the changes regarding the -9 version. In summary, three different projects modifying the CIP-003 and its TR with three different approaches. As a general comment, it would be helpful to the industry for the NERC SDTs to choose a way going forward that is applied across all NERC projects. In the case of the TR in this project, we suggest keeping one TR that includes the previous versions of the TR, as was done in the 2016-02 project.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	
Document Name	

Comment	
We would like to thank the SDT for their hard work and dedication to this project.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	
Document Name	
Comment	

ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
See EEI Comments	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
In general, it seems that the SDT has expanded the requirements beyond what was recommended by the LICRT. For example, the LICRT stated there should be a requirement for the "detection of malicious communications to/between assets containing low-impact BES Cyber Systems with ERC." This language allows greater flexibility in determining the location of detection compared to the SDT's specification of "for both inbound and outbound	

electronic access." Given that access is defined by communication "outside the asset containing low-impact BES Cyber System(s)," this language inherently mandates the detection to occur at the border of the low-impact asset.	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Mohamed Derbas - Sempra - San Diego Gas and Electric - 1	
Answer	
Document Name	
Comment	
SDG&E supports EEI's commnets.	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2023-04 Modifications to CIP-003 | Draft 2
Comment Period Start Date:	1/30/2024
Comment Period End Date:	3/14/2024
Associated Ballot(s):	2023-04 Modifications to CIP-003 CIP-003-A AB 2 ST 2023-04 Modifications to CIP-003 Implementation Plan AB 2 OT

There were 71 sets of responses, including comments from approximately 169 different people from approximately 111 companies representing 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, contact Director, Standards Development Latrice Harkness (via email) or at (404) 858-8088.

Questions

1. Do you agree with the language proposed in CIP-003-A Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

2. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

3. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-A. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.

4. The DT believes the language of CIP-003-A addresses the issues outlined in the SAR in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical, or procedural justification.

5. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Husam Al-Hadidi	Manitoba Hydro (System Performance)	1,3,5,6	MRO

Kimberly Bentley	Western Area Power Administration	1,6	MRO
Jaimin Patal	Saskatchewan Power Corporation (SPC)	1	MRO
George Brown	Pattern Operators LP	5	MRO
Larry Heckert	Alliant Energy (ALTE)	4	MRO
Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
Dane Rogers	Oklahoma Gas and Electric (OG&E)	1,3,5,6	MRO
Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
Michael Ayotte	ITC Holdings	1	MRO
Andrew Coffelt	Board of Public Utilities-Kansas (BPU)	1,3,5,6	MRO
Peter Brown	Invenergy	5,6	MRO

					Angela Wheat	Southwestern Power Administration	1	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC
					Nehtisha Rollis	Tennessee Valley Authority	5	SERC
Manitoba Hydro	Jay Sethi	1,3,5,6	MRO	Manitoba Hydro Group	Nazra Gladu	Manitoba Hydro	1	MRO
					Mike Smith	Manitoba Hydro	3	MRO
					Kristy-Lee Young	Manitoba Hydro	5	MRO
					Kelly Bertholet	Manitoba Hydro	6	MRO
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC

					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
Southern Company - Southern Company Services, Inc.	Jennifer Tidwell	1,3,5,6	SERC	Southern Company	Leslie Burke	Southern Company - Southern Company Generation	5	SERC
					Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Ron Carlsen	Southern Company - Southern	6	SERC

						Company Generation		
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Nick Fogleman	Prairie Power, Inc.	1,3	SERC
					Cooper Cash	North Carolina Electric Membership Corporation	3,4,5	SERC
Public Utility District No. 2 of Grant County, Washington	Karla Weaver	4		GCPD Group	Karla Weaver	Grant County PUD	4	WECC
					Nikkee Hebdon	Public Utility District No. 2 of Grant County, Washington	5	WECC
					Joanne Anderson	Public Utility District No. 2 of Grant	1	WECC

						County, Washington		
					Mike Stussy	Public Utility District No. 2 of Grant County, Washington	6	WECC
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
Black Hills Corporation	Rachel Schuldt	6		Black Hills Corporation - All Segments	Micah Runner	Black Hills Corporation	1	WECC
					Josh Combs	Black Hills Corporation	3	WECC
					Rachel Schuldt	Black Hills Corporation	6	WECC

					Carly Miller	Black Hills Corporation	5	WECC
					Sheila Suurmeier	Black Hills Corporation	5	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Alain Mukama	Hydro One Networks, Inc.	1	NPCC
					Deidre Altobell	Con Edison	1	NPCC
					Jeffrey Streifling	NB Power Corporation	1	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
					Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
					Randy Buswell	Vermont Electric Power Company	1	NPCC
					James Grant	NYISO	2	NPCC

John Pearson	ISO New England, Inc.	2	NPCC
Harishkumar Subramani Vijay Kumar	Independent Electricity System Operator	2	NPCC
Randy MacDonald	New Brunswick Power Corporation	2	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
David Burke	Orange and Rockland	3	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC

David Kwan	Ontario Power Generation	4	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
Glen Smith	Entergy Services	4	NPCC
Sean Cavote	PSEG	4	NPCC
Jason Chandler	Con Edison	5	NPCC
Tracy MacNicoll	Utility Services	5	NPCC
Shivaz Chopra	New York Power Authority	6	NPCC
Vijay Puran	New York State Department of Public Service	6	NPCC
ALAN ADAMSON	New York State Reliability Council	10	NPCC
David Kiguel	Independent	7	NPCC
Joel Charlebois	AESI	7	NPCC

					Joshua London	Eversource Energy	1	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC

					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
Santee Cooper	Vicky Budreau	3		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC

1. Do you agree with the language proposed in CIP-003-A Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	

SMUD does not agree with the wording of Attachment 1, Section 3.1.3 which states:

"Authenticate users when permitting **each user-initiated instance** of electronic access to a network(s) containing low impact BES Cyber Systems;"

It is not feasible to authenticate each user-initiated instance of electronic access since doing so limits the technical solutions for implementing such a control. For example – if a registered entity were to implement a jump host solution, a user may be able to authenticate to the jump host and be permitted to access the low impact BES Cyber System based on successfully authenticating to the jump host. If the user established multiple connections from the jump host into multiple low impact BES Cyber Systems at different low impact assets, the proposed language may be interpreted as requiring additional authentication for each connection to other low impact BES Cyber Systems.

Section 3.1.3 as currently written is stricter than the high or medium impact Interactive Remote Access (IRA) requirements where “each user-initiated instance” of IRA ***DOES NOT*** require additional authentication for each connection. SMUD recommends the Standards Drafting Team change the language in Section 3.1.3 to read: “3.1.3 Authenticate users prior to permitting user-initiated electronic access to a network(s) containing low impact BES Cyber Systems;” This suggested wording aligns better with the SAR, whereas the existing wording does not indicate that users must be authenticated ***before*** access is granted to networks containing low impact BES Cyber Systems. The way in which Section 3.1.3 is currently written, it is as if the connection requires the authentication rather than the user being authenticated. SMUD also recommends the Standards Drafting Team make the following conforming changes to the language in Section 3.1.4 to read: “3.1.4 Protect user authentication information for user-initiated electronic access while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and • the authentication system used to meet Section 3.1.3, or • the asset containing low impact BES Cyber System(s);”	
Likes 2	Orlando Utilities Commission, 5, Colon Dania; American Municipal Power, 5, Ritts Amy
Dislikes 0	
Response	
Thank you for your comments. The drafting team (DT) made changes in Part 3.1.3 to address these comments. For Part 3.1.4, conforming changes were made to support the changes made in Part 3.1.3.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	

NRG disagrees with the removal of the term "remote" when referencing "electronic remote access" throughout Attachment 1. Not only does this significantly expand the scope of the requirements with respect to any type of non-remote electronic access, but it also moves away from the original intent of the three recommendations initially proposed by the LICRT. NRG recommends expanding the definition of the current term "interactive remote access" to include Low Impact BES Cyber Systems and using that newly defined terminology throughout this requirement.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for your comment. The DT made changes to clarify what is meant by "remote" without including that language. Please see the changes before Section 3.1.1. An explanation on the purpose for removing "remote" has also been add to the TR.	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
Section 3.2 states the Responsible Entity shall implement a control(s) that authenticates all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability. Section 3.2 should be removed, and Dial-up connectivity should be excluded from CIP-003-A regulations for LOW impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT made no material modifications to Section 3.2, this part of the standard has been in effective since it was passed with the Version 5 project.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
NRG disagrees with the removal of the term “remote” when referencing “electronic remote access” throughout Attachment 1. Not only does this significantly expand the scope of the requirements with respect to any type of non-remote electronic access, but it also moves away from the original intent of the three recommendations initially proposed by the LICRT. NRG recommends expanding the definition of the current term “interactive remote access” to include Low Impact BES Cyber Systems and using that newly defined terminology throughout this requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT made changes to clarify what is meant by “remote” without including that language. Please see the changes before Section 3.1.1. An explanation on the purpose for removing “remote” has also been add to the TR.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
It appears that the Attachment 1 Section 3, Part 3.1.3 language is not restricted to the initial user authentication to a central management system that controls the access to multiple low impact BCS, as was intended by the SDT. Additionally, the lead-in statement in Section 3.1	

(and i-iii) defines what type of access to control, and it appears that the access described in the current Section 3.1.3 would not be in-scope of the electronic access defined in Section 3.1, and therefore would not create a required control. This is due to Section 3.1 (i) defining access as "between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing…", not "between a network containing a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing…".

Tacoma Power suggests the following language for Section 3.1.3:

"Authenticate user-initiated electronic access to a network(s) containing low impact BES Cyber Systems prior to establishing access applicable to Section 3.1;"

Note this change may be better as a new section in Attachment 1, for example, Section 3.3.

The above change would also lead to conforming changes in Section 3.1.4, as follows:

"Protect user authentication information for user-initiated electronic access while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and:

• the authentication system used to meet Section 3.1.3, or

• the asset containing low impact BES Cyber System(s);"

Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	

Response

Thank you for your comments. The drafting team (DT) made changes in Part 3.1.3 to address these comments. For Part 3.1.4, conforming changes were made to support the changes made in Part 3.1.3.

Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna

Answer	No
Document Name	

Comment

The wording in 3.1.3 as written could be read as requiring authentication each time a user accesses a network containing a Low Impact BES Cyber System, which would be stricter than the allowed jump host for medium and high impact requirements. Possible suggested wording to 3.1.3 are as follows:

"Authenticate users prior to user-initiated electronic access to a network(s) containing low impact BES Cyber Systems."

Or

"Authenticate users prior to user-initiated electronic access to a network(s) containing low impact BES Cyber Systems (multiple re-authentications are not required when accessing multiple sub networks within a larger network)"

The wording for 3.1.4 should be updated as well to match the suggested wording in 3.1.3:

"Protect authenticated information for user-initiated electronic access while in transit between …."

Likes 0	
Dislikes 0	

Response

Thank you for your comments, the DT made clarifying changes to 3.1.3 to address this comment that multiple re-authentications are not required.

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

Section 3.2 states the Responsible Entity shall implement a control(s) that authenticates all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 3.2 should be removed, and Dial-up connectivity should be excluded from CIP-003-A regulations for LOW impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, the DT made no material modifications to Section 3.2, this part of the standard has been in effective since it was passed with the Version 5 project.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Although section 3.1.2 is within the scope of the SAR, BPA still believes it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. The proposed language requires detection of known/suspected malicious communications for "inbound and outbound electronic remote access." There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5). BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS or the applicability be changed to bring it in-line with other requirements.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for your comments, the DT has responded to the requirements of the SAR which was based on the results of the Low Impact Criteria Review Team paper.	

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Matthew Jaramilla, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
Salt River Project agrees and supports comments from SMUD and Tacoma Power.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see the response to SMUD.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
Requirement 3.1.4 is not clear regarding what protection of the user authentication information is required. Please work to consolidate 3.1.3 and 3.1.4. The objectives are unclear. While substantial clarity was provided in the explanatory Webex, the proposed language lacks that clarity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, The DT made clarifying changes to 3.1.3 and 3.1.4 to address comments. What needs to be protected will depend on architecture and technology implemented by each Responsible Entity. The DT does not intend to prescribe what needs to be	

protected in the standard. The Technical Rationale for part 3.1.4 included some examples of what should be protected "…protect the user authentication information (e.g. username, password, MFA information, session token, etc)"	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	

SMUD does not agree with the wording of Attachment 1, Section 3.1.3 which states:

"Authenticate users when permitting **each user-initiated instance** of electronic access to a network(s) containing low impact BES Cyber Systems;"

It is not feasible to authenticate each user-initiated instance of electronic access since doing so limits the technical solutions for implementing such a control. For example – if a registered entity were to implement a jump host solution, a user may be able to authenticate to the jump host and be permitted to access the low impact BES Cyber System based on successfully authenticating to the jump host. If the user established multiple connections from the jump host into multiple low impact BES Cyber Systems at different low impact assets, the proposed language may be interpreted as requiring additional authentication for each connection to other low impact BES Cyber Systems.

Section 3.1.3 as currently written is stricter than the high or medium impact Interactive Remote Access (IRA) requirements where "each user-initiated instance" of IRA ***DOES NOT*** require additional authentication for each connection.

SMUD recommends the Standards Drafting Team change the language in Section 3.1.3 to read:

"3.1.3 Authenticate users prior to permitting user-initiated electronic access to a network(s) containing low impact BES Cyber Systems;"

This suggested wording aligns better with the SAR, whereas the existing wording does not indicate that users must be authenticated ***before*** access is granted to networks containing low impact BES Cyber Systems. The way in which Section 3.1.3 is currently written, it is as if the connection requires the authentication rather than the user being authenticated.

SMUD also recommends the Standards Drafting Team make the following conforming changes to the language in Section 3.1.4 to read:

"3.1.4 Protect user authentication information for user-initiated electronic access while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and • the authentication system used to meet Section 3.1.3, or • the asset containing low impact BES Cyber System(s);"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT made clarifying changes for Attachment 1, Part 3.1.3 to address these changes. For Part 3.1.4, conforming changes were made to support the changes made in Part 3.1.3. Please see the Technical Rationale for more information.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
Southern Indiana Gas and Electric (SIGE) appreciate the work of the drafting team to address previous feedback provided for CIP-003-A Attachment 1. SIGE suggests the following changes in bold in order to qualify the type of access that is being addressed by this standard. The use of the verbiage "user-initiated instance of electronic access" could easily be interpreted as any user log-in. The act of a user logging into a local HMI at a substation is technically a "user-initiated instance of electronic access ." The suggested changes are intended to mimic the Interactive Remote Access term as defined in the NERC Glossary of terms, while not making any reference to an ESP. 3.1.3 Authenticate users when permitting each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, to a network(s) containing low impact BES Cyber Systems; 3.1.4 Protect user authentication information for each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and	

• the authentication system used to meet Section 3.1.3, or • the asset containing low impact BES Cyber System(s); 3.1.5 Include one or more method(s) for determining vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted; and 3.1.6 Include one or more method(s) for disabling vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The drafting team (DT) made changes in Part 3.1.3 to address these comments. For Part 3.1.4, conforming changes were made to support the changes made in Part 3.1.3. These changes were made to clarify that 3.1.3 and 3.1.4 only apply to user based electronic access. The DT has chosen not to implement these changes as 3.1.5 and 3.1.6 are intended to capture both user based and system to system electronic access. This terminology was taken from the currently approved version of CIP-003-9 Attachment 1 section 6, and as there have been no material changes made to this requirement language, this DT is interested in preserving the associated language.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State agrees with SMUD's comments below: SMUD does not agree with the wording of Attachment 1, Section 3.1.3 which states:	

"Authenticate users when permitting **each user-initiated instance** of electronic access to a network(s) containing low impact BES Cyber Systems;" It is not feasible to authenticate each user-initiated instance of electronic access since doing so limits the technical solutions for implementing such a control. For example – if a registered entity were to implement a jump host solution, a user may be able to authenticate to the jump host and be permitted to access the low impact BES Cyber System based on successfully authenticating to the jump host. If the user established multiple connections from the jump host into multiple low impact BES Cyber Systems at different low impact assets, the proposed language may be interpreted as requiring additional authentication for each connection to other low impact BES Cyber Systems. Section 3.1.3 as currently written is stricter than the high or medium impact Interactive Remote Access (IRA) requirements where "each user-initiated instance" of IRA ***DOES NOT*** require additional authentication for each connection. SMUD recommends the Standards Drafting Team change the language in Section 3.1.3 to read: "3.1.3 Authenticate users prior to permitting user-initiated electronic access to a network(s) containing low impact BES Cyber Systems;" This suggested wording aligns better with the SAR, whereas the existing wording does not indicate that users must be authenticated ***before*** access is granted to networks containing low impact BES Cyber Systems. The way in which Section 3.1.3 is currently written, it is as if the connection requires the authentication rather than the user being authenticated. SMUD also recommends the Standards Drafting Team make the following conforming changes to the language in Section 3.1.4 to read: "3.1.4 Protect user authentication information for user-initiated electronic access while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and • the authentication system used to meet Section 3.1.3, or • the asset containing low impact BES Cyber System(s);"

Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The SDT made clarifying changes for Attachment 1, Part 3.1.3 to address these changes. For Part 3.1.4, conforming changes were made to support the changes made in Part 3.1.3. Please see the Technical Rationale for more information.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends aligning language with CIP-005-7 language or first focusing on modifying CIP-005-7 language prior to adjusting language for CIP-003-A.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has attempted to clarify the language to model CIP-005 as much as possible, however many NERC defined terms and other requirements in CIP-005 are not applicable to CIP-003 and Low Impact Systems, thus complete alignment is not possible.	
Carver Powers - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
The verbiage scoping required controls to the identified communication paths is eliminated in the proposed drafted language. Recommend clearly scoping the controls from 3.1.1 through 3.1.6 to the communications identified in 3.1 i-iii. Without this clarification: 1. There is no determination of the boundary for inbound and outbound in 3.1.1 and 3.1.2 2. 3.1.3 would require authentication for all user logins, including local logins.	

3. 3.1.5 and 3.1.6 would apply to vendors using TCAs. The information in Attachment 2 states "electronic access meets the criteria specified in Section 3.1" for 3.1.1 through 3.1.6, this language should be included in Attachment 1. The phrase “User initiated instance electronic access” should align more closely with the first sentence of the Interactive Remote Access definition to provide consistency and clarity. Without this clarity the language could include system to system communications. Recommending using a more consolidated term than “inbound and outbound electronic access”. If meaning bi-directional, then the standard should state that versus drawing a distinction between inbound and outbound.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT made some clarifying changes to the end of Section 3.1 to explicitly state its subparts 3.1.1 - 3.1.6 are only scoped for electronic access that meets the three romanettes embedded in Section 3.1. Since these subparts only apply to electronic access as described in romanette (i), the examples provided in your comment about local logins and TCA usage would not be in scope, so long as these connections are not traversing the asset boundary. The DT made changes to subparts 3.1.3 and 3.1.4 to clarify these subparts only apply to user-based electronic access. After a thorough review, the DT has decided that consolidating “inbound and outbound electronic access” to the term "bi-directional" could produce additional confusion due to instances that may arise where inbound and outbound electric access is not bi-directional. Therefore the DT has decided not to make any changes.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

Santee Cooper does not agree with the wording of Attachment 1, Section 3.1.3 which states: "Authenticate users when permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems;"

It would be difficult to authenticate each user-initiated instance of electronic access. For example, if a user established multiple connections from the jump host into multiple low impact assets, the proposed language may be interpreted as requiring additional authentication for each connection to other low impact assets. This would make the CIP-003 Attachment 1, Section 3.1.3 requirement stricter than the high or medium impact Interactive Remote Access (IRA) requirement that doesn't require additional authentication for each connection.

In addition, the existing wording does not indicate that users must be authenticated before access is granted to a network(s) containing low impact assets. The way 3.1.3 is currently written, it is as if the connection requires the authentication rather than the user being authenticated.

Likes 0	
Dislikes 0	

Response

Thank you for your comments, the DT made clarifying changes to 3.1.3 to address this comment that multiple re-authentications are not required.

Alain Mukama - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

For both sub-requirements 3.1.5 and 3.1.6 in Attachment 1, clarification is required on whether it includes both Interactive Remote Access and system-to-system remote access.

Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The DT didn't make material changes to 3.1.5 and 3.1.6. The previous DT stated that both interactive access and system to system was included.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
MRO interprets the draft Requirement language in Section 3.1.3 such that authentication is required each time a user initiates electronic access to any network(s) containing low impact BCSs. This interpretation of the language does not support the single authentication asserted by the SDT during the Project 2023-04 Webinar, relating to the jumphost in Figure 5 in the Technical Rationale. MRO recommends the Requirement language in Section 3.1.3 be changed to support the SDT's assertions. Any changes to the Requirement language needs to ensure that any electronic access directly from a network containing low impact BES Cyber Asset to a different network(s) containing low impact BES Cyber Systems, when not using a centralized electronic access system (e.g. jumphost), still requires authentication. Recommended language change: **Authenticate users prior to permitting user-initiated instances of electronic access to a network(s) containing low impact BES Cyber Systems**	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT made clarifying changes to 3.1.3 to address this comment that multiple re-authentications are not required.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	No
Document Name	

Comment
Attachment 1 appears to have exceeded the CIP-003 R2 (documented cybersecurity plan) due to the amount of technical controls that have now been added. Recommendation: if the SDT intends to keep expanding controls beyond the documented plans they should consider creating a new requirement. Why is this phrase used “User initiated instance electronic access”. Recommending using a more consolidated term than “inbound and outbound electronic access”. If meaning bi-directional, then the standard should state that versus drawing a distinction between inbound and outbound. Sub requirement 3.15, request clarification on whether the sub requirement applies to both system to system and user-initiated access by a vendor.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The purpose of Attachment 1 is to define any technical requirements for Low Impact BES. Hence DT team updated the attachment for consistency. The need for a new requirement can be discussed with NERC but that is not in-scope for this team. The DT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums. Additionally, the DT asserts that this is beyond the scope of the SAR. After a thorough review, the DT has decided that consolidating “inbound and outbound electronic access” to the term "bi-directional" could produce additional confusion due to instances that may arise where inbound and outbound electric access is not bi-directional. Therefore the DT has decided not to make any changes.

The DT didn't make material changes to 3.1.5 and 3.1.6. The previous DT stated that both interactive access and system to system was included.
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment
NCPA supports comments made by SMUD and Tacoma Power.

Likes 0	
Dislikes 0	

Response
Thank you for your comments, please see response to SMUD.
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment
EEI appreciates the work of the drafting team to address previous feedback provided for CIP-003-A Attachment 1, but proposes the following modifications to Section 3, Part 3.1.3: "Authenticate users **prior to** permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems **(multiple re-authentications to sub-networks within a larger network are not required)**;"

We also suggest including clear language in the implementation guidance describing the change from use of the term remote access to electronic access including the relationship between the term electronic access and scoping language used in Section 3, Part 3.1, i-iii.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, the DT made clarifying changes to 3.1.3 to address this comment that multiple re-authentications are not required.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	No
Document Name	
Comment	
The term “user-initiated instance” needs to be further clarified. We require more clarification on how much weight the technical rationale will have in interpreting compliance with Sections 3.1.3 and 3.1.4 with regulators when completing compliance monitoring activities. We believe the removal of the word “remote” from Section 3.1.3 in permitting user-initiated instances can create confusion on when a user is required to authenticate.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT clarified requirements within the Technical Rationale, and made clarifying changes to the standards with removal of “user-initiated instance”. The DT cannot speak on behalf of compliance related activities. Remote is defined in romanette (i).	
Richard Vendetti - NextEra Energy - 5	
Answer	No

Document Name	
Comment	
NEE's initial interpretation of CIP-003 Attachment 1 Section 3.1 was that the SDT's goal for inbound and outbound malicious communications protection was tied to firewalls or routers at each low BES Asset. However, the current language does not provide flexibility for managing inbound and outbound malicious communication security controls centrally, as illustrated in the Technical Rationale for Section 3.1.2. The standard language appears to imply medium impact Electronic Security Perimeter (ESP) and Electronic Access Point (EAP) protections at each low impact BES Asset without explicitly stating this. Section 3.1.4's authentication communication protection implies encryption at each remote cyber asset, exceeding medium impact requirements with Intermediate Systems. The Low Impact Criteria Review Team's (LICRT) intent was to address risk reduction for coordinated attacks on low BES Assets. Management of low impact security controls for authentication and malware mitigation, either locally or centrally, should be accommodated in Section 3.1 language. Implying controls are mandated at each low BES Asset goes beyond the LICRT's effort. While the Technical Rationale illustration for Section 3.1.2 provides for central aggregation, it does not address Section 3.1.4 if encrypted authentication communications pass through a central malware mitigation system for inbound and outbound traffic. The SDT should consider adjusting the language to allow both centralized and local security control options and clarify what options are available.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, the DT has made clarifying changes in both the Technical Rationale and the standard.	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The language used should prioritize risk-based assessment with a focus on operational impact.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, the DT has made clarifying changes in both the Technical Rationale and the standard.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy Houston Electric (CEHE) appreciates the work of the drafting team to address previous feedback provided for CIP-003-A Attachment 1. CEHE suggests the following changes in bold in order to qualify the type of access that is being addressed by this standard. The use of the verbiage "user-initiated instance of electronic access" could easily be interpreted as any user log-in. The act of a user logging into a local HMI at a substation is technically a "user-initiated instance of electronic access ." The suggested changes are intended to mimic the Interactive Remote Access term as defined in the NERC Glossary of terms, while not making any reference to an ESP. 3.1.3 Authenticate users when permitting each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, to a network(s) containing low impact BES Cyber Systems;	

3.1.4 Protect user authentication information for each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and • the authentication system used to meet Section 3.1.3, or • the asset containing low impact BES Cyber System(s); 3.1.5 Include one or more method(s) for determining vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted; and 3.1.6 Include one or more method(s) for disabling vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please explain why, and provide recommended language you would support and, if appropriate, technical, or procedural justification.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The drafting team (DT) made changes in Part 3.1.3 to address these comments. For Part 3.1.4, conforming changes were made to support the changes made in Part 3.1.3. These changes were made to clarify that 3.1.3 and 3.1.4 only apply to user based electronic access. The DT has chosen not to implement these changes as 3.1.5 and 3.1.6 are intended to capture both user based and system to system electronic access. This terminology was taken from the currently approved version of CIP-003-9 Attachment 1 section 6, and as there have been no material changes made to this requirement language, this DT is interested in preserving the associated language. The DT made changes to clarify what is meant by “remote” without including that language. Please see the changes before Section 3.1.1. An explanation on the purpose for removing “remote” has also been add to the TR.

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	

Comment	
Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
It is NST's understanding, based on the Technical Rationale document and the SDT's March 6, 2024 project webinar, that once a remote user has been authenticated in accordance with proposed requirement 3.1.3 and allowed to access a network containing low impact BCS, a Responsible Entity could, if it was so inclined, allow that user to connect to multiple BCS within that network, without re-authentication, for the duration of any given instance of remote electronic access. We believe that 3.1.3 should be modified to make this clear.	
Likes 1	LS Power Development, LLC, 5, Campbell C. A.
Dislikes 0	
Response	
Thank you for your comment. The DT made clarifying changes to 3.1.3 to address this comment that multiple re-authentications are not required.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	No
Document Name	

Comment	
LS Power Development agrees with comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
Seminole Electric votes negative because the standard drafting team has failed to justify within their technical rationale the need and the basis for all of the additional requirements for low impact sites	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see the background information in the Technical Rationale and the LICRT report for the rationale of the need.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	

Attachment 1 appears to have exceeded the CIP-003 R2 (documented cybersecurity plan) due to the amount of technical controls that have now been added.

Recommendation: if the SDT intends to keep expanding controls beyond the documented plans they should consider creating a new requirement.

Why is this phrase used “User initiated instance electronic access”. Recommending using a more consolidated term than “inbound and outbound electronic access”. If meaning bi-directional, then the standard should state that versus drawing a distinction between inbound and outbound.

Sub requirement 3.15, request clarification on whether the sub requirement applies to both system to system and user-initiated access by a vendor.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The purpose of Attachment 1 is to define any technical requirements for Low Impact BES. Hence DT team updated the attachment for consistency. The need for a new requirement can be discussed with NERC but that is not in-scope for this team.

The DT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums. Additionally, the DT asserts that this is beyond the scope of the SAR.

After a thorough review, the DT has decided that consolidating “inbound and outbound electronic access” to the term "bi-directional" could produce additional confusion due to instances that may arise where inbound and outbound electric access is not bi-directional. Therefore the DT has decided not to make any changes.

The DT didn't make material changes to 3.1.5 and 3.1.6. The previous DT stated that both interactive access and system to system was included.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, please see response to NPCC.	
Karla Weaver - Public Utility District No. 2 of Grant County, Washington - 4, Group Name GCPD Group	
Answer	No
Document Name	
Comment	
GCPD agrees and supports comments from SMUD and Tacoma Power about Appendix A section 3.13. This wording is more restrictive than IRAs utilized for Medium and High Impact access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to SMUD.	
Katrina Lyons - Georgia System Operations Corporation - 4	

Answer	No
Document Name	
Comment	
The modification to 3.1 iii is more limiting than intended. There are time-sensitive communications protocols that are unrelated to Protection Systems. The challenge for 3.1.2 lies in the fact these terms used have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, using these same words with different examples in the measures creates ambiguity in the expectations for compliance. The prescriptiveness of 3.1.3 and 3.1.4 seems to go beyond what is typically expected for Medium Impact.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, the DT has made conforming changes to the standard to match those approved in 2016-02. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems' level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The DT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums. Additionally, the DT asserts that this is beyond the scope of the SAR.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	

Comment	
Duke Energy supports the proposed langauge but also supports EEI's alternative language for added clarity.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by MRO NSRF.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for the comment, please see the response to MRO.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Time-sensitive communications of Protection Systems needs to be clearly defined.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments, the DT has made conforming changes to the standard to match those approved in 2016-02. Please see the standard revisions and CIP-005 Technical Rational drafted by the 2016-02 DT.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Thank you for considering and addressing the concerns by changing 3.1.4 in Section 3 to specifically include entity flexibility for the end target of the protection as either the "asset containing" or the authentication source used in 3.1.3 (such as an Intermediate System).	
Likes 0	
Dislikes 0	
Response	
The DT thanks you for your comment.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
For Section 3.1.3, the NSRF recommends changing "when" to "prior to" in order to clarify that the remote user be authenticated prior to access, as explained in the Technical Rationale.	

Additionally, the currently proposed language does not contain the clarification stated in the Technical Rationale that would allow a single authentication for user-initiated access to low impact BCS that reside in a sub-network contained within a larger network. The NSRF recommends adding a parenthetical to Section 3.1.3 to align with that intent. Example: 3.1.3 Authenticate users **prior to** permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems **(multiple re-authentications to sub-networks within a larger network are not required)**; MRO NSRF is of the belief that both of these suggested changes would be non-substantive and could be implemented prior to final ballot, if this ballot is successful.	
Likes 2	Orlando Utilities Commission, 5, Colon Dania; American Municipal Power, 5, Ritts Amy
Dislikes 0	
Response	
Thank you for the comment. The DT made changes in Part 3.1.3 to address these comments.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes

Document Name	
Comment	
For Section 3.1.3, Manitoba Hydro recommends changing “when” to “prior to” in order to clarify that the remote user be authenticated prior to access, as explained in the Technical Rationale. Additionally, the currently proposed language does not contain the clarification stated in the Technical Rationale that would allow a single authentication for user-initiated access to low impact BCS that reside in a sub-network contained within a larger network. Manitoba Hydro recommends adding a parenthetical to Section 3.1.3 to align with that intent. Example: 3.1.3 Authenticate users **prior to** when permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems **(multiple re-authentications to sub-networks within a larger network are not required)**; Manitoba Hydro is of the belief that both of these suggested changes would be non-substantive and could be implemented prior to final ballot, if this ballot is successful.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to MRO NSRF.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	

Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI's proposal for the following modifications to Section 3, Part 3.1.3: "Authenticate users **prior to** (*remove:* when) permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems **(multiple re-authentications to sub-networks within a larger network are not required);"** We also suggest including clear language in the implementation guidance describing the change from use of the term remote access to electronic access including the relationship between the term electronic access and scoping language used in Section 3, Part 3.1, i-iii.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	

Comment	
Southern Company is in agreement with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Jamie Monette - Jamie Monette On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Jamie Monette	
Answer	Yes
Document Name	
Comment	

The term user-initiated access creates ambiguity.	
Likes 0	
Dislikes 0	
Response	
The DT thanks you for your response, and has made clarifying changes to both the standard and the technical rationale.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF requests clarification regarding the language in section 3.1.3 for initial user-initiated access being adequate to move between low impact systems without additional authentication.	
Likes 0	
Dislikes 0	
Response	
The DT thanks you for your response. Clarifying changes have been made to show that one authentication should be sufficient.	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Recommended changes are in **bold**:	

3.1.3 Authenticate users **prior to** permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems **(multiple re-authentications to sub-networks within a larger network are not required)**;	
Likes 0	
Dislikes 0	
Response	
The DT thanks you for your response. Clarifying changes have been made to the standard. Please see the Technical Rationale for more information.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the MRO NSRF for questions #1.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the responses to EEI and MRO.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	

PNMR agrees with the language proposed in CIP-003-A Attachment 1. However, PNMR does agree with EEI in their suggestion to include clear language in the implementation guidance describing the change from the use of the term remote access to electronic access including the relationship between the term electronic access and scoping language used in Section 3, part 3.1, i-iii.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI's comments.	

Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	
Response	

Thank you for the comment, please see response to EEI.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
ACES approves of the proposed changes, but at some point, to make the standards clearer, we should consider distinguishing between "electronic access" a logical network connection and an individual's "electronic access" ie the ability to use credentials to log into a Cyber Asset.	
Likes 0	
Dislikes 0	
Response	
The DT thanks you for your response and support.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Selene Willis - Edison International - Southern California Edison Company - 5	

Answer	Yes
Document Name	
Comment	
See EEI Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Kristina Marriott - Miller Bros. Solar, LLC - 5 - MRO,WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for your support.	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	

Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Patricia Ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

2. Do you agree with the language proposed in CIP-003-A Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

We do not concur with the proposed language in Attachment 2 for the same reasons we do not agree with the language in Attachment 1. Please see the response to question 1 above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, please see the DT's response to question 1.	
Karla Weaver - Public Utility District No. 2 of Grant County, Washington - 4, Group Name GCPD Group	
Answer	No
Document Name	
Comment	
Item 3 is the measure for section 3.1.3 which is too restrictive.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT created the examples listed in Attachment 2 not as an exhaustive list of how an entity must comply with the requirement, but rather to provide entities with examples of how they can demonstrate compliance with the requirements.	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	

Seminole Electric votes negative and does not agree because the standard drafting team has failed to justify within their technical rationale the need and the basis for all of the additional requirements for low impact sites	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT maintains the Technical Rationale provides background on the modifications made by the drafting team. The SAR and the LICRT report provide background on the justification for the changes.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	No
Document Name	
Comment	
LS Power Development agrees with comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments	

Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

CEHE does not support the language proposed in CIP-003-A Attachment 2.

SIGE suggests the following changes in bold in order to qualify the type of access that is being addressed by this standard. The use of the verbiage “user-initiated instance of electronic access” could easily be interpreted as any user log-in. The act of a user logging into a local HMI at a substation is technically a “user-initiated instance of electronic access.” The suggested changes are intended to mimic the Interactive Remote Access term as defined in the NERC Glossary of terms, while not making any reference to an ESP.

Attachment 2, Section 3:

3. For Section 3.1.3, documentation showing the ability to authenticate users when permitting each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, where **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, to a network(s) containing low impact BES Cyber Systems, such as:

• Authentication mechanism(s) including but not limited to:

{C}§ Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or

{C}§ Enforcement of Multi-Factor Authentication (MFA).

• Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;

• Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BES Cyber System; or

• Other operational, procedural, or technical controls.

4. For Section 3.1.4, documentation showing the ability to protect user authentication information for each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, where electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

• the authentication system used to meet Section 3.1.3, or

• the asset containing low impact BES Cyber System(s),

such as:

• Protection mechanism(s) including but not limited to:

{C}§ Implementation of an encrypted protocol or service (Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH), etc.); or

{C}§ Implementation of an IPsec or Secure Sockets Layer (SSL) VPN.

{C}§ Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic remote access, where vendor electronic **remote** access, **not including system-to-system process communication**s, is permitted and electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, such as:

• Steps to preauthorize access;

• Alerts generated by vendor log on;

• Session monitoring;

• Security information management logging alerts;

• Time-of-need session initiation;

• Session recording;

• System logs; or

• Other operational, procedural, or technical controls.

6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted and electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, such as:

• Disabling vendor electronic **remote** access, **not including system-to-system process communications accounts**;

• Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic **remote** access, **not including system-to-system process communications**;

• Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic **remote** access, **not including system-to-system process communications**;

• Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);

• Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic **remote** access, **not including system-to-system process communications**; or

• Other operational, procedural, or technical controls.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The drafting team (DT) made changes in Part 3.1.3 to address these comments. For Part 3.1.4, conforming changes were made to support the changes made in Part 3.1.3. These changes were made to clarify that 3.1.3 and 3.1.4 only apply to user based electronic access. The DT has chosen not to implement these changes as 3.1.5 and 3.1.6 are intended to capture both user based and system to system electronic access. This terminology was taken from the currently approved version of CIP-003-9 Attachment 1 section 6, and as there have been no material changes made to this requirement language, this DT is interested in preserving the associated language. The drafting team made conforming changes to Attachment 2 due to the changes in Attachment 1.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The language used should prioritize risk-based assessment with a focus on operational impact.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, the DT has made clarifying changes in both the Technical Rationale and the standard.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	

Please updated Attachment 2 to include the updated Attachment 1 Section 3 controls requested in question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has made conforming changes to Attachment 2 based on the updates made to Attachment 1.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	No
Document Name	
Comment	
The additional discrete requirements and expansion to all inbound and outbound electronic access is a significant incremental increase in the requirements for low-impact assets. Pending on an organizations current cybersecurity maturity level, meeting and maintaining these requirements will take significant effort and cost. It is anticipated this will require entities to hire multiple additional full-time staff to maintain and partake in lengthy contract negotiations with OEMs and other remote access vendors to ensure the additional discrete details included in the language can be met. Although section 3.1.2 is within the scope of the SAR, we still believe it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. The proposed language requires detection of known/suspected malicious communications for “inbound and outbound electronic remote access.” There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5). We suggest that this requirement be removed for better consistency with the requirements for Medium BCS or the applicability be changed to bring it in-line with other requirements.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems' level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The DT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums. Additionally, the DT asserts that this is beyond the scope of the SAR.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI proposes the following revisions to align with the proposal provided in response to Question 1. "For Section 3.1.3, documentation showing the ability to authenticate users **prior to** permitting each user-initiated instance of electronic access, where electronic access meets the criteria specified in Section 3.1, to a network(s) containing low impact BES Cyber Systems, such as…"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the DT has made this change along with other conforming changes in response to updates made in Attachment 1.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	

Answer	No
Document Name	
Comment	
NCPA supports comments made by SMUD and Tacoma Power.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see SMUD and Tacoma Power responses.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
In Attachment 2, Section 3, Example 2, in the list of examples the "Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)" is the only one of the bulleted list that meets the security objective of the SAR. For example: · "Anti malware technologies" are at the host level and are not a great option for detecting "malicious communications at the network level". The controls should be network based and not host based. · "Automated or manual log reviews" are too ambiguous, it would be best to specify what types of logs that would meet the security objective. Simply reviewing electronic access logs, for example, is not sufficient. · "Alerting" and "Other operational, procedural, or technical controls" should be removed since they provide no real guidance.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has included some new suggested examples under Attachment 2 (note: not an exhaustive list of every example).	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Attachment 1 - Ameren would like clarity in section 3.1.3. Is the Responsible Entity capable of relying on services/support vendors for user accounts and authentication? Attachment 2 - For section 3.1.5, Ameren would like clarity around the phrase "Security information management logging alerts." In CIP-007, this is described as "Security event monitoring."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. This DT believes the Project 2020-03 DT who worked on CIP-003-9 drew comparisons to the measure language offered in CIP-005-7 R2.4 when they were working on section 6. “Security information management logging alerts” is just one example out of many that can demonstrate compliance with section 3.1.5. This terminology was taken from the currently approved version of CIP-003-9 Attachment 2 section 6.1, and as there have been no material changes made to this requirement language, this DT is interested in preserving the associated guidance language.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	

Comment	
Reclamation recommends aligning language with CIP-005-7 language or first focusing on modifying CIP-005-7 language prior to adjusting language for CIP-003-A.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the DT has responded to the requirements of the SAR which was based on the results of the Low Impact Criteria Review Team paper.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Please see response to question #1. Attachment 2 language would need to be updated based on the proposed changes in Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, please see the DT's response to question 1. The DT has made conforming changes to Attachment 2 based on the updates made to Attachment 1.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	

SIGE suggests the following changes in bold in order to qualify the type of access that is being addressed by this standard. The use of the verbiage “user-initiated instance of electronic access” could easily be interpreted as any user log-in. The act of a user logging into a local HMI at a substation is technically a “user-initiated instance of electronic access.” The suggested changes are intended to mimic the Interactive Remote Access term as defined in the NERC Glossary of terms, while not making any reference to an ESP.

Attachment 2, Section 3:

3. For Section 3.1.3, documentation showing the ability to authenticate users when permitting each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, where **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, to a network(s) containing low impact BES Cyber Systems, such as:

• Authentication mechanism(s) including but not limited to:

{C}§ Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or

{C}§ Enforcement of Multi-Factor Authentication (MFA).

• Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;

• Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BES Cyber System; or

• Other operational, procedural, or technical controls.

4. For Section 3.1.4, documentation showing the ability to protect user authentication information for each user-initiated instance of electronic **remote** access, **not including system-to-system process communications**, where electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

• the authentication system used to meet Section 3.1.3, or

• the asset containing low impact BES Cyber System(s),

such as:

• Protection mechanism(s) including but not limited to:

{C}§ Implementation of an encrypted protocol or service (Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH), etc.); or

{C}§ Implementation of an IPsec or Secure Sockets Layer (SSL) VPN.

{C}§ Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic remote access, where vendor electronic **remote** access, **not including system-to-system process communication**s, is permitted and electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, such as:

• Steps to preauthorize access;

• Alerts generated by vendor log on;

• Session monitoring;

• Security information management logging alerts;

• Time-of-need session initiation;

• Session recording;

• System logs; or

• Other operational, procedural, or technical controls.

6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic **remote** access, **not including system-to-system process communications**, where vendor electronic **remote** access, **not including system-to-system process communications**, is permitted and electronic **remote** access, **not including system-to-system process communications**, meets the criteria specified in Section 3.1, such as: • Disabling vendor electronic **remote** access, **not including system-to-system process communications accounts**; • Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic **remote** access, **not including system-to-system process communications**; • Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic **remote** access, **not including system-to-system process communications**; • Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment); • Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic **remote** access, **not including system-to-system process communications**; or • Other operational, procedural, or technical controls.	
Likes 0	
Dislikes 0	
Response	
These changes were made to clarify that 3.1.3 and 3.1.4 only apply to user based electronic access. The DT has chosen not to implement these changes as 3.1.5 and 3.1.6 are intended to capture both user based and system to system electronic access. This terminology was taken from the currently approved version of CIP-003-9 Attachment 1 section 6, and as there have been no material changes made to this requirement language, this DT is interested in preserving the associated language. Conforming changes were made in Attachment 2 to align with the changes made in Attachment 1.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No

Document Name	
Comment	

In Attachment 2, Section 3, Example 2, there is only one bullet in the list of examples provided that meet the security objective of the SAR. That example is “Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)”.

The other bullets are not good examples for the following reasons:

“Anti-malware technologies” are at the host level and is not a great control for detecting “malicious communications at the network level;” malicious code - YES, malicious communications - NO. The controls should be network based and not host based.

“Automated or manual log reviews” depending on how they are done, is not a great control. It would be best to specify what types of logs that would meet the security objective (e.g. Security Incident and Event Management logs, Netflow, Jflow etc.). Simply reviewing electronic access logs, for example, is not sufficient.

“Alerting” and “Other operational, procedural, or technical controls” do not add any value to the list of examples since they provide no real guidance.

SMUD recommends the Standards Drafting Team consider the following changes to Attachment 2, Section 3, Example 2:

“2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets the criteria specified in Section 3.1, such as:

• Anti-malware technologies; **[Delete]**

• Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)

- Monitor or alert for changes to communication baselines; [**Add]**
- Logging and alerting configuration for Security Incident and Event Management (SIEM) systems or other event correlation systems; [**Add]**

• Automated or manual log reviews; **[Delete]**

• Alerting; or **[Delete]** • Other operational, procedural, or technical controls**. [Delete]**	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has included some of the new suggested examples under Attachment 2 (note: not an exhaustive list).	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
Attachment 2, Section 3: All the Authentication Mechanisms identified represent some form of centralized account management. Due to economies of scale, reliability, this may not represent the best option. Additionally, it precludes usage of password vault tools that may provide effective security for managing credentials. Please re-word to allow flexibility of approach based on risk and technologies.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. While some of the examples in Attachment 2 include centralized authentication mechanisms, it is not the DT's intention to be an exhaustive/prescriptive list of only acceptable solutions. The DT understands that each Responsible Entity will have different architectures and thus included the last bullet "[or] Other operational, procedural, or technical controls" to allow each Responsible Entity flexibility in finding a tool that works for them.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Matthew Jaramilla, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	

Answer	No
Document Name	
Comment	
Salt River Project supports SMUD comments and also suggest deleting "automated or manual log reviews" and "alerting"	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to SMUD.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Although section 3.1.2 is within the scope of the SAR, BPA still believes it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. The proposed language requires detection of known/suspected malicious communications for “inbound and outbound electronic remote access.” There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5). BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS or the applicability be changed to bring it in-line with other requirements.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	

Thank you for your comments. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems' level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The DT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Tacoma Power recommends updating the Attachment 2 language based on the proposed changes to Attachment 1, Section 3.1.3 (see response to Comment 1). Tacoma Power also endorses the comments provided by SMUD.	
Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	
Response	
Thank you for your comment, please see the DT's response to question 1. The DT has made conforming changes to Attachment 2 based on the updates made to Attachment 1. Additionally, see response to SMUD's comment.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No

Document Name	
Comment	
Please reference the comments in response to Question 1 above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see the DT's response to question 1.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
NRG disagrees with the removal of the term "remote" when referencing "electronic remote access" throughout Attachment 1. Not only does this significantly expand the scope of the requirements with respect to any type of non-remote electronic access, but it also moves away from the original intent of the three recommendations initially proposed by the LICRT. NRG recommends expanding the definition of the current term "interactive remote access" to include Low Impact BES Cyber Systems and using that newly defined terminology throughout this requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT made changes to clarify what is meant by "remote" through romanette (i). Please see the changes before Section 3.1.1. An explanation on the purpose for removing "remote" has also been add to the Technical Rationale.	

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	

In Attachment 2, Section 3, Example 2, there is only one bullet in the list of examples provided that meet the security objective of the SAR. That example is “Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)”.

The other bullets are not good examples for the following reasons:

“Anti malware technologies” are at the host level and is not a great control for detecting “malicious communications at the network level;” malicious code - YES, malicious communications - NO. The controls should be network based and not host based.

“Automated or manual log reviews” depending on how they are done, is not a great control. It would be best to specify what types of logs that would meet the security objective (e.g. Security Incident and Event Management logs, Netflow, Jflow etc.). Simply reviewing electronic access logs, for example, is not sufficient.

“Alerting” and “Other operational, procedural, or technical controls” do not add any value to the list of examples since they provide no real guidance.

SMUD recommends the Standards Drafting Team consider the following changes to Attachment 2, Section 3, Example 2:

“2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets the criteria specified in Section 3.1, such as:

• Anti-malware technologies; [Delete]

• Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);

- Monitor or alert for changes to communication baselines; [Add]
- Logging and alerting configuration for Security Incident and Event Management (SIEM) systems or other event correlation systems; [Add]

• Automated or manual log reviews; [Delete]

• Alerting; or [Delete]

• Other operational, procedural, or technical controls. [Delete]

Likes 2	Orlando Utilities Commission, 5, Colon Dania; American Municipal Power, 5, Ritts Amy
Dislikes 0	

Response

Thank you for your comments. The DT has included some of the new suggested examples under Attachment 2 (note: not an exhaustive list).

Kristina Marriott - Miller Bros. Solar, LLC - 5 - MRO,WECC,Texas RE

Answer	No
Document Name	

Comment

Language throughout that states "such as" then listing multiple bullet points should be reworded to state: "one or more of the following". The “such as” verbiage may lead auditors to mark each item as being applicable.

Likes 0	
Dislikes 0	

Response

Thank you for your comment, the DT has decided to maintain the current language. The DT believes “such as” does afford flexibility to the Responsible Entity and does not prescribe a specific solution.

Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See EEI Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	

Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI's comments.	

Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the MRO NSRF for questions #2.	
Likes 0	
Dislikes 0	

Response	
Thank you for the comment, please see the response to EEI.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF requests clarification for section 3.1.3 to understand if the Responsible Entity can rely on services/support vendors for their user accounts and authentication.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. You may refer to the CMEP Practice Guide on Using the Work of Others on how CMEP staff may treat this type of evidence.	
Jamie Monette - Jamie Monette On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Jamie Monette	
Answer	Yes
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Recommend modifying the language in Attachment 1 to align with the language in Attachment 2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has made conforming changes to Attachment 2 based on the updates made to Attachment 1.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company is in agreement with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes

Document Name	
Comment	
Black Hills Corporation agrees with EEI's proposal for the following revisions to align with the proposal provided in response to Question 1. "For Section 3.1.3, documentation showing the ability to authenticate users **prior to (*remove:* when)** permitting each user-initiated instance of electronic access, where electronic access meets the criteria specified in Section 3.1, to a network(s) containing low impact BES Cyber Systems, such as…"	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see the response to EEI.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes

Document Name	
Comment	
Revise Section 3.1.3 based on Attachment 1 revisions recommended above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see the DT's response to question 1.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	

The language in CIP-003A Attachment 2 is acceptable as long as the wording for 3.1.3 and 3.1.4 are modified/updated as suggested	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see the DT's response to question 1. The DT has made conforming changes to Attachment 2 based on the updates made to Attachment 1.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Revise Section 3.1.3 based on Attachment 1 revisions recommended above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see the DT's response to question 1. The DT has made conforming changes to Attachment 2 based on the updates made to Attachment 1.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by MRO NSRF	

Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to MRO NSRF.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the proposed language but also supports EEI's alternative language for added clarity.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Patricia Ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

3. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-A. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
As Long as Dial-up is not in scope 3 years is agreeable. IF Dial-up is NOT removed, 3 years is not long enough.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for your comment. Part 3.2 of Attachment 1 for authentication of dial-up were not materially changed as part of this project. The modifications that were made to Part 3.2 from CIP-003-9 were in formatting only. Changes or exclusion of requirement for dial-up are outside the scope of the approved SAR for this project.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	

AZPS agrees with EEI's proposal to align the implementation plans for CIP-003 changes resulting from Project 2016-02 and Project 2023-04 to avoid separate versions and implementation plans which will require entities to make changes affecting low impact BCS under different regulatory deadlines resulting in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Until Tacoma Power's concern on the language in Attachment 1 Section 3.1.3 is resolved to include only the initial authentication, this implementation plan is not achievable. However, if these concerns are addressed, then 36 months is reasonable timeframe.	
Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	
Response	
Thank you for your comment, please see responses to Questions 1 and 2.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	

Comment	
As Long as Dial-up is not in scope 3 years is agreeable. IF Dial-up is NOT removed, 3 years is not long enough.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Part 3.2 of Attachment 1 for authentication of dial-up were not materially changed as part of this project. The modifications that were made to Part 3.2 from CIP-003-9 were in formatting only. Changes or exclusion of requirement for dial-up are outside the scope of the approved SAR for this project.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Until Questions 1 and 2 are resolved it is difficult for BPA to determine if the 3 year timeframe is appropriate.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see responses to questions 1 and 2.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	

Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Matthew Jaramilla, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
Salt River Project agrees and supports comments from AZPS and EEI. In addition, SRP would like to have a specific date of implementation as there is significant cost associated with this project (equipment and resources), time for planning, and work that would need to be done.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see responses to AZPS and EEI. The implementation plan specifies a 3-year timeline after final approvals. Final approvals depend on successful balloting, NERC Board and FERC approvals which are unknown at this time.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	

SIGE supports the comments as submitted by Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends that the CIP-003-A implementation plan consider the CIP-003-10 implementation plan to allow the effective use of resources.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. For this posting the drafting team included a CIP-003-12 draft standard and implementation plan which takes into account the timelines of the two versions of the standard.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company is in agreement with EEI comments.	

Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The NAGF recommends that the CIP-003-A implementation plan consider the CIP-003-10 implementation plan to allow the effective use of resources.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. For this posting the drafting team included a CIP-003-12 draft standard and implementation plan which takes into account the timelines of the two versions of the standard.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #3.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NEE supports EEI's comments: "EEI proposes the alignment of the implementation plan for CIP-003 in Project 2016-02 with the 3-year implementation plan proposed in Project 2023-04 allowing entities to only make changes to the affected sites once. We further suggest combining the revisions to CIP-003 resulting from Project 2023-04 and 2016-02 into one version for NERC Board approval after passing ballot if they will be presented to the Board at the same meeting. Separate versions and implementation plans will require entities to make changes affecting low impact BCS	

under different regulatory deadlines resulting in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated."	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The undertaking will demand significant effort, substantial capital investment and additional staffing.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The revisions to CIP-003-9 were made based on the scope of the approved SAR, and the DT appreciates that there may be cost associated with the implementation.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

Comments: CEHE does not agree with the proposed implementation plan because of the pending changes in Project 2016-02. CEHE agrees with EEI's comment on the implementation plan. EEI Comments: EEI proposes the alignment of the implementation plan for CIP-003 in Project 2016-02 with the 3-year implementation plan proposed in Project 2023-04 allowing entities to only make changes to the affected sites once. We further suggest combining the revisions to CIP-003 resulting from Project 2023-04 and 2016-02 into one version for NERC Board approval after passing ballot if they will be presented to the Board at the same meeting. Separate versions and implementation plans will require entities to make changes affecting low impact BCS under different regulatory deadlines resulting in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
See comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	No
Document Name	
Comment	
As a parent company to a fleet of over 25 Low Impact Generation Facilities, along with affiliates with equally sizeable fleets, 36 months will not be enough time for owners with multiple Low Impact generation facilities to onboard these controls. Recommend a provision for owners with multiple Low Impact facilities allowing up to 5 years.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team has not made changes to the implementation plan and asserts that the drafted implementation timeline is in-line with similar standards changes.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	

Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
We do not agree with the proposed implementation plan. Our apprehension primarily stems from the intersection of CIP-003-A and CIP-003-9, with a particular focus on the potential financial implications in Section 6.3, where additional expenditures may be necessitated to accommodate technological changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The revisions to CIP-003-9 were made based on the approved SAR and the DT appreciates that there may be cost associated with the implementation of the new standard.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	

SMUD agrees with a three-year implementation plan and believes it is the necessary amount of time for supply chains to support the changes registered entities will need to implement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the implementation plan, but also supports EEI's recommendation to align the implementation of the LICRT CIP-003 revisions with the implementation of the CIP-003 revisions from the 2016-02 Project.	
Likes 0	
Dislikes 1	Orlando Utilities Commission, 5, Colon Dania
Response	
Thank you for the comment, please see response to EEI.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by MRO NSRF	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to MRO NSRF.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
The 3 year implementation plan is sufficient unless there is a supply chain issue with the manufacturers of the equipment needed to implement this solution.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
OUC agrees with a three-year implementation plan and believes it is the necessary amount of time for supply chains to support the changes registered entities will need to implement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
If concerns are addressed in Attachment 1 then a 3 year implementation time is sufficient.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to other comments regarding Attachment 1.	

Jamie Monette - Jamie Monette On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Jamie Monette	
Answer	Yes
Document Name	
Comment	
Additional time should be considered to architect and implement authentication methods.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team has not made changes to the implementation plan and asserts that the drafted implementation timeline is in-line with similar standards changes.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI proposes the alignment of the implementation plan for CIP-003 in Project 2016-02 with the 3-year implementation plan proposed in Project 2023-04 allowing entities to only make changes to the affected sites once. We further suggest combining the revisions to CIP-003 resulting from Project 2023-04 and 2016-02 into one version for NERC Board approval after passing ballot if they will be presented to the Board at the same meeting. Separate versions and implementation plans will require entities to make changes affecting low impact BCS under different regulatory deadlines resulting in unnecessary and excessive entity costs and challenges to comply within the timeframe as mandated.	
Likes 1	Sempra - San Diego Gas and Electric, 5, Wright Jennifer
Dislikes 0	

Response	
Thank you for your comments. Thank you for your comment. For this posting the drafting team included a CIP-003-12 draft standard and implementation plan which takes into account the timelines of the two versions of the standard.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See EEI Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Mohamed Derbas - Sempra - San Diego Gas and Electric - 1	
Answer	Yes
Document Name	
Comment	
SDG&E supports EEI's comments on this item.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	

Kristina Marriott - Miller Bros. Solar, LLC - 5 - MRO,WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karla Weaver - Public Utility District No. 2 of Grant County, Washington - 4, Group Name GCPD Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Ireland - DTE Energy - 4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
WECC leaves comments on the implementation plan to the applicable entities.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

4. The DT believes the language of CIP-003-A addresses the issues outlined in the SAR in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical, or procedural justification.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
3.1.2 exceeds the Standards for Medium Impact and incurs substantial costs. The challenge lies in the fact these terms have acquired specific connotations, such as those associated with medium/high controls centers. Consequently, using these same words with different examples in the measures creates ambiguity in the expectations for compliance.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high impact BCS are subject to all	

relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems' level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The DT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums. Additionally, the DT asserts that this is beyond the scope of the SAR.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	
Some entities implemented electronic access controls not expecting these added controls. The added malicious communication detection(s) may require a complete redesign to properly implement this control making it costly.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	No
Document Name	
Comment	

Since there is no cost recovery mechanism for generation facilities, from a business perspective, these technical controls and compliance processes have the potential to significantly impact the cost structure of support at each site. It would be accurate to say that we have the framework in place to support these technologies, but the concern would be the human-capital required to support the recurring maintenance of such processes. Because of how Low Impact Generation Facilities are setup, the objectives outlined in the proposed controls would require effort from IT/OT support providers, O&Ms, and OEMs. Needless to say, 36 months will not be enough time for owners with multiple Low Impact generation facilities to implement these requirements.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The undertaking will demand significant effort, substantial capital investment and additional staffing.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems	

against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	No
Document Name	
Comment	
The additional discrete requirements and expansion to all inbound and outbound electronic access is a significant incremental increase in the requirements for low-impact assets. Pending on an organization's current cybersecurity maturity level, meeting and maintaining these requirements will take significant effort and cost. It is anticipated this will require entities to hire multiple additional full-time staff to maintain and partake in lengthy contract negotiations with OEMs and other remote access vendors to ensure the additional discrete details included in the language can be met.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Marty Hostler, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	

NCPA supports comments made by SMUD and Tacoma Power.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, please see response to SMUD and Tacoma Power.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response, the DT has made clarifying changes to the standard.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends minimizing churn among standard versions and clearly identify the scope; Reclamation also recommends the DT take additional time to coordinate the modifications with other existing drafting teams for related standards. This will help minimize	

the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. Reclamation will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The DT has worked with other teams to minimize the churn in the standards as much as possible. For this posting the drafting team included a CIP-003-12 draft standard and implementation plan which takes into account the timelines of the two versions of the standard.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State would need to have more details before costs could be accurately determined.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response, the DT has made clarifying changes to the standard.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	

NIPSCO has not determined whether this will be cost effective. The procurement process for a tool(s) and resources will be initiated should the requirement language remain as is.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
For small Entities implementation of the controls outlined in the proposed standard could be financially burdensome. Entities with a large number of Low stations may have difficulty meeting the 36 months implementation timeframe.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.	

The drafting team has not made changes to the implementation plan and asserts that the drafted implementation timeline is in-line with similar standards changes.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
For small Entities implementation of the controls outlined in the proposed standard could be financially burdensome. Entities with a large number of Low stations may have difficulty meeting the 36 months implementation timeframe.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective. The drafting team has not made changes to the implementation plan and asserts that the drafted implementation timeline is in-line with similar standards changes.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Matthew Jaramilla, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	

Salt River Project agrees and supports Tacoma's comment. In addition, SRP believes that more information required as it is difficult to determine the exact financial impact, even though we are expecting a significant cost that would need to be budgeted.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective. Additionally, the DT has made clarifying changes to the standard.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	
Comment	
As Long as Dial-up is not in scope the project can be performed in a cost-effective manner. IF Dial-up is not removed, the project will not be cost-effective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Part 3.2 of Attachment 1 for authentication of dial-up were not materially changed as part of this project. The modifications that were made to Part 3.2 from CIP-003-9 were in formatting only. Changes or exclusion of requirement for dial-up are outside the scope of the approved SAR for this project.	

Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
It cannot be determined at this time if the SAR addresses the issues in a cost effective manner.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective. Additionally, the DT has made clarifying changes to the standard.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Until Tacoma Power's concern on the language in Attachment 1 Section 3.1.3 is resolved to include only the initial authentication, this is not a cost effective requirement, both in terms of upfront cost of implementing significant additional tooling, as well as ongoing stakeholder time to update and perform work practices in a compliant manner.	

Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	

Response

The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.

Additionally, the DT has made clarifying changes to the standard.

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

Irrespective of cost effectiveness, NRG does not believe that the proposed changes address the original issues outlined in the SAR. Please reference comments in response to Question 1 above for additional detail.

Likes 0	
Dislikes 0	

Response

Thank you for your comments, please see response to question 1.

James Keele - Entergy - 3

Answer	No
Document Name	

Comment

As Long as Dial-up is not in scope the project can be performed in a cost-effective manner. IF Dial-up is not removed, the project will not be cost-effective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Part 3.2 of Attachment 1 for authentication of dial-up were not materially changed as part of this project. The modifications that were made to Part 3.2 from CIP-003-9 were in formatting only. Changes or exclusion of requirement for dial-up are outside the scope of the approved SAR for this project.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
Irrespective of cost effectiveness, NRG does not believe that the proposed changes address the original issues outlined in the SAR. Please reference comments in response to Question 1 above for additional detail.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, please see response to question 1.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No

Document Name	
Comment	
SMUD views the changes as neither cost effective nor cost ineffective.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for your response.	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your response.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See EEI Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	

No additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by MRO NSRF	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, please see response to MRO NSRF.	
Patricia Ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Karla Weaver - Public Utility District No. 2 of Grant County, Washington - 4, Group Name GCPD Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kristina Marriott - Miller Bros. Solar, LLC - 5 - MRO,WECC,Texas RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	
Document Name	
Comment	
ITC does not respond to cost questions	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	

NST lacks the information necessary to comment on this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the DT has made clarifying changes in the standard.	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE does not comment on costs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Jamie Monette - Jamie Monette On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Jamie Monette	
Answer	
Document Name	
Comment	
NA	

Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren has no comment on the cost effectiveness of the project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost-effectiveness.	
Likes 0	
Dislikes 0	
Response	

Thank you for your response.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
WECC leaves comments on the cost-effectiveness to the applicable entities.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	

5. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC
Answer
Document Name
Comment
In the revised Technical Rationale document on page 7, the paragraph directly above Figure 4 references “Figure 4” but is actually referencing Figure 5. If confirmed and appropriate, the paragraph should be moved below Figure 4 and the text changed to say:

"***Figure 5*** depicts an example of protected authentication at a central intermediate system before accessing a network containing a LIBCS. This protection mitigates the unintended disclosure of authentication information for remote access of LIBCS."	
Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	
Response	
Thank you for your comment, this change has been made.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	
Document Name	
Comment	
Duke Energy supports EEI's comments and thanks the Drafting Team for their work.	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
Alliant Energy supports comments submitted by MRO NSRF	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment, please see response to MRO NSRF.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
James Keele - Entergy - 3	
Answer	
Document Name	
Comment	
As Long as Dial-up is not in scope the new requirements for CIP-003-A can be implemented.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Part 3.2 of Attachment 1 for authentication of dial-up were not materially changed as part of this project. The modifications that were made to Part 3.2 from CIP-003-9 were in formatting only. Changes or exclusion of requirement for dial-up are outside the scope of the approved SAR for this project.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	
Document Name	
Comment	
Tacoma Power supports SMUD's comments on the technical rationale changes.	
Likes 1	American Municipal Power, 5, Ritts Amy
Dislikes 0	
Response	
Thank you for your comment, please see response to SMUD.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	
Document Name	2023-04 Unofficial Comment Form Additional Ballot_NSRF FINAL_20240306.docx
Comment	
The High VSL column for R2 regarding electronic access (Section 3) contains a typo at the end of the second paragraph. "Section 2" should read "Section 3".	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	

Response	
Thank you for your comment, this change has been made.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	
Document Name	
Comment	
As Long as Dial-up is not in scope the new requirements for CIP-003-A can be implemented.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Part 3.2 of Attachment 1 for authentication of dial-up were not materially changed as part of this project. The modifications that were made to Part 3.2 from CIP-003-9 were in formatting only. Changes or exclusion of requirement for dial-up are outside the scope of the approved SAR for this project.	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE recommends revising Requirement Part 3.1 from “shall implement a control(s) that” to “shall implement one or more controls that.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, this change has been made.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	

Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Matthew Jaramilla, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	
Document Name	
Comment	
Salt River Project still has concerns on how CIP-003 is written for low impact requirements to contain parts of all existing standards (for medium and high impact). Seems like there is an opportunity to just add low impact requirements to the existing standard(s). This will also help in keeping language consistent.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows “low impact only Entities” to comply with those two standards.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	

Document Name	
Comment	
BC Hydro appreciates the drafting team's efforts and the opportunity to comment, and offers the following suggestion. BC Hydro suggests included in the Technical Rationale more pertinent use cases and examples to clarify the language used in the revised standards. Specifically the use of 'operational, procedural or technical' methods mentioned in the revised CIP-003 standard Attachment 2 Section 3.5 and 3.6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT provided several technical options in Attachment 2 and in the Technical Rationale document.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	
Document Name	
Comment	
TVA does not agree with the inappropriate scaling of Medium and High controls to BCAs at Low assets. If additional requirement are scaled to Low BCAs, TVA recommends NERC identify Low BCS in the applicability of the CIP-004 - CIP-013 requirements instead of extending CIP-003 R2 to apply the same requirements to Lows.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also	

attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems' level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The DT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums. Additionally, the DT asserts that this is beyond the scope of the SAR. The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows "low impact only Entities" to comply with those two standards.	
Dania Colon - Orlando Utilities Commission - 5	
Answer	
Document Name	
Comment	
TVA does not agree with the inappropriate scaling of Medium and High controls to BCAs at Low assets. If additional requirements are scaled to Low BCAs, TVA recommends NERC identify Low BCS in the applicability of the CIP-004 - CIP-013 requirements instead of extending CIP-003 R2 to apply the same requirements to Lows.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems' level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The DT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o	

ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums. Additionally, the DT asserts that this is beyond the scope of the SAR. The SDT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows "low impact only Entities" to comply with those two standards.

TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	
Document Name	
Comment	

SIGE appreciates the work of the drafting team to address previous feedback provided for CIP-003-A Technical Rationale. SIGE suggests the following changes in order to qualify the type of access that is being addressed by this standard. The use of the verbiage "user-initiated instance of electronic access" could easily be interpreted as any user log-in. The act of a user logging into a local HMI at a substation is technically a "user-initiated instance of electronic access ". The suggested changes are intended to mimic the Interactive Remote Access term as defined in the NERC Glossary of terms, while not making any reference to an ESP.

Section 3.1.3

This is a new cyber security control outlined in the SAR, which requires entities to implement controls to authenticate users when permitting (allowing) each instance of **user-initiated instance of** electronic remote access, **not including system-to-system process communications,** to networks containing low impact BES Cyber Systems. The intent is at the time any access to the "network containing low impact BES Cyber Systems" is being permitted, the remote user is already authenticated. Figure 3 below depicts a situation where the authentication of the remote user is occurring after the user already has access to the "network containing LIBCS" as the authentication servers are on the same network with the LIBCS. The firewall in this scenario allows the user through to the network on which the LIBCS reside before the user is authenticated.

The intention of "each instance" phrase is meant to include the initial authorization and all subsequent re-connection instances of **user-initiated instance of electronic remote access, not including system-to-system process communications,** to the network. If there is a

collection of sub-networks or Cyber Assets within the network containing LIBCS, then multiple re-authentications at those levels would not be required. This control mitigates the risk of unauthenticated user access to networks on which LIBCS reside.

Section 3.1.4 contains an incorrect reference to Figure 4. The correct reference should be Figure 5.

Section 3.1.4

This is a new cyber security control outlined in the SAR. The objective of Attachment 1, Section 3.1.4 is for entities to protect the user authentication information (e.g., username, password, multi-factor authentication (MFA) information, session token, etc.) while in transit between the remote user's Cyber Asset and either the asset containing the LIBCS or the entity's authentication system used to meet Section 3.1.3. The intent is not to specify authentication directly to a particular device, but to allow for entities that desire to use an existing compliant CIP-005 Requirement R2 Intermediate System or similar architecture for access to networks containing LIBCS as well. For example, Figure 4 below depicts authentication at the boundary of the asset containing a LIBCS. In this example, the authentication server and jump host are on a different network than the "network containing LIBCS", making it uniquely different from Figure 3 above.

Figure 5 depicts an example of protected authentication at a central intermediate system before accessing a network containing a LIBCS. This protection mitigates the unintended disclosure of authentication information for remote access of LIBCS.

Section 3.1.5

The objective of Section 3.1.5 is to maintain the original language used in CIP-003-9, Section 6.1, as much as possible. One or more method(s) can be identified as part of this electronic access control. Entities must determine **user-initiated instances of vendor electronic remote access, not including system-to-system process communications**, where permitted, to their low impact BES Asset(s) and/or LIBCS. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular **user-initiated instance of vendor electronic remote access, not including system-to-system process**.

Section 3.1.6

The objective of Section 3.1.6 is to maintain the original language used in CIP-003-9, Section 6.2, as much as possible. One or more method(s) can be identified as part of this electronic access control. Entities must have the ability to disable **user-initiated instances of**

vendor electronic remote access, not including system-to-system process communications, where permitted, for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing LIBCS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. These changes were made to clarify that 3.1.3 and 3.1.4 only apply to user based electronic access. The DT has chosen not to implement these changes as 3.1.5 and 3.1.6 are intended to capture both user based and system to system electronic access. This terminology was taken from the currently approved version of CIP-003-9 Attachment 1 section 6, and as there have been no material changes made to this requirement language, this DT is interested in preserving the associated language. The Technical Rationale has been updated to correctly reference the figures.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	
Black Hills Corporation agrees with EEI's comments which request clarification around VPN tunnels and 3rd party authentication. (EEI comments included below) EEI proposes clarification in the Technical Rationale regarding the use of VPN tunnels as a permanent connection between OEMS and/or continuous monitoring vendors who use an HMI to remotely connect to an entity SCADA system to remotely maintain in-scope sites in the context of compliance with Attachment 1, R3, Part 3.1.3. As an example, wind farms can be maintained remotely by the OEM and/or have a continuous monitoring vendor (third-party) using HMIs remotely connected to the SCADA system via VPN tunnel. The VPN tunnel is typically established between a switch or firewall at the wind farm and a similar device at the third-party location. An HMI is set up at the third-party location. VPN tunnels are generally configured to	

connect automatically using pre-established authentication mechanisms. Once a VPN tunnel is formed it is a connection between the OEM and/or continuous monitoring vendor and the SCADA system for the vendor to manage the turbines. In this scenario, discussion in the Technical Rationale about an entity's ability to comply with Attachment 1, R3, Part 3.1.3. would be beneficial because third-party authentication would take place at the HMI and/or SCADA system devices, and the entity would not be in control of each user-initiated instance of electronic access because they occur on the third-party vendor's side of the VPN tunnel. Clarification could include discussion of this scenario in the context of Interactive Remote Access (IRA), and/or what is meant by "user-initiated instance of access to a network containing." EEI believes this change to the Technical Rationale document could be made without a substantive change requiring another ballot.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Richard Jackson - U.S. Bureau of Reclamation - 1	

Answer	
Document Name	
Comment	
Reclamation recommends when adjusting CIP-003 that changes first be made to Medium and High impact standards. CIP-003 should mirror higher impact requirements but at an equal to or less restrictive level.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems' level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The DT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums. Additionally, the DT asserts that this is beyond the scope of the SAR.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
Southern Company is in agreement with EEI comments.	
Likes 0	

Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Carver Powers - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	
Provide guidance on how a system similar to an Intermediate System could be used to meet 3.1.3 and 3.1.4. Technical guidance diagrams. The information in figure 4 should be included in the diagram for figure 1 and figure 2. Figure 4 provides confusion because it does not meet the criteria listed in 3.1.1 and 3.1.2. Figure 5 is not referenced in any of the guidance and is unclear if there is user authentication information between the jump host and the BES Cyber System.	

Several projects were/are modifying CIP-003 in parallel (2016-02, 2020-03 and 2023-04) and a different approach is used in dealing with the previous Technical Rationale content. For example, in Project 2023-04, hyperlinks to the previous TRs are added in the document, whereas in 2016-02, information from the previous TRs is kept and information was added related to the 2016-02 changes. Furthermore, the recently approved CIP-003-9 TR filed with the 2020-03 project contained only 8 pages from the initial 32 pages. These 8 pages consisted only the changes regarding the -9 version. In summary, three different projects modifying the CIP-003 and its TR with three different approaches. As a general comment, it would be helpful to the industry for the NERC SDTs to choose a way going forward that is applied across all NERC projects. In the case of the TR in this project, we suggest keeping one TR that includes the previous versions of the TR, as was done in the 2016-02 project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has made changes to clarify the Technical Rationale and believes the changes made address your comments. The TR written by 2016-02 contains the historical TR for previous versions of the standard. Prior to final ballot, the DT for 2023-04 will combine both TR files and retain the historical TR.	
Jamie Monette - Jamie Monette On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Jamie Monette	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	
Document Name	
Comment	
Jump Server comment. Technical guidance diagrams. Within the Technical Guidance diagrams there is a concern on Figure 3 and Figure 4 concerning if both diagrams are approved configurations or if figure 3 is an incorrect configuration and Figure 4 is an appropriate configuration. Additionally, in Figure 4 there needs to be a key for the line colors and a DMZ designation. Several projects were/are modifying CIP-003 in parallel (2016-02, 2020-03 and 2023-04) and a different approach is used in dealing with the previous Technical Rationale content. For example, in Project 2023-04, hyperlinks to the previous TRs are added in the document, whereas in 2016-02, information from the previous TRs is kept and information was added related to the 2016-02 changes. Furthermore, the recently approved CIP-003-9 TR filed with the 2020-03 project contained only 8 pages from the initial 32 pages. These 8 pages consisted only the changes regarding the -9 version. In summary, three different projects modifying the CIP-003 and its TR with three different approaches. As a general comment, it would be helpful to the industry for the NERC SDTs to choose a way going forward that is	

applied across all NERC projects. In the case of the TR in this project, we suggest keeping one TR that includes the previous versions of the TR, as was done in the 2016-02 project. We note that according to the proposed texts and considering the current version of CIP-005 for Medium Impact Systems, the level of security required for remote access of Low Impact systems is higher than for that of Medium Impact systems without Control Center. We assume that the future revision of CIP-005 will correct this apparent inconsistency.ma	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has made changes to clarify the Technical Rationale and believes the changes made address your comments. The TR written by 2016-02 contains the historical TR for previous versions of the standard. Prior to final ballot, the DT for 2023-04 will combine both TR files and retain the historical TR. Thank you for your comments. The DT notes that medium and high impact standards currently exist for remote access. The DT also notes that the required cyber security program for lows is not generally as strict or comprehensive as that for medium or high impact and also attempts to account for a wide diversity of entities that may have only low impact BCS. Medium and high impact BCS are subject to all relevant cyber security requirements in CIP-003 through CIP-013, whereas low impact systems are only subject to the requirements in CIP-003, which are not down to individual cyber systems' level. Medium impact BCS w/o ERC have a reduced remote access attack surface, yet still have more requirements on the individual cyber systems throughout the CIP standards. The DT asserts that remote access to low impact BCS with external routable protocol is a potential higher risk in this one specific area than a medium impact BCS w/o ERC and may require a singular stricter requirement on that remote access capability, while still maintaining a lower overall cyber security program level than mediums. Additionally, the DT asserts that this is beyond the scope of the SAR.	
Ben Hammer - Western Area Power Administration - 1	
Answer	
Document Name	

Comment	
The High VSL column for R2 regarding electronic access (Section 3) contains a typo at the end of the second paragraph. “Section 2” should read “Section 3”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, this change has been made.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the MRO NSRF for questions #5.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	

EEI proposes clarification in the Technical Rationale regarding the use of VPN tunnels as a permanent connection between OEMS and/or continuous monitoring vendors who use an HMI to remotely connect to an entity SCADA system to remotely maintain in-scope sites in the context of compliance with Attachment 1, R3, Part 3.1.3.

As an example, wind farms can be maintained remotely by the OEM and/or have a continuous monitoring vendor (third-party) using HMIs remotely connected to the SCADA system via VPN tunnel. The VPN tunnel is typically established between a switch or firewall at the wind farm and a similar device at the third-party location. An HMI is set up at the third-party location. VPN tunnels are generally configured to connect automatically using pre-established authentication mechanisms. Once a VPN tunnel is formed it is a connection between the OEM and/or continuous monitoring vendor and the SCADA system for the vendor to manage the turbines.

In this scenario, discussion in the Technical Rationale about an entity's ability to comply with Attachment 1, R3, Part 3.1.3. would be beneficial because third-party authentication would take place at the HMI and/or SCADA system devices, and the entity would not be in control of each user-initiated instance of electronic access because they occur on the third-party vendor's side of the VPN tunnel.

Clarification could include discussion of this scenario in the context of Interactive Remote Access (IRA), and/or what is meant by "user-initiated instance of access to a network containing."

EEI believes this change to the Technical Rationale document could be made without a substantive change requiring another ballot.

Likes 1	Sempra - San Diego Gas and Electric, 5, Wright Jennifer
Dislikes 0	

Response

Thank you for your comments. Changes have been made to clarify these points in the Technical Rationale.

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	
Document Name	

Comment

We operate within a geographical region characterized by limited access of local academic enrichment opportunities for young professionals in cybersecurity. Moreover, this project will require significant technical effort, substantial capital investment, and the augmentation of staffing resources.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The revisions to CIP-003-9 were made based on the scope of the approved SAR, and the SDT appreciates that there may be cost associated with the implementation of the new standard. The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of low BES Cyber Systems against compromise. Considering this, the drafting team left flexibility for the industry to implement changes with widely used industry tools and practices, which makes them cost-effective.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	
Document Name	
Comment	
Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
(None)	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	
Document Name	

Comment
LS Power Development agrees with comments submitted by EEL. Thank you for the opportunity to comment.

Likes 0	
Dislikes 0	

Response
Thank you for the comment, please see response to EEI.

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC

Answer	
Document Name	

Comment
Jump Server comment. Technical guidance diagrams. Within the Technical Guidance diagrams there is a concern on Figure 3 and Figure 4 concerning if both diagrams are approved configurations or if figure 3 is an incorrect configuration and Figure 4 is an appropriate configuration. Additionally, in Figure 4 there needs to be a key for the line colors and a DMZ designation. Several projects were/are modifying CIP-003 in parallel (2016-02, 2020-03 and 2023-04) and a different approach is used in dealing with the previous Technical Rationale content. For example, in Project 2023-04, hyperlinks to the previous TRs are added in the document, whereas in 2016-02, information from the previous TRs is kept and information was added related to the 2016-02 changes. Furthermore, the recently approved CIP-003-9 TR filed with the 2020-03 project contained only 8 pages from the initial 32 pages. These 8 pages consisted only the changes regarding the -9 version. In summary, three different projects modifying the CIP-003 and its TR with three different approaches. As a general comment, it would be helpful to the industry for the NERC SDTs to choose a way going forward that is applied across all NERC projects. In the case of the TR in this project, we suggest keeping one TR that includes the previous versions of the TR, as was done in the 2016-02 project.

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Changes have been made to clarify the Technical Rationale. The SDT believes the changes made address your comments. The TR written by 2016-02 contains the historical TR for previous versions of the standard. Prior to final ballot, the DT for 2023-04 will combine both TR files and retain the historical TR.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	
Document Name	
Comment	
We would like to thank the SDT for their hard work and dedication to this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	

Response	
Thank you for the comment, please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is responding in alignment with the comments from the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	

Answer	
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to NPCC Regional Standards Committee.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
See EEI Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	

In general, it seems that the SDT has expanded the requirements beyond what was recommended by the LICRT. For example, the LICRT stated there should be a requirement for the "detection of malicious communications to/between assets containing low-impact BES Cyber Systems with ERC." This language allows greater flexibility in determining the location of detection compared to the SDT's specification of "for both inbound and outbound electronic access." Given that access is defined by communication "outside the asset containing low-impact BES Cyber System(s)," this language inherently mandates the detection to occur at the border of the low-impact asset.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The verbiage "both inbound and outbound" and "outside the asset containing low-impact BES Cyber System(s)" is included in the currently approved CIP-003-9 Standard. The SDT has reused this verbiage to consistently address all remote access (in addition to vendor remote access addressed in CIP-003-9) to satisfy the revisions necessary to address the SAR. The SDT has made further revisions in Section 3 to clarify.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	
Mohamed Derbas - Sempra - San Diego Gas and Electric - 1	

Answer	
Document Name	
Comment	
SDG&E supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment, please see response to EEI.	

End of Report

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reminder
Standards Announcement
Project 2023-04 Modifications to CIP-003

Additional Ballots and Non-binding Poll Open through March 14, 2024

Now Available

Additional ballots for draft two of **CIP-003-A – Cyber Security – Security Management Controls** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels are open through **8 p.m. Eastern, Thursday, March 14, 2023.**

The standard drafting team's considerations of the responses received from the last comment period are reflected in this draft of the standard.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Balloting

Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here.

Note: Votes cast in previous ballots, will not carry over to additional ballots. It is the responsibility of the registered voter in the ballot pools to place votes again. To ensure a quorum is reached, if you do not want to vote affirmative or negative, cast an abstention.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Chris Larson (via email) or at 404-446-9708. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003 observer list” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-04 Modifications to CIP-003

Formal Comment Period Open through March 14, 2024

Now Available

A 45-day formal comment period for draft two of **CIP-003-A – Cyber Security – Security Management Controls**, is open through **8 p.m. Eastern, Thursday, March 14, 2023.**

The standard drafting team's considerations of the responses received from the previous comment period are reflected in this draft of the standard.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An additional ballot for the standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **March 5 - 14, 2024**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Chris Larson (via email) or at 404-446-9708. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003 observer list” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/314)
Ballot Name: 2023-04 Modifications to CIP-003 CIP-003-A AB 2 ST
Voting Start Date: 3/5/2024 12:01:00 AM
Voting End Date: 3/14/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 266
Total Ballot Pool: 292
Quorum: 91.1
Quorum Established Date: 3/14/2024 12:19:12 PM
Weighted Segment Value: 60.34

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	83	1	45	0.672	22	0.328	0	9	7
Segment: 2	6	0	0	0	0	0	0	5	1
Segment: 3	62	1	38	0.679	18	0.321	0	4	2
Segment: 4	16	1	6	0.462	7	0.538	0	1	2
Segment: 5	77	1	34	0.531	30	0.469	0	5	8
Segment: 6	40	1	19	0.576	14	0.424	0	3	4
Segment: 7	1	0	0	0	0	0	0	0	1
Segment: 8	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	4	0.4	1	0.1	0	1	1
Totals:	292	5.5	146	3.319	92	2.181	0	28	26

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Corn Belt Power Cooperative	Larry brusseau		Abstain	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Negative	Comments Submitted
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy	Brian Lindsey		Negative	Comments Submitted
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	JEA	Joseph McClung		Negative	Third-Party Comments
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Third-Party Comments
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	LS Power Transmission, LLC	Jennifer Richardson		Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Nikki Carson-Marquis	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Daniel Valle		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Pedernales Electric Cooperative, Inc.	Bradley Collard		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Platte River Power Authority	Marissa Archie		Negative	Third-Party Comments
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Matthew Jaramilla	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Olivia Olson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southwestern Power Administration	Angela Wheat		Abstain	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Unisource - Tucson Electric Power Co.	Jessica Cordero		None	N/A
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Abstain	N/A
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	BC Hydro and Power Authority	Ming Jiang		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Negative	Third-Party Comments
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Negative	Comments Submitted
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Negative	Comments Submitted
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lakeland Electric	Steven Marshall		Negative	Third-Party Comments
3	Los Angeles Department of Water and Power	Fausto Serratos		Abstain	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	Manitoba Hydro	Mike Smith		Affirmative	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Negative	Comments Submitted
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Owensboro Municipal Utilities	William Berry		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Tri-State G and T Association, Inc.	Ryan Walter		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		Abstain	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Negative	Comments Submitted
4	Illinois Municipal Electric Agency	Mary Ann Todd		Negative	Third-Party Comments
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Affirmative	N/A
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Negative	Comments Submitted
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
4	Utility Services, Inc.	Carver Powers		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	AES - AES Corporation	Ruchi Shah		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	American Municipal Power	Amy Ritts		Negative	Third-Party Comments
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	Basin Electric Power Cooperative	Amanda Wangler		None	N/A
5	BC Hydro and Power Authority	Quincy Wang		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier	Carly Miller	Affirmative	N/A
5	Bonneville Power Administration	Pamela Van Calcar		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Negative	Third-Party Comments
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar	Jamie Monette	Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Decatur Energy Center LLC	Megan Melham		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Comments Submitted
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	None	N/A
5	Great River Energy	Jacalynn Bentz		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	JEA	John Babik		Negative	Third-Party Comments
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Robert Kerrigan		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		Negative	Comments Submitted
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Robin Berry		Negative	Third-Party Comments
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NextEra Energy	Richard Vendetti		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Reid Cashion	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Abstain	N/A
5	Pattern Operators LP	George E Brown		Affirmative	N/A
5	Pine Gate Renewables	Michiko Sell		None	N/A
5	Platte River Power Authority	Jon Osell		Negative	Third-Party Comments
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		Negative	Comments Submitted
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Don Cribb		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Comments Submitted
5	Tennessee Valley Authority	Darren Boehm		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	TransAlta Corporation	Ashley Scheelar	Adam Burlock	Abstain	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Clarice Zellmer		Abstain	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman	Brandon Smith	Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Imane Mrini		None	N/A
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco	Jamie Monette	Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Entergy	Julie Hall	Kristen Long	None	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Negative	Third-Party Comments
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Powerex Corporation	Raj Hundal		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		Negative	Comments Submitted
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		None	N/A
10	Midwest Reliability Organization	Mark Flanary		Negative	Comments Submitted
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 292 of 292 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/314)
Ballot Name: 2023-04 Modifications to CIP-003 Implementation Plan AB 2 OT
Voting Start Date: 3/5/2024 12:01:00 AM
Voting End Date: 3/14/2024 8:00:00 PM
Ballot Type: OT
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 266
Total Ballot Pool: 293
Quorum: 90.78
Quorum Established Date: 3/14/2024 12:19:29 PM
Weighted Segment Value: 60.95

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	84	1	43	0.662	22	0.338	0	11	8
Segment: 2	6	0	0	0	0	0	0	5	1
Segment: 3	63	1	38	0.667	19	0.333	0	3	3
Segment: 4	16	1	7	0.538	6	0.462	0	1	2
Segment: 5	77	1	34	0.548	28	0.452	0	7	8
Segment: 6	40	1	17	0.515	16	0.485	0	3	4
Segment: 7	1	0	0	0	0	0	0	0	1
Segment: 8	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.3	3	0.3	0	0	0	3	0
Totals:	293	5.3	142	3.23	91	2.07	0	33	27

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Corn Belt Power Cooperative	Larry brusseau		Abstain	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Negative	Comments Submitted
1	Duke Energy	Katherine Street		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Edison International - Southern California Edison Company	Robert Blackney		Negative	Comments Submitted
1	Entergy	Brian Lindsey		Negative	Comments Submitted
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	JEA	Joseph McClung		Negative	Third-Party Comments
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Third-Party Comments
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	LS Power Transmission, LLC	Jennifer Richardson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Nikki Carson-Marquis	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Daniel Valle		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pedernales Electric Cooperative, Inc.	Bradley Collard		None	N/A
1	Platte River Power Authority	Marissa Archie		Negative	Third-Party Comments
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Matthew Jaramilla	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Olivia Olson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southwestern Power Administration	Angela Wheat		Abstain	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Unisource - Tucson Electric Power Co.	Jessica Cordero		None	N/A
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Negative	Third-Party Comments
2	California ISO	Darcy O'Connell		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Abstain	N/A
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	BC Hydro and Power Authority	Ming Jiang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Entergy	James Keele		Negative	Comments Submitted
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Third-Party Comments
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	Manitoba Hydro	Mike Smith		Affirmative	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Negative	Comments Submitted
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Tri-State G and T Association, Inc.	Ryan Walter		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		Abstain	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Negative	Comments Submitted
4	Illinois Municipal Electric Agency	Mary Ann Todd		Negative	Third-Party Comments
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Affirmative	N/A
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Negative	Comments Submitted
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	AES - AES Corporation	Ruchi Shah		None	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	American Municipal Power	Amy Ritts		Negative	Third-Party Comments
5	APS - Arizona Public Service Co.	Andrew Smith		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	Basin Electric Power Cooperative	Amanda Wangler		None	N/A
5	BC Hydro and Power Authority	Quincy Wang		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier	Carly Miller	Affirmative	N/A
5	Bonneville Power Administration	Pamela Van Calcar		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar	Jamie Monette	Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Negative	Third-Party Comments
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Decatur Energy Center LLC	Megan Melham		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Comments Submitted
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	None	N/A
5	Great River Energy	Jacalynn Bentz		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	JEA	John Babik		Negative	Third-Party Comments
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Robert Kerrigan		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		Negative	Comments Submitted
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Robin Berry		Negative	Third-Party Comments
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NextEra Energy	Richard Vendetti		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Reid Cashion	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		Affirmative	N/A
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Abstain	N/A
5	Pattern Operators LP	George E Brown		Affirmative	N/A
5	Pine Gate Renewables	Michiko Sell		None	N/A
5	Platte River Power Authority	Jon Osell		Negative	Third-Party Comments
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		Negative	Comments Submitted
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Don Cribb		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Comments Submitted
5	Tennessee Valley Authority	Darren Boehm		Negative	Comments Submitted
5	TransAlta Corporation	Ashley Scheelar	Adam Burlock	Abstain	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Clarice Zellmer		Abstain	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Third-Party Comments
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman	Brandon Smith	Negative	Comments Submitted
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Imane Mrini		None	N/A
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco	Jamie Monette	Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Entergy	Julie Hall	Kristen Long	None	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Negative	Third-Party Comments
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Powerex Corporation	Raj Hundal		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
6	Xcel Energy, Inc.	Steve Szablya		Negative	Third-Party Comments
7	Amazon Web Services	Maggy Powell		None	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 293 of 293 entries

BALLOT RESULTS

Ballot Name: 2023-04 Modifications to CIP-003 CIP-003-A | Non-binding Poll AB 2 NB
Voting Start Date: 3/5/2024 12:01:00 AM
Voting End Date: 3/14/2024 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 244
Total Ballot Pool: 280
Quorum: 87.14
Quorum Established Date: 3/14/2024 1:14:10 PM
Weighted Segment Value: 60.1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	38	0.679	18	0.321	15	9
Segment: 2	6	0	0	0	0	0	5	1
Segment: 3	59	1	31	0.674	15	0.326	8	5
Segment: 4	16	1	5	0.417	7	0.583	1	3
Segment: 5	74	1	27	0.509	26	0.491	9	12
Segment: 6	38	1	14	0.519	13	0.481	6	5
Segment: 7	1	0	0	0	0	0	0	1
Segment: 8	0	0	0	0	0	0	0	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	6	0.4	4	0.4	0	0	2	0
Totals:	280	5.4	119	3.197	79	2.203	46	36

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		None	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Corn Belt Power Cooperative	Larry brusseau		Abstain	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Negative	Comments Submitted
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A
1	Entergy	Brian Lindsey		Negative	Comments Submitted
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	JEA	Joseph McClung		Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	LS Power Transmission, LLC	Jennifer Richardson		Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Nikki Carson-Marquis	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Daniel Valle		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Pedernales Electric Cooperative, Inc.	Bradley Collard		None	N/A
1	Platte River Power Authority	Marissa Archie		Negative	Comments Submitted
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Matthew Jaramilla	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Abstain	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Olivia Olson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southwestern Power Administration	Angela Wheat		Abstain	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Unisource - Tucson Electric Power Co.	Jessica Cordero		None	N/A
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
2	California ISO	Darcy O'Connell		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Abstain	N/A
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	BC Hydro and Power Authority	Ming Jiang		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	None	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Negative	Comments Submitted
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Ryan Walter		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		Abstain	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Illinois Municipal Electric Agency	Mary Ann Todd		Negative	Comments Submitted
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Affirmative	N/A
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Negative	Comments Submitted
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
4	Utility Services, Inc.	Carver Powers		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		None	N/A
5	AEP	Thomas Foltz		None	N/A
5	AES - AES Corporation	Ruchi Shah		None	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	Basin Electric Power Cooperative	Amanda Wangler		None	N/A
5	BC Hydro and Power Authority	Quincy Wang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier	Carly Miller	Affirmative	N/A
5	Bonneville Power Administration	Pamela Van Calcar		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Negative	Comments Submitted
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar	Jamie Monette	Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Decatur Energy Center LLC	Megan Melham		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Comments Submitted
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	None	N/A
5	Great River Energy	Jacalynn Bentz		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	JEA	John Babik		Negative	Comments Submitted
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Brittany Millard		Abstain	N/A
5	Los Angeles Department of Water and Power	Robert Kerrigan		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Robin Berry		Negative	Comments Submitted
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NextEra Energy	Richard Vendetti		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Reid Cashion	Scott Brame	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		Affirmative	N/A
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Abstain	N/A
5	Pattern Operators LP	George E Brown		Affirmative	N/A
5	Pine Gate Renewables	Michiko Sell		None	N/A
5	Platte River Power Authority	Jon Osell		Negative	Comments Submitted
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG Nuclear LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		Negative	Comments Submitted
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Santee Cooper	Don Cribb		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Comments Submitted
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	TransAlta Corporation	Ashley Scheelar	Adam Burlock	Abstain	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Clarice Zellmer		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman	Brandon Smith	Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Imane Mrini		None	N/A
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco	Jamie Monette	Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Entergy	Julie Hall	Kristen Long	None	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Shelly Dineen		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	Powerex Corporation	Raj Hundal		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		Negative	Comments Submitted
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Abstain	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
7	Amazon Web Services	Maggy Powell		None	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 280 of 280 entries

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard for a 30-day formal comment period with additional ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023
45-day formal comment period with initial ballot	October 24 – December 7, 2023
45-day formal comment period with additional ballot	January 30 – March 14, 2024

Anticipated Actions	Date
30-day formal comment period with additional ballot	June 12 – July 11, 2024
10-day final ballot	July 2024
Board adoption	August 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

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

2. **Number:** CIP-003-11

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-003-11:

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

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

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

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

5. Effective Dates: See Implementation Plan for CIP-003-11.

B. Requirements and Measures

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

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

1.1.1. Personnel and training (CIP-004);

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

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

1.1.4. System security management (CIP-007);

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

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

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

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

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

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

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

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

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

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

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

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

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

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

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

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

C. Compliance

1. Compliance Monitoring Process

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

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

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

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

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

Violation Severity Levels

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

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the six topics required by Requirement R1. (Part1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part1.2) OR The Responsible Entity did not complete its approval of the	16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the six topics required by Requirement R1. (Part1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part1.2) OR The Responsible Entity did not complete its approval of the	17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the six topics required by Requirement R1. (Part1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part1.2) OR The Responsible Entity did not complete its approval of the	Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part1.1) OR The Responsible Entity did not address four or more of the six topics required by Requirement R1. (Part1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1. (Part1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part1.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part1.2)	one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part1.2)	one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part1.2)	
R2.	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document the electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to implement one or two controls listed in Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to implement three or more controls listed in Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code	notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	
R3.	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity -did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4.	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2023-04
- CIP-003-11 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from

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

Version	Date	Action	Change Tracking
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
11	TBD	Adopted by the NERC Board of Trustees.	TBD

Attachment 1

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

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

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

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

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented in Section 3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, where electronic access is:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

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

the Responsible Entity shall implement one or more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic access;

3.1.3 Authenticate each user prior to permitting access to a network(s) containing low impact BES Cyber Systems, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted;

3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BES Cyber System(s);

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement one or more control(s) that authenticates all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

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

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

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

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

4.4 Incident handling for Cyber Security Incidents;

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

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

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

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

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

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

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

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

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

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

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Attachment 2

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

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

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

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

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

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

1. For Section 3.1.1, documentation showing the permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, such as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
   - Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways); or
   - Original Equipment Manufacturer (OEM) specification sheets that

provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
    - Anti-malware technologies;
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - Monitor or alert for changes to communication baselines;
    - Logging and alerting configuration for Security Incident and Event Management (SIEM) systems or other event correlation systems;
    - Automated or manual log reviews;
    - Alerting; or
    - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate each user prior to permitting access to a network(s) containing low impact BES Cyber Systems, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted, such as:
    - Authentication mechanism(s) including but not limited to:
        - Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or
        - Enforcement of Multi-Factor Authentication (MFA).
    - Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
    - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BES Cyber System; or
    - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and
    - the authentication system used to meet Section 3.1.3, or
    - the asset containing low impact BES Cyber System(s),

    such as:
    - Protection mechanism(s) including but not limited to:
        - Implementation of an encrypted protocol or service (Hypertext

Transfer Protocol Secure (HTTPS), Secure Shell (SSH), etc.); or

- Implementation of an IPsec or Secure Sockets Layer (SSL) VPN.
- Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
    - Steps to preauthorize access;
    - Alerts generated by vendor log on;
    - Session monitoring;
    - Security information management logging alerts;
    - Time-of-need session initiation;
    - Session recording;
    - System logs; or
    - Other operational, procedural, or technical controls.
6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
    - Disabling vendor electronic access user or system accounts;
    - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic access;
    - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
    - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
    - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or
    - Other operational, procedural, or technical controls.
7. For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

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

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

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

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

   Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not

limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

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

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard for a 30-day formal comment period with additional ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023
45-day formal comment period with initial ballot	October 24 – December 7, 2023
45-day formal comment period with additional ballot	January 30 – March 14, 2024

Anticipated Actions	Date
30-day formal comment period with additional ballot	June 12 – July 11, 2024
10-day final ballot	July 2024
Board adoption	August 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

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

2. **Number:** CIP-003-~~A~~11

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-003-~~9~~11:

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

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

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

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

5. Effective Dates: See Implementation Plan for CIP-003-~~A~~11.

B. Requirements and Measures

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

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

1.1.1. Personnel and training (CIP-004);

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

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

1.1.4. System security management (CIP-007);

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

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

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

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

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

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

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

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents~~;~~, revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records, and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address one of the nine topics required by Requirement R1. (~~R1~~Part1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (~~R1~~Part1.1) OR The Responsible Entity did not complete its approval of the	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address two of the nine topics required by Requirement R1. (~~R1~~Part1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (~~R1~~Part1.1) OR The Responsible Entity did not complete its approval of the	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address three of the nine topics required by Requirement R1. (~~R1~~Part1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (~~R1~~Part1.1) OR The Responsible Entity did not	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address four or more of the nine topics required by Requirement R1. (~~R1~~Part1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1. (~~R1~~Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (~~R1~~Part1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the six topics required by Requirement R1. (~~R1~~Part1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (~~R1~~Part1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the six topics required by Requirement R1. (~~R1~~Part1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar	complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the six topics required by Requirement R1. (~~R1~~Part1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 17 calendar months but did complete this review in less	complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (~~R1~~Part1.1) OR The Responsible Entity ~~documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but~~ did not address four or more of the six topics required by Requirement R1. (~~R1~~Part1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1. (~~R1~~Part1.2) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (~~R1~~Part1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (~~R1~~Part1.2)	months of the previous review. (~~R1~~Part1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (~~R1~~Part1.2)	than or equal to 18 calendar months of the previous review. (~~R1~~Part1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (~~R1~~Part1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (~~R1~~Part1.2)
R2.	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity ~~implemented all electronic access controls, but~~ failed to	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity ~~documented its cyber security~~	The Responsible Entity ~~documented the physical access controls for its assets containing low impact BES Cyber Systems, but~~ failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for electronic access controls for its assets~~	The Responsible Entity failed to document and implement one or more cyber security plan(s) ~~for its assets containing low impact BES Cyber Systems~~ according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	document the electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR ~~The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to	~~plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for electronic access controls, but~~ failed to implement one or two controls listed in Requirement R2, Attachment 1, Section 3. (Requirement R2) OR ~~The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~The Responsible Entity failed to include the process for identification, classification,	~~containing low impact BES Cyber Systems, but~~ failed to implement three or more controls listed in Requirement R2, Attachment 1, Section ~~2. (~~3. (Requirement R2) OR ~~The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~The Responsible Entity failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but~~ failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity~~-documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity~~-documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity~~-documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3.	1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity~~-documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		(Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has identified by name a CIP Senior Manager, but did~~ not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has~~ did not ~~identified~~identify, by name, a CIP Senior Manager. OR The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4.	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has used delegated authority for actions where allowed by the CIP Standards, but~~ does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2023-04
- CIP-003-11 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from

Version	Date	Action	Change Tracking
			Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	

Version	Date	Action	Change Tracking
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
~~A~~11	TBD	Adopted by the NERC Board of Trustees.	TBD

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented in Section 3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, where electronic access is:

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive communications of Protection Systems~~,~~;

the Responsible Entity shall implement ~~a control(s)~~one or more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic access;

3.1.3 Authenticate ~~users when~~ each user prior to permitting ~~each user-initiated instance of electronic~~ access to a network(s) containing low impact BES Cyber Systems~~;~~, through which user-initiated electronic access applicable to Section 3.1 is

subsequently permitted;

3.1.4 Protect user authentication information for ~~each~~ user-initiated ~~instance of~~ electronic access applicable to Section 3.1.3 while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BES Cyber System(s);

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement ~~a~~one or more control(s) that authenticates all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the

introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. For Section 3.1.1, documentation showing the permittance of only inbound and outbound electronic access, where electronic access meets ~~the criteria specified in~~ Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, such as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
   - Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways); or

- Original Equipment Manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets ~~the criteria specified in~~ Section 3.1, Parts (i), (ii), and (iii), such as:
   - Anti-malware technologies;
   - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
   - Monitor or alert for changes to communication baselines;
   - Logging and alerting configuration for Security Incident and Event Management (SIEM) systems or other event correlation systems;
   - Automated or manual log reviews;
   - Alerting; or
   - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate ~~users when~~ each user prior to permitting ~~each user-initiated instance of electronic~~ access~~, where electronic access meets the criteria specified in Section 3.1,~~ to a network(s) containing low impact BES Cyber Systems, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted, such as:
   - Authentication mechanism(s) including but not limited to:
     - Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or
     - Enforcement of Multi-Factor Authentication (MFA).
   - Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
   - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BES Cyber System; or
   - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for ~~each~~ user-initiated ~~instance of~~ electronic access~~, where electronic access meets the criteria specified in~~ applicable to Section 3.1~~,~~.3 while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and
   - the authentication system used to meet Section 3.1.3, or
   - the asset containing low impact BES Cyber System(s),

such as:

- Protection mechanism(s) including but not limited to:
  - Implementation of an encrypted protocol or service (Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH), etc.); or
  - Implementation of an IPsec or Secure Sockets Layer (SSL) VPN.
  - Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets ~~the criteria specified in~~ Section 3.1, Parts (i), (ii), and (iii), such as:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;
   - Security information management logging alerts;
   - Time-of-need session initiation;
   - Session recording;
   - System logs; or
   - Other operational, procedural, or technical controls.
6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets ~~the criteria specified in~~ Section 3.1, Parts (i), (ii), and (iii), such as:
   - Disabling vendor electronic access user or system accounts;
   - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or
   - Other operational, procedural, or technical controls.
7. For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems,

modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a

party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard for a 30-day formal comment period with additional ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023
45-day formal comment period with initial ballot	October 24 – December 7, 2023
45-day formal comment period with additional ballot	January 30 – March 14, 2024

Anticipated Actions	Date
30-day formal comment period with additional ballot	June 12 – July 11, 2024
10-day final ballot	July 2024
Board adoption	August 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-~~9~~11

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-~~9~~11:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-~~9~~11.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets and Removable Media malicious code risk mitigation; and

~~**1.2.6.** Vendor electronic remote access security controls; and~~

~~**1.2.7.**~~**1.2.6.** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents~~;~~, revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security

plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with ~~the NERC~~mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records, and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels ~~(CIP-003-9)~~			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1. (~~R1~~Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by

R #	Violation Severity Levels ~~(CIP-003-9)~~			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the six topics required by Requirement R1. (Part1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part1.2) OR The Responsible Entity did not complete its approval of the	16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the six topics required by Requirement R1. (Part1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part1.2) OR The Responsible Entity did not complete its approval of the	17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address three of the six topics required by Requirement R1. (Part1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part1.2) OR The Responsible Entity did not complete its approval of the	Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part1.1) OR The Responsible Entity did not address four or more of the six topics required by Requirement R1. (Part1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1. (Part1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part1.2)

R #	Violation Severity Levels ~~(CIP-003-9)~~			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part1.2)	one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part1.2)	one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part1.2)	
R2.	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document the electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to implement one or two controls listed in Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to include the process for	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to implement three or more controls listed in Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels ~~(CIP-003-9)~~			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets	notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious	

R #	Violation Severity Levels ~~(CIP-003-9)~~			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	
R3.	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity -did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4.	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change.

R #	Violation Severity Levels ~~(CIP-003-9)~~			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				(Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2023-04
- CIP-003-11 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
11	TBD	Adopted by the NERC Board of Trustees.	TBD

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented ~~for~~in Section 3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, ~~the Responsible Entity shall implement~~where electronic access ~~controls to~~is:

~~**3.2** Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:~~

i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

iii. not used for time-sensitive ~~protection~~communications of Protection Systems;

the Responsible Entity shall implement one or ~~control functions between intelligent~~more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

~~**3.2.1**~~**3.1.1** Permit only necessary inbound and outbound electronic ~~devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).~~access as determined by the Responsible Entity;

3.1.2 ~~Authenticate~~Detect known or suspected malicious

communications for both inbound and outbound electronic access;

3.1.3 Authenticate each user prior to permitting access to a network(s) containing low impact BES Cyber Systems, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted;

3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BES Cyber System(s);

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

~~**3.3**~~**3.2** For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement one or more control(s) that authenticates all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s)

test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

~~**Section 6.** Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks~~

~~associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:~~

~~**6.1** One or more method(s) for determining vendor electronic remote access;~~

~~**6.2** One or more method(s) for disabling vendor electronic remote access; and~~

~~**6.3** One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.~~

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
  b. The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. ~~Documentation~~ For Section 3.1.1, documentation showing ~~that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside~~ the ~~asset is restricted by electronic access controls to permit~~permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, ~~except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of~~ such ~~documentation may include, but are not limited to representative~~as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s~~) or lists~~);

- Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways~~).~~); or
- ~~Documentation~~Original Equipment Manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Anti-malware technologies;
   - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
   - Monitor or alert for changes to communication baselines;
   - Logging and alerting configuration for Security Incident and Event Management (SIEM) systems or other event correlation systems;
   - Automated or manual log reviews;
   - Alerting; or
   - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate each user prior to permitting access to a network(s) containing low impact BES Cyber Systems, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted, such as:
   - Authentication mechanism(s) including but not limited to:
     - Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or
     - Enforcement of Multi-Factor Authentication (MFA).
   - Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
   - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BES Cyber System; or
   - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and
   - the authentication system used to meet Section 3.1.3, or
   - the asset containing low impact BES Cyber System(s),

   such as:

- Protection mechanism(s) including but not limited to:
  - Implementation of an encrypted protocol or service (Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH), etc.); or
  - Implementation of an IPsec or Secure Sockets Layer (SSL) VPN.
  - Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;
   - Security information management logging alerts;
   - Time-of-need session initiation;
   - Session recording;
   - System logs; or
   - Other operational, procedural, or technical controls.
6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Disabling vendor electronic access user or system accounts;
   - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or
   - Other operational, procedural, or technical controls.

~~2.~~7. For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or

process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset

does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

~~**Section 6.** Vendor Electronic Remote Access Security Controls: Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:~~

~~1. For Section 6.1, documentation showing:~~

- ~~steps to preauthorize access;~~
- ~~alerts generated by vendor log on;~~
- ~~session monitoring;~~
- ~~security information management logging alerts;~~
- ~~time-of-need session initiation;~~
- ~~session recording;~~
- ~~system logs; or~~
- ~~other operational, procedural, or technical controls.~~

~~2. For Section 6.2, documentation showing:~~

- ~~disabling vendor electronic remote access user or system accounts;~~
- ~~disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;~~
- ~~disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;~~
- ~~Removing physical layer connectivity (e.g., disconnect an Ethernet~~

~~cable, power down equipment);~~

- ~~administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or~~
- ~~other operational, procedural, or technical controls.~~

~~For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:~~

- ~~Anti-malware technologies;~~
- ~~Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);~~
- ~~Automated or manual log reviews;~~
- ~~alerting; or~~

~~other operational, procedural, or technical controls.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-04 Modifications to CIP-003
Reliability Standard CIP-003-11

Applicable Standard(s)

- CIP-003-11 – Cyber Security – Security Management Controls

Requested Retirement(s)

- CIP-003-9 – Cyber Security – Security Management Controls; or, if CIP-003-9 has been superseded, the version of the CIP-003 Reliability Standard then in effect[1]

Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

New/Modified/Retired Terms in the NERC Glossary of Terms

- None

Background

Project 2023-04 addresses modifications to CIP-003-9 in response to recommendations from the Low Impact Criteria Review Team (LICRT), which was formed by the NERC Board of Trustees to consider the potential threat and risk posed by a coordinated cyber-attack on low impact Bulk

[1] On May 9, 2024, the NERC Board of Directors approved the retirement of Reliability Standard CIP-003-9, which was scheduled to take effect on April 1, 2026, when it approved revised Reliability Standard CIP-003-10. CIP-003-10 is pending regulatory approval. This implementation plan is intended to retire whichever version of the CIP-003 Reliability Standard that is then in effect.

Electric System (BES) Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommended actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the standard authorization request (SAR) at its March 22, 2023 meeting. In response to the SAR, Project 2023-04 proposes merging Sections 3 and 6 of CIP-003-9, Attachment 1 and 2 to consolidate all electronic access requirements.

General Considerations

This implementation plan provides entities with thirty-six (36) months to become compliant with the revised Reliability Standard. This implementation plan reflects the following considerations for entities to implement the new controls of Requirement R2, Attachment 1:

- Revise cyber security policy, plan, and procedures.
- Hire and train new staff to implement the new cyber security controls.
- Reconfigure system, network, or security architectures.
- Purchase, procure, and install new technology(s).
- The effective date of CIP-003-9 is April 1, 2026. The cyber security controls implemented with CIP-003-11 do not conflict and build upon the implementation of CIP-003-9 for vendor electronic remote access.

Effective Date

Reliability Standard CIP-003-11

Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, "… at least once every 15 calendar months…"Responsible Entities shall comply initially with those periodic requirements in CIP-003-11 as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.3 on or before the effective date of CIP-003-11. Responsible Entities shall initially comply with all other periodic requirements in CIP-003-11 within the periodic timeframes of their last performance under CIP-003-9.

Retirement Date

Reliability Standard CIP-003-9

Reliability Standard CIP-003-9 shall be retired immediately prior to the effective date of CIP-003-11 in the jurisdiction in which the revised standard is becoming effective. If CIP-003-9 has been superseded by another version of Reliability Standard CIP-003, the currently effective version will be retired.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

CIP-003-12 is the combination of Project 2023-04's changes in on top of Project 2016-02's changes for virtualization. The following key describes the origin of changes in CIP-003-12:

Redline Text	Project 2023-04 original changes
Text	Project 2016-02 changes
Text	Project 2023-04 conforming changes to align with 2016-02 changes

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-~~10~~12

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-12~~0~~:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-12~~1~~.~~See "Project 2016-02 Modifications to CIP Standards Implementation Plan."~~

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

~~**1.2.6.** Vendor electronic remote access security controls; and~~

~~**1.2.7.**~~**1.2.6.** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS,

that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-12)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-12)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by Requirement R1. (Part1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part1.2) OR	impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1. (Part1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of

R #	Violation Severity Levels (CIP-003-12)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part1.2)	the previous approval. (Part1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-12)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the	according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Asset managed by the Responsible Entity according to Requirement R2, Attachment	

R #	Violation Severity Levels (CIP-003-12)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Asset managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment	1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote	

R #	Violation Severity Levels (CIP-003-12)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (Requirement R2)	access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60

R #	Violation Severity Levels (CIP-003-12~~0~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of the change. (Requirement R3)			calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project ~~2016-02~~2023-04
- CIP-003-1~~0~~ Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
10	TBD	Modified by Project 2016-02	
11	TBD	Modified by Project 2023-04	TBD

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: ~~For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the~~Each Responsible Entity shall ~~implement~~ control electronic access ~~controls to~~as outlined below.~~:~~

3.1 ~~Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are~~For each asset containing low impact BCS identified pursuant to CIP-002 or SCI that supports a low impact BCS, where electronic access is:

i. Between:

- a low impact BCS; or
- An SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:

- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems.

the Responsible Entity shall implement one or more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic access;

3.1.3 Authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted;

3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System(s) outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BCS or SCI that supports a low impact BCS;

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BCS identified pursuant to CIP-002 or SCI that supports a low impact BCS, the Responsible Entity shall implement one or more controls(s) that a~~A~~uthenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

~~**Section 6.** Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:~~

~~**6.1** One or more method(s) for determining vendor electronic remote access;~~

~~**6.2** One or more method(s) for disabling vendor electronic remote access; and~~

~~***6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.***~~

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. For Section 3.1.1, d~~D~~ocumentation showing ~~that at each asset or group of assets,~~ the ~~routable protocol communication as outlined in Section 3 is restricted by electronic access controls to~~ permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, ~~except where an entity provides rationale that communications are used for time-sensitive communications of Protection Systems. Examples of~~ such as: ~~documentation may include, but are not limited to~~

   - ~~r~~Representative diagrams that illustrate control of inbound and outbound communication(s) ~~or~~ between the low impact BCS or SCI that supports a low impact BCS and a Cyber System outside the asset containing low impact BCS.
   - ~~l~~Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways)~~.~~; or

- Original Equipment Manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1~~2~~.2~~1~~, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Anti-malware technologies;
   - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
   - Monitor or alert for changes to communication baselines;
   - Logging and alerting configuration for Security Incident and Event Management (SIEM) systems or other event correlation systems;
   - Automated or manual log reviews;
   - Alerting; or
   - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate each user prior to permitting access to a network(s) containing low impact ~~BES Cyber Systems,~~ BCS or SCI that supports a low impact BCS through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted, such as:
   - Authentication mechanism(s) including but not limited to:
     - Utilization of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), and/or similar implemented solutions; or
     - Enforcement of Multi-Factor Authentication (MFA).
   - Virtual Private Network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
   - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BES Cyber System; or
   - Other operational, procedural, or technical controls.

4. For Section 3.1.4, documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber ~~Asset~~System outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- The authentication system used to meet Section 3.1.3, or
- The asset containing low impact BCS or SCI that supports a low impact BCS,

such as:

- Protection mechanism(s) including but not limited to:
  - Implementation of an encrypted protocol or service (Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH), etc.);
  - Implementation of an IPsec or Secure Sockets Layer (SSL) VPN; or~~.~~
  - Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;
   - Security information management logging alerts;
   - Time-of-need session initiation;
   - Session recording;
   - System logs; or
   - Other operational, procedural, or technical controls.

6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Disabling vendor electronic access user or system accounts;
   - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or

- Other operational, procedural, or technical controls.

~~1.~~7. For Section 3.2, ~~D~~documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of system hardening performed

by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code

~~**Section 6.** Vendor Electronic Remote Access Security Controls: Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:~~

~~1. For Section 6.1, documentation showing:~~

- ~~steps to preauthorize access;~~
- ~~alerts generated by vendor log on;~~
- ~~session monitoring;~~
- ~~security information management logging alerts;~~
- ~~time-of-need session initiation;~~
- ~~session recording;~~
- ~~system logs; or~~
- ~~other operational, procedural, or technical controls.~~

~~2. For Section 6.2, documentation showing:~~

- ~~disabling vendor electronic remote access user or system accounts;~~
- ~~disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;~~
- ~~disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;~~
- ~~Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);~~
- ~~administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or~~
- ~~other operational, procedural, or technical controls.~~

3. ~~For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:~~
   - ~~Anti-malware technologies;~~
   - ~~Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);~~
   - ~~Automated or manual log reviews;~~
   - ~~alerting; or~~
   - ~~other operational, procedural, or technical controls.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-04 Modifications to CIP-003
Reliability Standard CIP-003-12

Applicable Standard(s)

- CIP-003-12 – Cyber Security – Security Management Controls

Requested Retirement(s)

- CIP-003-11 – Cyber Security – Security Management Controls

Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- CIP-003-11 – Cyber Security – Security Management Controls

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

New/Modified/Retired Terms in the NERC Glossary of Terms

- None

Background

Project 2016-02 proposed revisions to the suite of CIP standards, including the development of CIP-003-10, to incorporate virtualization. On May 9, 2024, the NERC Board of Trustees approved Reliability Standard CIP-003-10 and the retirement of Reliability Standard CIP-003-9, which was scheduled to take effect on April 1, 2026.

Project 2023-04 addresses modifications to CIP-003 in response to recommendations from the Low Impact Criteria Review Team (LICRT), which was formed by the NERC Board of Trustees to consider

the potential threat and risk posed by a coordinated cyber-attack on low impact Bulk Electric System (BES) Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommended actions to address those risks. The NERC Board of Trustees accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the standard authorization request (SAR) at its March 22, 2023 meeting. In response to the SAR, Project 2023-04 proposes merging Sections 3 and 6 of CIP-003-9, Attachment 1 and 2 to consolidate all electronic access requirements. The Project 2023-04 revisions were captured in Reliability Standard CIP-003-11.

Reliability Standard CIP-003-12 combines the changes proposed in CIP-003-10 and CIP-003-11 into a single CIP-003 Reliability Standard. It does not include any new revisions to CIP-003 beyond combining the two versions. Creating a single combined CIP-003 standard that reflects the work the Project 2016-02 and Project 2023-04 drafting teams is prudent because the projects overlapped in development, resulting in competing versions of CIP-003. Likewise, the required implementation plans for both versions should be aligned in a manner that preserves the intent of the respective drafting teams.

General Considerations

This implementation plan takes into account the overlapping implementation timelines for CIP-003-10 and CIP-003-11, which are combined into one implementation plan as discussed herein for Reliability Standard CIP-003-12. This implementation plan does not change or modify the early adoption provisions set forth in the implementation plan for CIP-003-10, nor does it change or modify the implementation plan set forth by Project 2016-02 for any other CIP Reliability Standard.

Early Adoption

With respect to the early adoption provisions set forth in the implementation plan for CIP-003-10, those provisions are hereby incorporated by reference into this implementation plan and will only apply to the CIP-003-10 revisions. The early adoption provisions, incorporated herein, will not apply to the revised language in CIP-003-11.

Effective Date

Reliability Standard CIP-003-12

Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is the later of: (1) thirty-six (36) months after the effective date of the applicable governmental authority's order approving Reliability Standard CIP-003-11; or (2) twenty-four (24) months after the effective date of the applicable governmental authority's order approving Reliability Standard CIP-003-12, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is the later of: (1) thirty-six (36) months after the date Reliability Standard CIP-003-11 is adopted by the NERC Board of Trustees; or (2) twenty-four (24) months after the date Reliability Standard CIP-003-12 is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and Responsible Entities shall comply initially with those periodic requirements in CIP-003-12 as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.3 on or before the effective date of CIP-003-12. Responsible Entities shall initially comply with all other periodic requirements in CIP-003-12 within the periodic timeframes of their last performance under the version of the CIP-003 Reliability Standard then in effect.

Retirement Date

Reliability Standard CIP-003

The currently effective version of Reliability Standard CIP-003 shall be retired immediately prior to the effective date of CIP-003-12 in the jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard
CIP-003-11 – Low Impact BES Cyber Security Criteria Revisions

Introduction
This document is the technical rationale and justification for Reliability Standard CIP-003-11 and includes the rationale for changes in the current proposed version, as well as previous versions of the standard.

It is intended to provide stakeholders and the ERO Enterprise with an understanding of the revisions, technology, and technical concepts of Reliability Standard CIP-003-11. This is not a Reliability Standard and should not be considered mandatory and enforceable.

Background
In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact Bulk Electric System (BES) Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts, representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber-attack on low impact BES Cyber Systems (LIBCS). In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the Standard Authorization Request (SAR) at its March 22, 2023 meeting.

The LICRT conclusions regarding LIBCS are as follows:

- Individually, LIBCS are truly low impact to BES reliability. This corresponds to the longstanding work of NERC and the stakeholders to design and operate the BES to withstand the loss of any of its individual assets. A medium or high impact BES Cyber System is more than an impact to a typical single BES Element/Facility. Therefore, the team does not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems.
- The team recognizes that LIBCS may introduce BES reliability risks of a higher impact where distributed LIBCS are used for a coordinated attack. The team recommends enhancing the existing low impact category to further mitigate the coordinated attack risk.

Those LICRT report recommendations are as follows:

- Requirement(s) for authentication of remote users before access is granted to networks containing LIBCS at assets containing those systems that have external routable connectivity.

- Requirement(s) for protection of user authentication information in transit for remote access to LIBCS at assets containing those systems that have external routable connectivity.
- Requirement(s) for detection of malicious communications to/between assets containing LIBCS with external routable connectivity.

Rationale for Attachment 1, Section 3 and Section 6

The drafting team's (DT) review of the SAR and industry comment initiated a discussion about the placement of requirements within CIP-003-11. CIP-003-9 was used as the baseline for revisions, since this version is the most recent version approved by FERC. Attachment 1, Section 3 and Attachment 1, Section 6 were identified as ideal locations to integrate the requirements due to their focus on electronic access controls and vendor electronic remote access security controls. The DT investigated two options:

Option A: Modify Sections 3 and 6, integrating the requirements, but keeping the sections separate.
Option B: Merge Sections 3 and 6.

The DT agreed to Option B: Merge Sections 3 and 6. The following rationale was used to support the decision:

1. Merging Section 3 and Section 6 would present a single section for all electronic access with sub-sections providing additional requirements based on the type of access (vendor, dial-up, local, etc.)
2. Section 6 has not been implemented or required by industry at this time and therefore there would be no impact to merging it with Section 3

While merging Section 3 and 6, the DT made conforming changes to the language. The DT uses the phrase "implement controls" to replace "implement a process" or "implement one or more method(s)". The DT believes a "control" can include an operation, process, procedure, or technology as described in the examples of Attachment 2. Additionally, the word "remote" was removed from the phrase "electronic remote access" as the section now covers all electronic access as described in Section 3, Part 3.1, (i), (ii), and (iii) as those define more specifically the remote nature of the in-scope access.

Glossary Terms

The DT also discussed the potential reintroduction of the retired NERC Glossary Term:, Low Impact External Routable Connectivity (LERC), or creating a new Glossary Term. The rationale for using LERC or a new term would be to provide a shorthand way of discussing external routable connectivity when dealing with assets containing LIBCS.

The DT decided to keep the language from the previous CIP-003-9 Attachment 1, Section 3.1 intact rather than creating a new NERC Glossary Term or reintroducing LERC. Rationale used for the decision:

1. Possible confusion with reintroducing the retired term LERC.
2. Possible friction with industry stakeholders with using a new term.
3. Actual requirement for LERC or a new term beyond Section 3.

To clarify scope of requirements for industry and regulators alike, the drafting team placed the requirements in Attachment 1 Section 3.1 into a logical "if, then" order to further clarify the three identifying low impact asset characteristics or conditions (romanettes i, ii, iii) when implementing controls.

Section 3.1

The objective of Section 3.1 is to maintain the original language used in CIP-003-9, Section 3.1, Subsections (i) - (iii). There is one revision to 3.1(iii) replacing the previous language concerning "intelligent electronic devices" with reference to the existing glossary term "Protection Systems" which is a conforming change to that made by Project 2016-02, CIP-003-10. Figure 1 provides a graphical representation of Section 3.1, Subsections (i)-(iii).

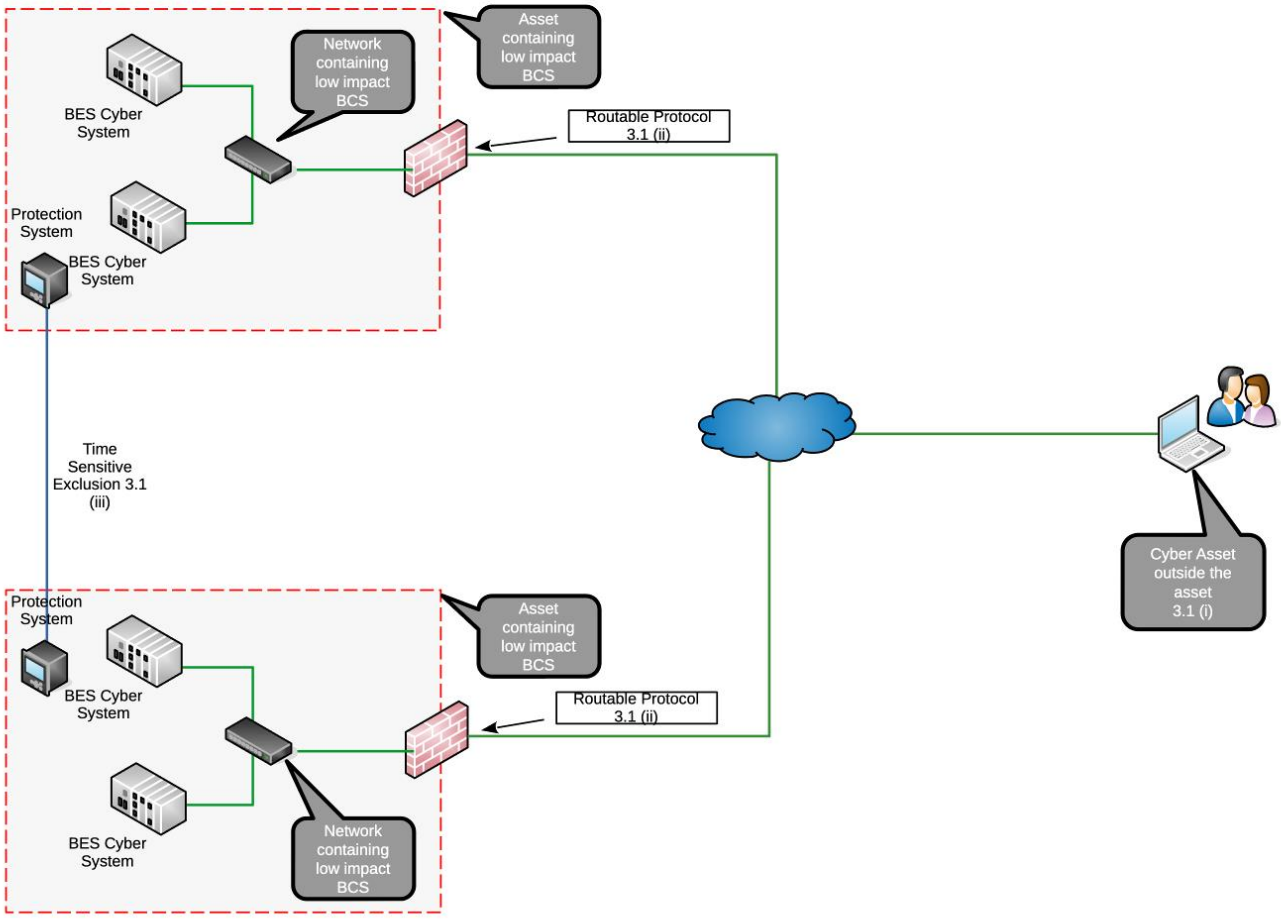


Figure 1

Section 3.1.1

The objective of Section 3.1.1 is to maintain the original language used in CIP-003-9, Section 3.1.

Section 3.1.2

This is an expanded cyber security control outlined in the SAR. The scope is expanded from CIP-003-9, Section 6.3 to include all communications rather than vendor specific communications. The objective of Attachment 1 Section 3.1.2 is for entities to mitigate the risk posed by malicious communications to or from LIBCS. The detection of known or suspected malicious communications can be accomplished in several ways. For example, Figure 2 below, depicts implementing the control (e.g., Intrusion Detection System (IDS)) in a centralized location (e.g., at a corporate hub site) rather than at every distributed "asset containing LIBCS" such as substations in this example "hub and spoke" model. The obligation in Section 3.1.2 requires that entities implement controls to detect known or suspected inbound and outbound malicious communications between a low impact BES Cyber System and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) thus allowing entity flexibility in where the control is implemented based on their architecture.

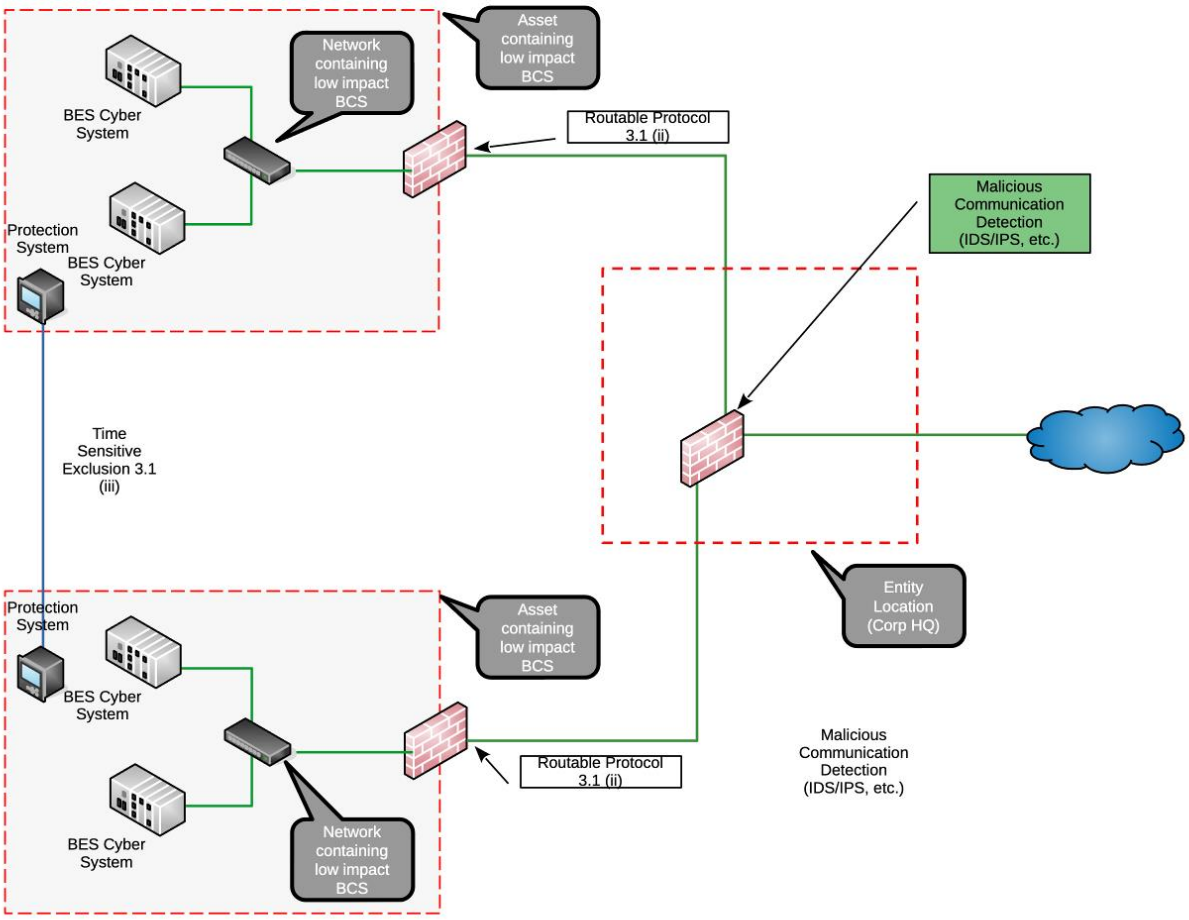


Figure 2

Section 3.1.3

This is a new cyber security control outlined in the SAR that requires entities to implement controls to authenticate users prior to permitting (allowing, establishing, gaining) access to networks containing LIBCS. This control mitigates the risk of unauthenticated access to networks on which LIBCS reside. The intent is for each user to be authenticated (verifying a user) *before* they gain access to the "network containing low impact BES Cyber Systems"; thus they have no ability to enumerate hosts on those networks, scan those networks for vulnerabilities, attempt logons to systems or perform actions on those networks and systems before the entity has authenticated their identity.

Figure 3, below, depicts a situation where the authentication of the remote user is not occurring "prior to" but after the user already has access to the "network containing LIBCS" — as the authentication servers are on the same network with the LIBCS. The firewall in this scenario allows the user through to the network on which the LIBCS reside before the user is authenticated, and this does not meet the intent of the requirement.

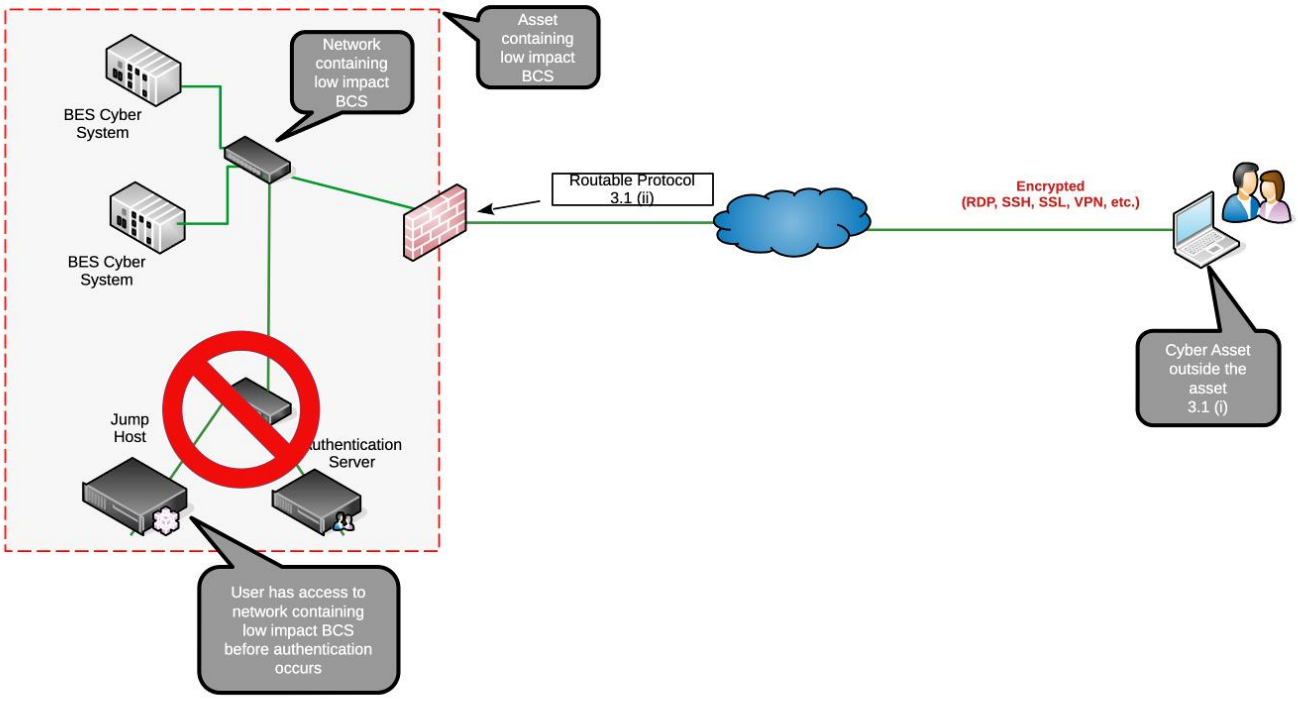


Figure 3

The intention of the phrase "each user prior to permitting access to a network(s)…" is meant to include the initial authentication and not all subsequent access to other downstream networks. If there is a collection of sub-networks or Cyber Assets within the network containing LIBCS, then multiple re-authentications at those levels would not be required by this specific requirement. Regardless of how many subsequent networks or BES Cyber Systems a user may access, as long as the entity's implemented control(s) have authenticated the user prior to their access to those subsequent networks, that meets the intent. This may include, but is not limited to configurations where authentication is local device specific authentication, or centralized authentication using technologies such as an access, terminal, or proxy server ("Intermediate System"), which processes authentication to the low impact asset networks through a centralized gateway.

The DT has not required the use of an "Intermediate System" as is prescribed in CIP-005 Requirement R2 for high and medium impact BES Cyber Systems. However, the DT's intent is that those entities who have established or implemented such infrastructure or technologies, may use them for authenticating access to the assets containing low impact BES Cyber Systems to satisfy these requirements. While prescribing such an architecture as in CIP-005 Requirement R2 would further clarify CIP-003's requirements, the DT has chosen not to prescribe such requirements due to the impact to a broad and diverse range of entities and their specific technologies and processes used to meet low impact BES Cyber Systems authentication requirements. For example, it would be excessive to require an entity with a single CIP-003 applicable renewable generation site to implement architectures and technologies (Intermediate Systems) to meet the CIP-005 Requirement R2 Interactive Remote Access requirements. Such an entity may only need a Secure Sockets Layer (SSL) VPN to an access control device (e.g., firewall) at the one site that authenticates the user prior to allowing access to the network containing low impact BES Cyber Systems on its inside interface. The entity may also choose to authenticate a local non-low impact BES Cyber Systems network first, then control access to the LIBCS from that access point. Conversely, an entity with many assets distributed over a large geographic area, with a variety of impact categorizations and supporting BES Cyber Systems, may want to use their existing CIP-005 R2 remote access solutions for all of their sites (centralized access controls). The DT's intent in the CIP-003 language is to allow flexibility for both cases.

The phrase, "through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted" is included in Section 3.1.3 to clarify scoping. As 3.1.3 is written at a different granularity of "network(s) containing" (which is not mentioned in the romanettes), this phrasing simply clarifies that the intended scope remains those networks through which the specific access described in the Section 3.1 romanettes is subsequently permitted. The romanettes (i), (ii), and (iii) in Section 3.1 define the ultimate access that is in scope, which is from a remote client outside the asset containing the LIBCS and destined for a LIBCS within the asset.

Section 3.1.4

This is a new cyber security control outlined in the SAR. The objective of Attachment 1, Section 3.1.4 is for entities to protect the user authentication information (e.g., username, password, multi-factor

authentication (MFA) information, session token, etc.) while in transit between the remote user's Cyber Asset and either the asset containing the low impact BES Cyber Systems or the entity's authentication system used to meet Section 3.1.3. This mitigates the risk of user authentication information being captured, especially as some BES equipment may still require protocols that transmit such information in clear text. The intent is not to specify authentication directly to a particular device but to allow entities that desire to use an existing compliant CIP-005 Requirement R2 Intermediate System, or similar architecture, access to networks containing LIBCS (Figure 4). For example, Figure 4 below depicts protection of the user authentication information to the asset containing a LIBCS.

Figure 5 depicts an alternative example of protecting the user authentication information to/from a central system (i.e. jump host) *before* accessing a network containing a LIBCS. This protection mitigates the unintended disclosure of authentication information for electronic access to low impact cyber systems.

Note that both Figure 4 and Figure 5 have a significant difference from Figure 3 above in that although the authentication services are also within the asset containing the LIBCS, they are located on a separate network from those containing BES Cyber Systems. In this example, assuming the firewall is configured to only allow authenticated user sessions on the jump host through to the network containing the LIBCS, this would meet the intent of the 3.1.3 requirement part.

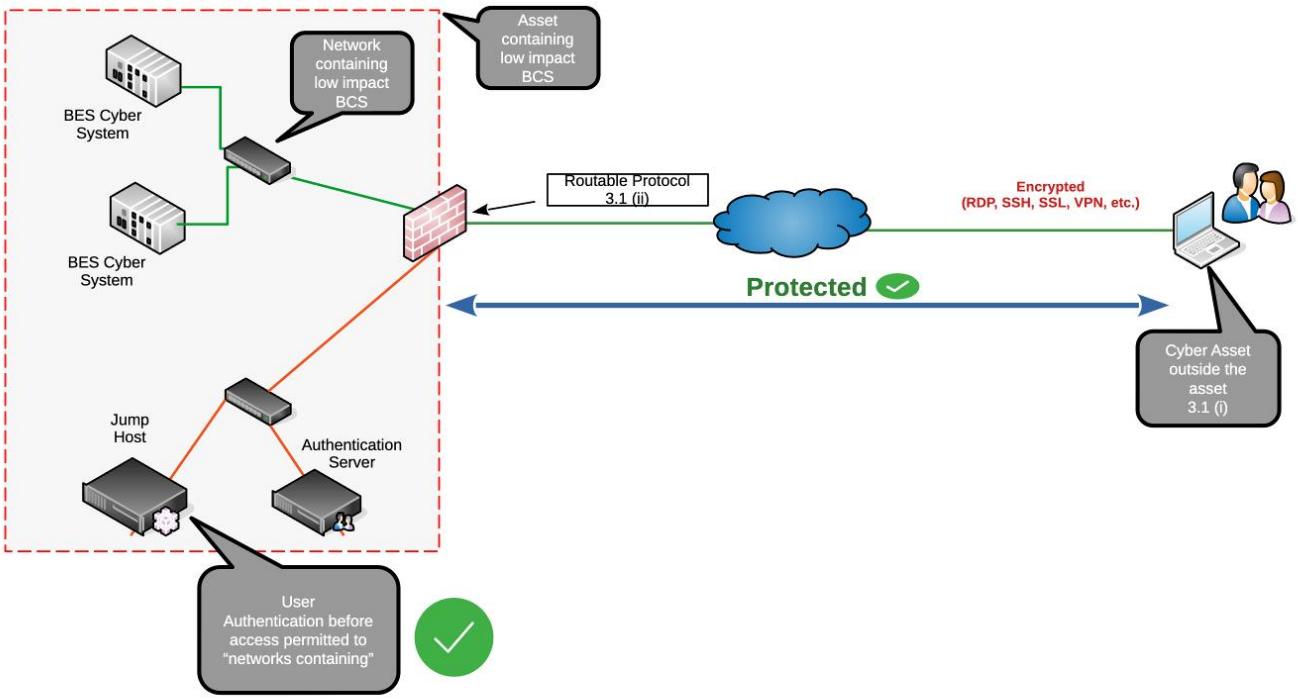

Asset containing low impact BCS
Network containing low impact BCS
BES Cyber System
BES Cyber System
Routable Protocol 3.1 (ii)
Encrypted (RDP, SSH, SSL, VPN, etc.)
Protected
Cyber Asset outside the asset 3.1 (i)
Jump Host
Authentication Server
User Authentication before access permitted to "networks containing"

Figure 4

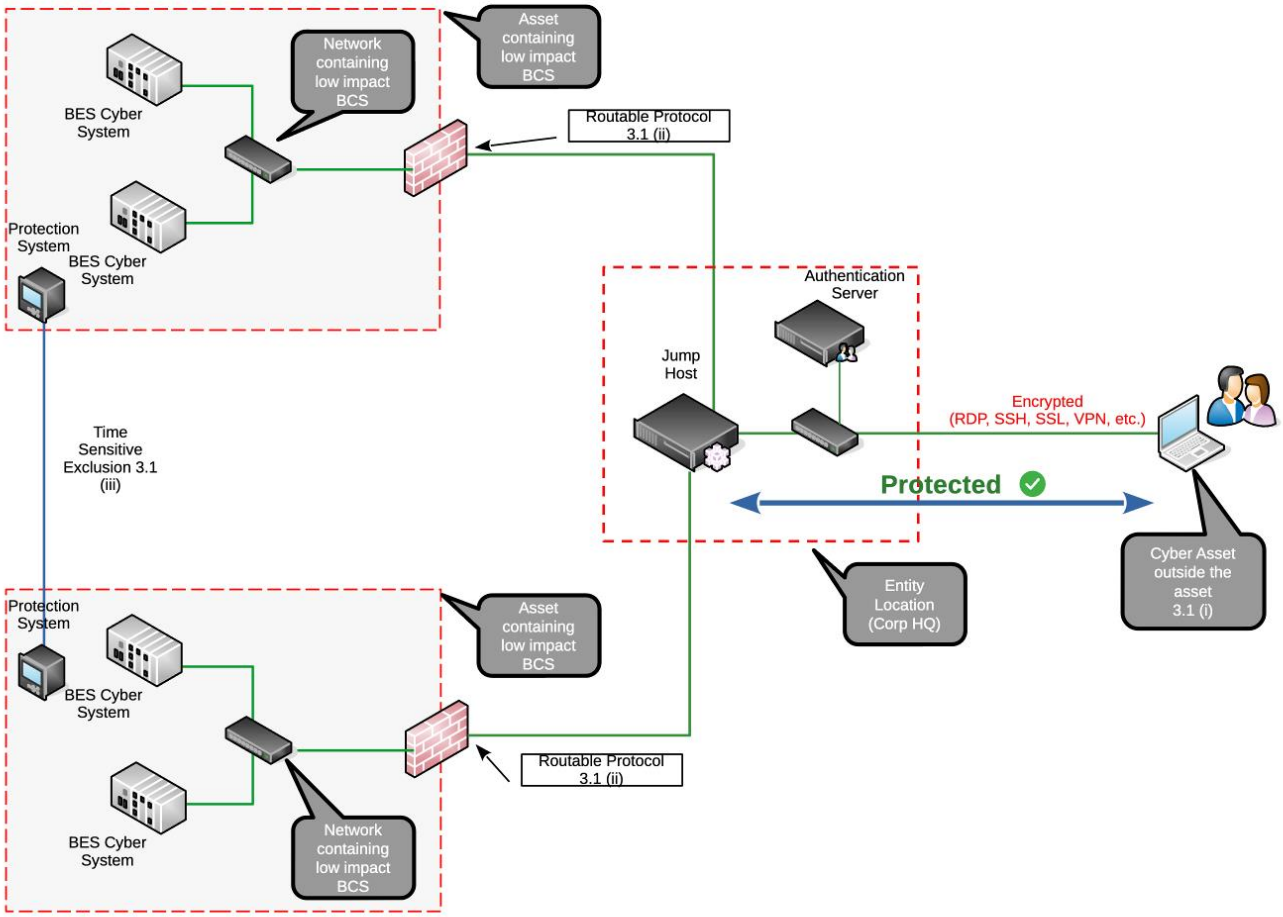


Figure 5

The DT has not required the use of an "Intermediate System" as is prescribed in CIP-005 Requirement R2 for high and medium impact BES Cyber Systems. However, the DT's intent is that those who have such infrastructures in place can, if they choose, use them for access to the assets containing low impact BES Cyber Systems as well, meeting the intent of these requirements. While prescribing such an architecture as in CIP-005 Requirement R2 would make the target of CIP-003's requirements clearer to describe, the DT has chosen not to prescribe it due to the wide diversity of entities that may have only LIBCS. For example, an entity may have one small renewable generation site that falls under CIP-003 and implementing a full CIP-005 Requirement R2 "Interactive Remote Access with Intermediate System" architecture for access to one site may be excessive. That entity may only need an SSL VPN to an access control device (e.g., firewall) at the one site that authenticates the user and then allows access to the network containing LIBCS on its inside interface. However, an entity with 100 assets with BES Cyber Systems of varying impact categorization over a large geographic area may want to use their CIP-005 Requirement R2 remote access solution for all of their sites. The DT's intent in the CIP-003 language is to allow flexibility for both.

Section 3.1.5

The objective of Section 3.1.5 is to maintain the original language used in CIP-003-9, Section 6.1. One or more method(s) can be identified as part of this electronic access control. Entities must determine vendor electronic remote access, where permitted, to their LIBCS. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access.

Section 3.1.6

The objective of Section 3.1.6 is to maintain the original language used in CIP-003-9, Section 6.2. One or more method(s) can be identified as part of this electronic access control. Entities must have the ability to disable vendor electronic remote access, where permitted, for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing LIBCS.

Section 3.2

The objective of Section 3.2 is to maintain the original intent of CIP-003-9, Section 3.2.

Special Scenarios

One low impact BES Cyber System across more than one asset containing that system.
In this scenario, a low impact BES Cyber System is not entirely located within one asset. For example, a generation resource has the majority of its BES Cyber System components within the site, but its network is extended full-time (e.g., over a dedicated circuit or dedicated B2B VPN) to an operator console located at another site, and the console is part of the single BES Cyber System.

Since the components of the BES Cyber System are all located in "assets containing low impact BES Cyber System", just not a single asset, then this scenario is not in scope as it does not meet the condition of Section 3.1(i) of "between a low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber System(s)." The intent of Section 3.1.3 is authentication of users who are not located within any other "assets containing low impact BES Cyber System." This keeps CIP-003 analogous to the same concept in CIP-005 and the Interactive Remote Access definition that excludes from Interactive Remote Access user access that originates in another of the entity's Electronic Security Perimeters, such that operators in Control Centers are not required to implement CIP-005 Requirement R2 controls such as Intermediate Systems to operate field assets. It also avoids CIP-003 becoming circular when a local user at the BES Cyber System console would need to authenticate prior to permitting access to the extended network they are already on while seated at the console.

Rationale for Attachment 2

The DT made conforming changes to Attachment 2 merging Sections 3 and 6 and provided examples of compliance related activities.

Previous CIP-003 Versions Technical Rationale

Project 2020-03 Supply Chain Low Impact Revisions (CIP-003-9) Technical Rationale
Project 2016-02 Modifications to CIP Standards (CIP-003-10) Technical Rationale

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2023-04 Modifications to CIP-003

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on draft three of Reliability Standard **CIP-003-11 – Cyber Security – Security Management Controls** by **8 p.m. Eastern, Thursday, July 11, 2024.**

Additional information is available on the project page. If you have questions, contact Manager, Standards Development, Alison Oswald (via email) or at 404-275-9410.

Background

In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact Bulk Electric System (BES) Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts who were representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the Standard Authorization Request (SAR) at its March 22, 2023 meeting.

The LICRT report recognized that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The LICRT recommended enhancing the existing low impact category to further mitigate the coordinated attack risk. The proposed project will revise CIP-003-9 to add electronic access controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications for assets containing low impact BES Cyber Systems with external routable connectivity.

Please provide your responses to the questions listed below, along with any detailed comments.

Questions

1. Do you agree with the language proposed in CIP-003-11 Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

2. Do you agree with the language proposed in CIP-003-11 Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

3. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-11. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.

   ☐ Yes
   ☐ No

   Comments:

4. The DT believes the language of CIP-003-11 addresses the issues outlined in the SAR in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

5. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.

   Comments:

   The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering the following questions.

6. Do you have any concerns in the way CIP-003-10 (Project 2016-02 changes) and CIP-003-11 (Project 2023-04 changes) were combined to create standard CIP-003-12?
   ☐ Yes
   ☐ No
   Comments:

7. Do you have any concerns in the CIP-003-12 implementation plan that should be addressed?
   ☐ Yes
   ☐ No
   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2023-04 Modifications to CIP-003

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2023-04 Modifications to CIP-003. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

Justification for VRFs and VSLs

- Requirement R1: There were no changes to VRFs from the previously FERC-approved CIP-003-9 Reliability Standard and only conforming or non-substantive changes to the VSLs.
- Requirement R2: The VRF did not change from the previously FERC-approved CIP-003-9 Reliability Standard. VSL changes are outlined below.
- Requirement R3: There were no changes to VRFs from the previously FERC-approved CIP-003-9 Reliability Standard and only conforming or non-substantive changes to the VSLs.
- Requirement R4: There were no changes to VRFs from the previously FERC-approved CIP-003-9 Reliability Standard and only conforming or non-substantive changes to the VSLs.

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document the electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2)	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security controls according to Requirement R2, Attachment 1,	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to implement three or more controls listed in Requirement R2, Attachment 1, Section 2. (Requirement R2)	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	Section 2. (Requirement R2) OR The Responsible Entity failed to implement one or two controls listed in Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code	OR The Responsible Entity failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code	

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

VSL Justifications for CIP-003-A, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSLs for Requirement R2 are similar to the previous VSLs of CIP-003-9, with a few revisions. Created Moderate and High VSL based on the number of controls implemented. Removed mentions of Attachment 1, Section 6, since Section 6 was merged with Section 3.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Requirement R2 is not a "binary" type requirement. Violation severity levels are clear, quantitative, and non-ambiguous.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The VSL level assignments are consistent with language in Requirement R2 and Attachment 1.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The violation severity levels relate to a single violation. A failure to do multiple portions of Requirement R2, Attachment 1 is considered a single violation.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Summary of Changes

Project 2023-04 Modifications to CIP-003
Reliability Standard CIP-003-11 and CIP-003-12

Background

Two drafting teams (2016-02 and 2023-04) were simultaneously working on modifications to CIP-003-9, the approved version of CIP-003 that included the low impact supply chain revisions.

- Project 2016-02 adding virtualization and other conforming changes to CIP-003-9.
- Project 2023-04 adding the recommendations from the Low Impact Criteria Review Team (LICRT) report.

Project 2016-02's work passed final ballot and was approved by the NERC Board in May, 2024 and became CIP-003-10 while Project 2023-04 was still in progress and became CIP-003-11. However, both were still based on the CIP-003-9 version.

Project 2023-04 is therefore also producing CIP-003-12, which is for illustrative purposes to show a combination of the -10 and -11 versions into one. In summary:

- Project 2016-02 changed -9 to create -10
- Project 2023-04 changed -9 to make -11
- Project 2023-04 has combined -10 and -11 to create -12

Project 2023-04 is posting both versions of CIP-003-11 and CIP-003-12 as well as corresponding Implementation Plans. As Project 2016-02's work is part of a large package consisting of changes to eleven CIP standards plus new and modified glossary terms and Project 2023-04 is making few changes to one section of Attachment 1 within CIP-003 only, it is unknown the speed or order in which these two versions of CIP-003 may achieve final regulatory approval in the future.

The two versions are being maintained and posted by Project 2023-04 such that either one can go forward based on the future approval timelines.

Summary of Changes in CIP-003-12

CIP-003-12 is the combination of Project 2023-04's changes in Attachment 1 on top of Project 2016-02's changes for virtualization. The conforming modifications that Project 2023-04 has made to Section 3 of Attachment 1 are:

- *The inclusion of Shared Cyber Infrastructure (SCI)*. As SCI is the underlying infrastructure of virtualized environments on which low impact BES Cyber Systems (BCS) may reside, changes have been made to add SCI as an option for both the origin and target of the access defined

and the controls required in CIP-003. Thus references to low impact BCS now include the phrase "or SCI that supports a low impact BCS".

- *References to "Cyber Asset" have been changed to "Cyber System"*. As Project 2016-02 defined new glossary terms for Virtual Cyber Assets (VCA) as well as SCI, that project also created "Cyber System" as a term to include all three forms of Cyber Asset, VCA, or SCI into one term.
- *Use of acronyms*. As the NERC Glossary of Terms includes official acronyms for many terms, conforming changes have been made from Project 2016-02's work of replacement of full terms (after first use in a standard) with its acronym as defined in the glossary, such as BCS in place of "BES Cyber System".

Key for Change Identifiers in CIP-003-12

The following key describes the origin of changes in CIP-003-12:

Redline Text	Project 2023-04 original changes
Text	Project 2016-02 changes
Text	Project 2023-04 conforming changes to align with 2016-02 changes

Implementation Plans

Along with the CIP-003-11 implementation plan, which is substantially similar to the implementation plan that was previously posted by the Project 2023-04 drafting team, the drafting team is also publishing a separate CIP-003-12 implementation plan. The CIP-003-12 implementation plan is associated with a version of CIP-003 that combines the revisions in CIP-003-10 with the revisions in CIP-003-11. As a result, it combines elements of the CIP-003-10 and CIP-003-11 implementation plans to help ensure that the timelines associated with the revisions in each version are maintained while providing governing authorities an option to approve only the revisions in CIP-003-11 or a standard combining revisions from both CIP-003-10 and CIP-003-11 (e.g., CIP-003-12).

The CIP-003-12 implementation plan would preserve the early adoption provisions that are contained in the CIP-003-10 implementation plan. Thus, it would continue to allow those entities that wish to take advantage of the virtualization changes earlier than that implementation plan's two year implementation timeframe for the CIP-003-10 changes. The early adoption provisions do not apply to the revisions contained in CIP-003-11. The CIP-003-12 implementation does not affect the implementation plan of any other Reliability Standard that was addressed by Project 2016-02.

In addition, the CIP-003-12 implementation plan proposes that the standard shall become effective on the first day of the first calendar quarter that is the later of: (1) thirty-six (36) months after the effective date of the applicable governmental authority's order approving Reliability Standard CIP-

003-11; or (2) twenty-four (24) months after the effective date of the applicable governmental authority's order approving Reliability Standard CIP-003-12, or as otherwise provided for by the applicable governmental authority. This proposal would allow entities to have, at a minimum, the 24 months that was established by Project 2016-02 for the CIP-003-10 revisions. Likewise, entities would be allowed, at least, the 36 months to comply with the CIP-003-11 changes, as previously proposed by the Project 2023-04 drafting team.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-04 Modifications to CIP-003

Formal Comment Period Open through July 11, 2024

Now Available

A **30-day** formal comment period for **CIP-003-11 – Cyber Security – Security Management Controls**, is open through **8 p.m. Eastern, Thursday, July 11, 2024**.

The third draft of CIP-003 is being posted for a 30-day formal comment and ballot period per the Standard Processes Manual Section 4.12.

Based on recent board adopted standards for CIP-003-9, the posted versions for the 2023-04 Modifications to CIP-003 was updated to reflect CIP-003-11. The Standards Balloting and Commenting System (SBS) does not allow edits once a ballot pool has been formed. Even though the standard versioning within the SBS states CIP-003-A, the version numbers within this posting are correct and entities will be voting on CIP-003-11 and CIP-003-12 in the same ballot.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in this draft of the standard.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*

- *Please be mindful of ballot and comment period closing dates. We ask to* ***allow at least 48 hours*** *for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts* ***prior to the last day*** *of a comment/ballot period.*

Next Steps

An additional ballot for the standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **July 2-11, 2024**.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Manager, Standards Development, Alison Oswald (via email) or at 404-275-9410. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003 observer list” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2023-04 Modifications to CIP-003 | Draft 3
Comment Period Start Date:	6/12/2024
Comment Period End Date:	7/11/2024
Associated Ballots:	2023-04 Modifications to CIP-003 CIP-003-A AB 3 ST 2023-04 Modifications to CIP-003 Implementation Plan AB 3 OT

There were 54 sets of responses, including comments from approximately 156 different people from approximately 92 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the language proposed in CIP-003-11 Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

2, Do you agree with the language proposed in CIP-003-11 Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

3. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-11. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.

4. The DT believes the language of CIP-003-11 addresses the issues outlined in the SAR in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical, or procedural justification.

5. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.

The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering this question.

6. Do you have any concerns in the way CIP-003-10 (Project 2016-02 changes) and CIP-003-11 (Project 2023-04 changes) were combined to create standard CIP-003-12?

The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering this question.

7. Do you have any concerns in the CIP-003-12 implementation plan that should be addressed?

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Husam Al-Hadidi	Manitoba Hydro (System Preformance)	1,3,5,6	MRO
					Kimberly Bentley	Western Area Power Adminstration	1,6	MRO
					Jaimin Patal	Saskatchewan Power Coporation (SPC)	1	MRO
					George Brown	Pattern Operators LP	5	MRO
					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Dane Rogers	Oklahoma Gas and Electric (OG&E)	1,3,5,6	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Ayotte	ITC Holdings	1	MRO
					Andrew Coffelt	Board of Public Utilities-Kansas (BPU)	1,3,5,6	MRO
					Peter Brown	Invenergy	5,6	MRO

					Angela Wheat	Southwestern Power Administration	1	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC
					Nehtisha Rollis	Tennessee Valley Authority	5	SERC
Santee Cooper	Carey Salisbury	5		Santee Cooper	Rodger Blakely	Santee Cooper	1,3,5,6	SERC
					Christine Pope	Santee Cooper	1,3,5,6	SERC
					Lachelle Brooks	Santee Cooper	1,3,5,6	SERC
					Rene' Free	Santee Cooper	1,3,5,6	SERC
					Bob Rhett	Santee Cooper	1,3,5,6	SERC
					Bridget Coffman	Santee Cooper	1,3,5,6	SERC
					Wanda Williams	Santee Cooper	1,3,5,6	SERC
					Jordan Steele	Santee Cooper	1,3,5,6	SERC
WEC Energy Group, Inc.	Christine Kane	3		WEC Energy Group	Christine Kane	WEC Energy Group	3	RF
					Matthew Beilfuss	WEC Energy Group, Inc.	4	RF
					Clarice Zellmer	WEC Energy Group, Inc.	5	RF
					David Boeshaar	WEC Energy Group, Inc.	6	RF
Manitoba Hydro	Jay Sethi	1,3,5,6	MRO	Manitoba Hydro Group	Nazra Gladu	Manitoba Hydro	1	MRO

					Mike Smith	Manitoba Hydro	3	MRO
					Kristy-Lee Young	Manitoba Hydro	5	MRO
					Kelly Bertholet	Manitoba Hydro	6	MRO
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					Tyler Brun	Pacific Gas and Electric Company	5	WECC

Black Hills Corporation	Rachel Schuldt	6		Black Hills Corporation - All Segments	Micah Runner	Black Hills Corporation	1	WECC
					Josh Combs	Black Hills Corporation	3	WECC
					Rachel Schuldt	Black Hills Corporation	6	WECC
					Carly Miller	Black Hills Corporation	5	WECC
					Sheila Suurmeier	Black Hills Corporation	5	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Deidre Altobell	Con Edison	1	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
					Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
					Randy Buswell	Vermont Electric Power Company	1	NPCC
					James Grant	NYISO	2	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					David Burke	Orange and Rockland	3	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC

					David Kwan	Ontario Power Generation	4	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
					Sean Cavote	PSEG	4	NPCC
					Jason Chandler	Con Edison	5	NPCC
					Tracy MacNicoll	Utility Services	5	NPCC
					Shivaz Chopra	New York Power Authority	6	NPCC
					Vijay Puran	New York State Department of Public Service	6	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					Joshua London	Eversource Energy	1	NPCC
					Nicolas Turcotte	Hydro-Quebec (HQ)	1	NPCC
					Jeffrey Streifling	NB Power Corporation	1,4,10	NPCC
					Joel Charlebois	AESI	7	NPCC
					John Hastings	National Grid	1	NPCC
					Erin Wilson	NB Power	1	NPCC
					James Grant	NYISO	2	NPCC
					Michael Couchesne	ISO-NE	2	NPCC
					Kurtis Chong	IESO	2	NPCC
					Michele Pagano	Con Edison	4	NPCC
					Bendong Sun	Bruce Power	4	NPCC
					Carvers Powers	Utility Services	5	NPCC
					Wes Yeomans	NYSRC	7	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable

					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC

1. Do you agree with the language proposed in CIP-003-11 Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

FirstEnergy finds the scope is too great for larger utilities to be successfully accomplished as well as within the timeframe suggested by these proposals.

Likes 0	
Dislikes 0	

Response

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Although section 3.1.2 is within the scope of the SAR BPA still believes it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. The proposed language requires detection of known/suspected malicious communications for "inbound and outbound electronic remote access." There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5).

BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS or the applicability be changed to bring it in-line with other requirements.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; Tyler Brun, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

Section 3.1.2 is requiring malicious communication detection which is not even required at medium sites (CIP-005-7 or CIP-005-8). It does not make sense to require it at lows unless there is going to be a change to require it for mediums as well.

Section 4 and Section 5 cannot be accomplished without knowing the individual assets that are part of the low impact Cyber Systems. The note that states a list of low assets in not required is a fallback that entities are using to justify not accomplishing the requirements of section 4 and 5. The requirement to classify individual assets should be required to accomplish all the changes in requirements.

Likes 0	
Dislikes 0	

Response

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1 - RF

Answer	No
Document Name	

Comment

The additional language in Section 3 does not fully mitigate the coordinated attack risk for LIBCS as the controls do not address distributed network accessibility from IBRs. Also, the suggested Requirements are more stringent than BCS classified as Medium Impact without ERC.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

CIP-003-11 Attachment 1, Section 3, Part 3.1.2 does not specify whether the requirement is to detect known or suspected malicious communications for ***both*** encrypted and/or unencrypted traffic.

SMUD recommends changing the language to:

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic ***unencrypted*** access;

Likes 0	
Dislikes 0	

Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	
We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language. CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. We recommend merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
For Attachment 1, Part 3.1.2 – As proposed, this currently applies to all low impact BES Cyber Systems but does not apply to Medium Impact Facilities that are not Control Centers. The DT needs to ensure that the reliability risks of both low and medium impact facilities are appropriately and consistently applied.	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
Comments: Section 3.1.3 could be reworded to be less confusing. The intent appears to be requiring authentication of remote access into a LIBCS based on the verbiage “through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted”. However, the Section 3.1 that is referenced may bring local access into question, as Section 3.1 includes both inbound (remote) and outbound access (local) from the LIBCS as it only mentions traffic “between a [LIBCS] and a Cyber Asset(s) outside the asset containing [LIBCS]” with no mention of traffic direction or origination	

point. This could require authentication in all cases of network access where traffic is leaving the site, if users could even be 100% aware of the destination of all information generated by their session and authentication may need to be implemented for all sessions. It may be difficult to implement an outbound access solution, and would potentially bring authentication prior to connecting to a non-CIP system into scope.

The Technical Rationale section again supports the notion that the scope includes access “from a remote client outside the asset containing the LIBCS and destined for a LIBCS within the asset”. This specifically notes an origination point and a traffic direction, which is missing in the language of the requirement.

The requirement should specify traffic origination and direction for authentication if it is indeed scoped only to remote access. If local network access is intended to be included, then a requirement for remote access authentication and a separate requirement for local system access should be created and mirror the requirements of CIP-005 and CIP-007.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee’s comments.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez

Answer	No
Document Name	

Comment

• The proposed changes to the language in section 1.1 of the “C. Compliance” area of the standard is problematic. What “Applicable Governmental Authority” could enforce compliance other than FERC, NERC or the Regional Entity in their “respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions”? How is “Applicable” defined?
• Language in section 3, particularly 3.1.1 through 3.1.6 and 3.2, is perceived to be arduous and expensive to implement and maintain compliance with, and could result in negative results. More money and people will be required to ensure compliance rather than focus on the goal, which is to

secure the systems against adversaries. Low impact assets are low impact or they are not. By adding the requirements to permit only necessary inbound and outbound access, detect known or suspected malicious communications, authenticate each user prior to permitting access, protecting user authentication information, determine vendor electronic access and disabling vendor access this is, in essence, raising the level of compliance requirements, and subsequently to the audit requirements thereof, to a state equivalent to Medium impact.
• Recommendations: Leave it alone. Unless there are metrics to prove that the existing standards are not adequately protecting the critical infrastructure relating directly to root causes identifying these sections of the standards, then modifications to them should not be made, especially modifications that would result in an undue burden to the financial stability of the Responsible entity due to additional compliance requirements, labor, capital costs and potential fines for non-compliance.
• Cancel all changes to CIP-003-9 and the SAR should be reviewed and recommendations made to change the criterion for Medium impact based on objective and measurable criteria rather than expect responsible entities to acquiesce to the recommendation by the LICRT to change all low impact requirements.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	Yes
Document Name	

Comment

Duke Energy supports the proposed language.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	Yes
Document Name	

Comment

NEE supports EEI’s comments: “EEI supports the language proposed in CIP-003-11 Attachment 1.“

Likes 0	
Dislikes 0	

Response

Michelle Pagano - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	Yes
Document Name	
Comment	
Supporting EEI comments	
Likes 0	
Dislikes 0	
Response	
Matt Carden - Southern Company - Southern Company Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Southern Company is in agreement with EEI along with the following comment: Southern asks that a clarification as to intent be made at least in the Technical Rationale document that for 3.1.3 when it states “Authenticate each user” that it does not imply that every remote user must have an individual user account, precluding the use of shared accounts by valid and authorized users for remote access.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligned with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) supports the proposed language in CIP-003-11 Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
TVA requests clarification that a list of users is not required to be maintained for vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
EEI supports the language proposed in CIP-003-11 Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the proposed language in CIP-003-11 Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See comments from EEI	
Likes 0	
Dislikes 0	
Response	
Michael Moltane - International Transmission Company Holdings Corporation - 1	
Answer	Yes
Document Name	

Comment	
Support EEI	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Fausto Serratos - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Kerrigan - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leshel Hutchings - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Carey Salisbury - Santee Cooper - 5, Group Name Santee Cooper

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC

Answer	
Document Name	

Comment

We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language. CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. We recommend merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot.

Likes 0	
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	
Document Name	

Comment

WEC Energy Group supports the language proposed in CIP-003-11.

Likes 0	
Dislikes 0	
Response	

2, Do you agree with the language proposed in CIP-003-11 Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez

Answer	No
Document Name	

Comment

• Suggested language changes throughout section 3 have completely vacated the approved CIP-003-8 and the changes are monumental. All changes are perceived to be arduous and expensive to implement and maintain compliance with, and could result in negative results. More money and people will be required to ensure compliance rather than focus on the goal, which is to secure the systems against adversaries. Low impact assets are low impact or they are not. By adding the requirements to show the ability to detect and authenticate, protect, determine and disable, this is, in essence, raising the level of compliance requirements, and subsequently the audit requirements thereof, to a state equivalent to a Medium impact facility.

• Cancel all changes to CIP-003-9 and the SAR should be reviewed and recommendations made to change the criterion for Medium impact based on objective and measurable criteria rather than expect responsible entities to acquiesce to the recommendation by the LICRT to change all low impact requirements.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee’s comments.

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren suggests removing OEM sheets from the list of documentation. An OEM would not provide recommendations on how to use a device or consider what is necessary for electronic access by the entity.

Likes 0	
Dislikes 0	

Response

Jeffrey Streifling - NB Power Corporation - 1

Answer	No
Document Name	

Comment

We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language. CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. We recommend merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST suggests adding username/password to the list of user authentication mechanisms cited in Section 3, Item 3 as possible ways to address requirement 3.1.3 of Attachment 1, Section 3. We believe this addition to be justified by the fact the Technical Rationale document mentions username and password in its discussion of Attachment 1, Section 3.1.4.

Likes 0	
Dislikes 0	

Response

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1 - RF

Answer	No
Document Name	

Comment
Please refer to the comments provided in Question 1 above.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; Tyler Brun, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment
Do not agree with 3.1.2 for Malware Detection unless it is going to be required at medium sites as well.

Likes 0	
Dislikes 0	

Response

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment
Although section 3.1.2 is within the scope of the SAR BPA still believes it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. The proposed language requires detection of known/suspected malicious communications for “inbound and outbound electronic remote access.” There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5). BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS or the applicability be changed to bring it in-line with other requirements. BPA recommends the SDT include a documentation option outside of OEM spec sheets as, depending on equipment, these may not be available. BPA also believes internal proof of testing should be allowable in case OEM was not available.

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy finds the scope is too great for larger utilities to be successfully accomplished as well as within the timeframe suggested by these proposals.	
Likes 0	
Dislikes 0	
Response	
Michael Moltane - International Transmission Company Holdings Corporation - 1	
Answer	Yes
Document Name	
Comment	
Support EEI	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See comments from EEI	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	

Answer	Yes
Document Name	
Comment	
The NAGF supports the proposed language in CIP-003-11 Attachment 2.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the language proposed in CIP-003-11 Attachment 2 as it conforms with the revised language in Attachment 1. EEI provides the non-substantive edit to change the case of the terms “Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)” and “Security Incident and Event Management (SIEM)” in Attachment 2, Section 3, part 2 to lowercase because they are not NERC Glossary defined terms and do not require capitalization.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute for Question #2.	
Likes 0	
Dislikes 0	
Response	

Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

CEHE tentatively supports the proposed language in CIP-003-11 Attachment 2, but would like to request further clarification on Section 3, part 1, bullet 3 in the snippet included below:

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. For Section 3.1.1, documentation showing the permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, such as:

• Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);

• Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways); or

• Original Equipment Manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

CEHE requests further clarification on the process in determining how the inclusion of OEM specification sheets would be considered sufficient evidence for Electronic Access Controls. CEHE understands that the provided example is merely a suggestion but would like to request more clarification on how this could be utilized.

Likes 0	
Dislikes 0	
Response	

Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligned with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Matt Carden - Southern Company - Southern Company Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Southern Company is in agreement with the EEEI comments: EEI supports the language proposed in CIP-003-11 Attachment 2 as it conforms with the revised language in Attachment 1. EEI provides the non-substantive edit to change the case of the terms “Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)” and “Security Incident and Event Management (SIEM)” in Attachment 2, Section 3, part 2 to lowercase because they are not NERC Glossary defined terms and do not require capitalization.	
Likes 0	
Dislikes 0	
Response	
Michelle Pagano - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	Yes
Document Name	
Comment	
Supporting EEI comments	
Likes 0	
Dislikes 0	
Response	

Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
EEI provides the non-substantive edit to change the case of the terms “Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)” and “Security Incident and Event Management (SIEM)” in Attachment 2, Section 3, part 2 to lowercase because they are not NERC Glossary defined terms and do not require capitalization.“	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the proposed language and supports the non-substantive revisions proposed by EEI.	
Likes 0	
Dislikes 0	
Response	
Carey Salisbury - Santee Cooper - 5, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leshel Hutchings - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3,	

6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Robert Kerrigan - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Fausto Serratos - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	
We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language. CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. We recommend merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot.	
Likes 0	
Dislikes 0	
Response	

3. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-11. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

FirstEnergy finds this an enormous undertaking for larger organizations/entities to meet expectations within the 3-year implementation plan. Considerations for network buildouts and firewalls as well as coordination with transmission planning and implementation must be taken into consideration. FirstEnergy requests the Drafting Team to consider a staged implementation plan to allow for planning, scheduling, budgeting, and implementing to ensure full compliance toward the scope of CIP-003 and protection of the BES. These required steps would necessitate a longer implementation that allows 18-24 months to develop an implementation plan, budget and staff for the implementation over time, and permit a number of years for staged implementations following CIP-003-09 based on reasonable criteria set by the utility which would, of course, be overseen by the RE.

Likes 0	
Dislikes 0	

Response

TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

Southern Indiana Gas and Electric d/b/a CenterPoint Energy Indiana South (SIGE) has concerns that having multiple versions of the standard and simultaneously working on modifications, is causing confusion. Without having approved versions, further proposed revisions seem a bit premature.

Likes 0	
Dislikes 0	

Response

Jeffrey Streifling - NB Power Corporation - 1

Answer	No
Document Name	

Comment

CIP-003-11 and CIP-003-12 implementation plan should be combined and repost after FERC approves CIP-003-10 in a new ballot. NPCC recommends only having one implementation timeframe and TFIST prefers 36-month timeframe.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy recommends a 5-year implementation plan with a phased approach for the implementation of devices required to achieve compliance with the IDS / IDP provisions in Part 3.1.2, The milestones and methodology for the implmentation should be at the direction of the Registered Entity.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	No
Document Name	
Comment	

• By adding the requirements to show the ability to detect and authenticate, protect, determine and disable, this is, in essence, raising the level of compliance requirements, and subsequently the audit requirements thereof, to a state equivalent to a Medium impact facility.
• Cancel all changes to CIP-003-9 and the SAR should be reviewed and recommendations made to change the criterion for Medium impact based on objective and measurable criteria rather than expect responsible entities to acquiesce to the recommendation by the LICRT to change all low impact requirements.

Likes 0	
Dislikes 0	

Response

Carey Salisbury - Santee Cooper - 5, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Santee Cooper would request a five-year implementation plan for the additional security controls listed in CIP-003-11. It would take time and money to implement these controls into over 100 low impact sites. Santee Cooper is in the process of rolling out routable communication to its low impact sites and this would require us to revisit each site to implement these additional security controls.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	Yes
Document Name	

Comment

Duke Energy supports EEI comments.

Likes 0	
Dislikes 0	

Response

Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE

Answer	Yes
Document Name	

Comment
The implementation plan for CIP-003-11 includes a footnote that states: “1 On May 9, 2024, the NERC Board of Directors approved the retirement of Reliability Standard CIP-003-9, which *was* scheduled to take effect on April 1, 2026, when it approved revised Reliability Standard CIP-003-10. CIP-003-10 is pending regulatory approval. This implementation plan is intended to retire whichever version of the CIP-003 Reliability Standard that is then in effect.” With many concurrent CIP-003 version projects, it is possible that CIP-003-11 gets approved before CIP-003-10. Regardless of which version gets approved first, the wording in the footnote states that CIP-003-9 *was* to take effect on April 1, 2026. Is CIP-003-9 still effective April 1, 2026, or will CIP-003-10 or CIP-003-11 (or CIP-003-12) supersede the effective date of CIP-003-9?

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	

Comment
NEE supports EEI’s comments: “EEI supports the proposed three-year implementation plan for CIP-003-11 and appreciates the drafting team’s acknowledgement that the revisions proposed in CIP-003-11 do not conflict but build upon the implementation of CIP-003-9 which has an effective date of April 1, 2026, however, we recommend removing the footnote on page 1 of the implementation plan regarding the retirement of CIP-003-9. The effective dates and retirement dates of the different versions of CIP-003 are discussed clearly in the General Considerations section and Retirement Date Section. Including the information in a footnote has not been standard practice and the Implementation Plan is clearer without it.“

Likes 0	
Dislikes 0	

Response

Michelle Pagano - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	Yes
Document Name	

Comment
Supporting EEI comments

Likes 0	

Dislikes 0	
Response	
Matt Carden - Southern Company - Southern Company Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Southern Company is in agreement with the EEI comments: EEI supports the proposed three-year implementation plan for CIP-003-11 and appreciates the drafting team's acknowledgement that the revisions proposed in CIP-003-11 do not conflict but build upon the implementation of CIP-003-9 which has an effective date of April 1, 2026, however, we recommend removing the footnote on page 1 of the implementation plan regarding the retirement of CIP-003-9. The effective dates and retirement dates of the different versions of CIP-003 are discussed clearly in the General Considerations section and Retirement Date Section. Including the information in a footnote has not been standard practice and the Implementation Plan is clearer without it.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligned with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

CEHE supports the comments as submitted by the Edison Electric Institute (EEI)

EEI Comments:

EEI supports the proposed three-year implementation plan for CIP-003-11 and appreciates the drafting team's acknowledgement that the revisions proposed in CIP-003-11 do not conflict but build upon the implementation of CIP-003-9 which has an effective date of April 1, 2026, however, we recommend removing the footnote on page 1 of the implementation plan regarding the retirement of CIP-003-9.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	Yes
Document Name	

Comment

Exelon supports the comments submitted by the EEI for this question.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer	Yes
Document Name	

Comment

Black Hills Corporation agrees with EEI's comments on question 7: Black Hills Corporation is concerned about the proposed effective date for CIP-003-12. CIP-003-12 is the alignment of the Project 2023-04 changes with conforming changes from Project 2016-02 Virtualization, which is pending FERC approval. Given its pending approval, it is difficult to understand if the 24-month period would provide a shorter implementation timeframe than the 36-month period proposed for CIP-003-11. EEI supports a 36-month implementation period for the draft revisions and asks for that timeframe regardless of the version of CIP-003 approved.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute for Question #3.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed three-year implementation plan for CIP-003-11 and appreciates the drafting team's acknowledgement that the revisions proposed in CIP-003-11 do not conflict but build upon the implementation of CIP-003-9 which has an effective date of April 1, 2026, however, we recommend removing the footnote on page 1 of the implementation plan regarding the retirement of CIP-003-9. The effective dates and retirement dates of the different versions of CIP-003 are discussed clearly in the General Considerations section and Retirement Date Section. Including the information in a footnote has not been standard practice and the Implementation Plan is clearer without it.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the proposed three (3) year implementation plan for CIP-003-11.	
Likes 0	
Dislikes 0	
Response	

Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See comments from EEI	
Likes 0	
Dislikes 0	
Response	
Michael Moltane - International Transmission Company Holdings Corporation - 1	
Answer	Yes
Document Name	
Comment	
Support EEI	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
WEC Energy Group supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Fausto Serratos - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Kerrigan - Los Angeles Department of Water and Power - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; Tyler Brun, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes

Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leshel Hutchings - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	
CIP-003-11 and CIP-003-12 implementation plan should be combined and repost after FERC approves CIP-003-10 in a new ballot. NPCC recommends only having one implementation timeframe and TFIST prefers 36-month timeframe.	
Likes 0	
Dislikes 0	
Response	

4. The DT believes the language of CIP-003-11 addresses the issues outlined in the SAR in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical, or procedural justification.

Carey Salisbury - Santee Cooper - 5, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Implementing CIP-003-11 would not be cost effective for Santee Cooper. We are installing routable communication at our low impact facilities. However, when developing the plans to roll out routable communication to our low impact facilities we didn't consider CIP-003-11. To comply with CIP-003-11 we would have to add additional support and incur significant cost in adding equipment or software licenses to comply.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez

Answer	No
Document Name	

Comment

• Just the recommended changes to Appendix 2 make the DT claims that the language addresses the issues outlined in the SAR cost effectively objectively false. Just the technology needed to comply with the language makes that claim unreasonable, much less the cost of labor for implementation, maintenance, audit, troubleshooting and lifecycle replacement.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

Dominion Energy does not think the methods listed in the SAR are cost effective. Any methods that require installation of devices that support IDS/IDP for Low Impact within larger Registered Entities is an expensive undertaking. Other methods that can be used to comply with the standard, such as manual reviews and SIEMs also have a significant cost associated with them.

Likes 0	
Dislikes 0	

Response

Jeffrey Streifling - NB Power Corporation - 1

Answer	No
Document Name	

Comment

We have no comments on the cost-effectiveness of CIP-003-11. We will note that the cost effectiveness of CIP-003-12 was not asked in this comment form.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment
SMUD views the language in CIP-003-11 as neither cost effective nor cost ineffective. If CIP-003-11 Attachment 1, Section 3, Part 3.1.2 requires the detection of suspected malicious communications that is ***encrypted*** [emphasis added], then the language of CIP-003-11 would not be cost effective due to the additional cost of implementing the inspection of encrypted traffic.

Likes 0	
Dislikes 0	

Response

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1 - RF	
Answer	No
Document Name	

Comment
There will be costs associated with implementing additional IDS, monitoring, equipment upgrades, and resources to both implement and maintain. It is uncertain at this time if the language will provide a cost-effective solution.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; Tyler Brun, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	

Comment
PG&E will not comment on costs that have not been analyzed, there are too many factors that will go into this question.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	

Comment	
Reclamation identifies that more information is needed to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
See FirstEnergy's comments above.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
There will be costs associated with adding new software/technology and upgrading legacy equipment.	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	

Comment	
It cannot be determined at this time if the language of CIP-003-11 addresses the issues in a cost effective manner.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the revisions and does not have any concerns regarding the cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matt Carden - Southern Company - Southern Company Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Kerrigan - Los Angeles Department of Water and Power - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Fausto Serratos - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Moltane - International Transmission Company Holdings Corporation - 1	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	

Document Name	
Comment	
Ameren has no comment on the cost effectiveness of the project.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	
We have no comments on the cost-effectiveness of CIP-003-11. We will note that the cost effectiveness of CIP-003-12 was not asked in this comment form.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	

CEHE does not comment on cost.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE does not comment on cost.	
Likes 0	
Dislikes 0	
Response	

5. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
FirstEnergy thanks the DT for their work on these drafts but requests an increase in the implementation plan's timeline to ensure efficient and manageable protection of the Bulk Electric System.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	
Document Name	
Comment	
Duke Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	

Fausto Serratos - Los Angeles Department of Water and Power - 3	
Answer	
Document Name	
Comment	
CIP-003-11 references “Technical Rationale for Reliability Standard CIP-003-11 – Low Impact BES Cyber Security Criteria Revisions”. We recommend the following sentences be reviewed: 1) On page 1 of the Technical Rationale, please note that the following is not a complete sentence: “Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified.” 2) On page 6 of the Technical Rationale, under Section 3.1.3, says “(allowing, establishing, gaining)” after “permitting”. It is recommended that this phrase in the parentheses should just be deleted. It is unnecessary and confusing, given that these other words do not appear in the standard.	
Likes 0	
Dislikes 0	
Response	

Robert Kerrigan - Los Angeles Department of Water and Power - 5	
Answer	
Document Name	
Comment	
Comments: CIP-003-11 references “Technical Rationale for Reliability Standard CIP-003-11 – Low Impact BES Cyber Security Criteria Revisions”. We recommend the following sentences be reviewed: 1) On page 1 of the Technical Rationale, please note that the following is not a complete sentence: “Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified.” 2) On page 6 of the Technical Rationale, under Section 3.1.3, says “(allowing, establishing, gaining)” after “permitting”. It is recommended that this phrase in the parentheses should just be deleted. It is unnecessary and confusing, given that these other words do not appear in the standard. The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering the following questions.	
Likes 0	
Dislikes 0	
Response	

Richard Vendetti - NextEra Energy - 5

Answer	
Document Name	

Comment

NEE supports EEI's comments: "The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering the following questions."

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; Tyler Brun, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	
Document Name	

Comment

The rationale comments that jump host for low sites is not required, but in reality, there are limited ways to meet the requirements stated here other than using jump hosts. Since it is required in CIP 005, it should be here too.

The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering the following questions.

Likes 0	
Dislikes 0	

Response

Matt Carden - Southern Company - Southern Company Services, Inc. - 1

Answer	
Document Name	

Comment

Southern Company is in agreement with the EEi comments

Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligned with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	
Black Hills Corporation is concerned about having multiple CIP-003 projects and multiple virtualization projects occurring simultaneously as it is becoming difficult to maintain oversight of the changes to a degree that allows sufficient review. In addition, how is NERC ensuring that the direction of these multiple projects maintain alignment?	
Likes 0	

Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	
Document Name	
Comment	
The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering the following questions.	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST considers it unfortunate that industry has been afforded only a single, up or down vote on two distinctly different implementation plans, one for CIP-003-11 and one for CIP-003-12. Our "Negative" vote reflects our concerns about only the "-12" implementation plan. Given the opportunity to vote on just the "-11" implementation plan, our vote would have been "Affirmative."	
Likes 0	

Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	
In the Technical Rationale the information in figure 4 should be included in the diagram for figure 1 and figure 2. Figure 4 provides confusion because it does not meet the criteria listed in 3.1.1 and 3.1.2. Recommend that the Technical Rationale clearly states for each diagram if they are depicting compliance with only an individual subsection of the requirement. In figure 5 can the jump host now be part of an associated data center for a Control Center?	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	
Document Name	
Comment	
We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language.	

CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. We recommend merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC

Answer	
Document Name	

Comment

We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language. CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. We recommend merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot.

Likes 0	
Dislikes 0	

Response

Leshel Hutchings - AEP - 3

Answer	
Document Name	

Comment

VCA is used in the document but never defined as Virtual Cyber Asset anywhere, if an end user needs to look up acronym, it would be useful to define VCA in the Glossary of Terms.

Likes 0	
Dislikes 0	

Response

Selene Willis - Edison International - Southern California Edison Company - 5

Answer	
Document Name	

Comment

See comments from EEI	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Michael Moltane - International Transmission Company Holdings Corporation - 1	
Answer	
Document Name	
Comment	
Support EEI	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	

Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	
Document Name	
Comment	
• Cancel all changes to CIP-003-9 and the SAR should be reviewed and recommendations made to change the criterion for Medium impact based on objective and measurable criteria rather than expect responsible entities to acquiesce to the recommendation by the LICRT to change all low impact requirements resulting in unreasonable technological and labor costs.	
Likes 0	
Dislikes 0	
Response	

The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering this question.

6. Do you have any concerns in the way CIP-003-10 (Project 2016-02 changes) and CIP-003-11 (Project 2023-04 changes) were combined to create standard CIP-003-12?

David Jendras Sr - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

EACMS and PCAs have previously not been applicable for Low-Impact CIP Assets. However, SCI could be introducing an opportunity for EACMS and PCA requirements. Would a centralized engineering or cyber tool suite that is only used to support Low-Impact CIP assets from outside the ESP qualify as a SCI? If so, would EACMS or PCA requirements then apply to such a system even if such protections are not required for the BCS? Ameren suggests adding a statement to the SCI definition clarifying which requirements are for low, medium, and high impact BCS or SCI.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST has no concerns about the content of proposed CIP-003-12. We do, however, have concerns about the implementation plan, as explained below.

Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CEHE supports the comments as submitted by EEI.

EEI has reviewed the redline of CIP-003-9 to CIP-003-12 and understands that the revisions make conforming changes in alignment with Project 2016-02 and is supportive of the alignment.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Tacoma Power has no concerns.	
Likes 0	
Dislikes 0	
Response	
Carey Salisbury - Santee Cooper - 5, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	

Answer	Yes
Document Name	
Comment	
• Expecting responsible entities to understand the unintended consequences of multiple changes to the same standard without any implementation time or settling time is unreasonable. Suggest following precedent set during changes to CIP-015 by making suggested changes in a new standard such as CIP-016, where CIP-003 would remain unchanged and requirements for low impact assets would be captured in the new standard. We do not agree that any changes should be made for Low Impact, but if forced to do so, the recommendation is to create a new standard. • Recommend canceling all changes to CIP-003-9 and the SAR should be reviewed and recommendations made to change the criterion for Medium impact based on objective and measurable criteria rather than expect responsible entities to acquiesce to the recommendation by the LICRT to change all low impact requirements.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See comments from EEI	
Likes 0	
Dislikes 0	
Response	
Michael Moltane - International Transmission Company Holdings Corporation - 1	
Answer	Yes
Document Name	
Comment	
Support EEI	
Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
WEC Energy Group supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Leshel Hutchings - AEP - 3	
Answer	Yes
Document Name	
Comment	
AEP has reviewed the redlines and concur with EEI's comments below understands that the revisions make conforming changes in alignment with Project 2016-02 and is supportive of the alignment. EEI suggests the following clarification, which we feel is non-substantive and in alignment with the intention of the DT, in Attachment 1: Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). **Responsible Entities with Shared Cyber Infrastructure (SCI) that supports a low impact BCS can utilize policies, procedures, and processes for their SCI supporting high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s).** Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.	

The defined term SCI applies when it hosts or provides storage resources required for system functionality for one or more Virtual Cyber Assets (VCAs) and one or more VCAs that are not included in, or associated with, BCS of the same impact categorization. Where a higher level of controls is applied to the SCI supporting low impact BCS, Entities should be able to use them to satisfy the requirements applicable to SCI in CIP-003-12, Attachment 1.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	Yes
Document Name	

Comment

Dominion Energy would like clarification on the SCI and the phrase from the technical rationale document for Project 2021-02, “However, network switches and other hardware that does enforce an ESP” specifically clarification on “other hardware”. Does this term include the firewall that is creating the ESP?

Likes 0	
Dislikes 0	

Response

Jeffrey Streifling - NB Power Corporation - 1

Answer	Yes
Document Name	

Comment

It’s very confusing to review two separate versions of the same standard at the same time. Preferably one version should be reviewed at a time. Also having so many different projects working on one standard at the same time creates confusion.

We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language. CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. TFIST recommends merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot.

Additionally, we have concerns with the use of the SCI term and the possibility the EACMS, PACS at High or Medium Facilities may also have to comply with CIP-003-12 requirements which may be different than High and Medium requirements. We observed that SCI devices at High or Medium locations may be subject to documenting all inbound communication at the location which could be a substantial burden at a High and Medium location which would include corporate and non-BCS communications. It is proposed that SCI devices be high water marked to High/Medium or Low requirements.

Likes 0	
Dislikes 0	

Response

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI has reviewed the redline of CIP-003-9 to CIP-003-12 and understands that the revisions make conforming changes in alignment with Project 2016-02 and is supportive of the alignment. EEI suggests the following clarification, which we feel is non-substantive and in alignment with the intention of the DT, in Attachment 1:

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). **Responsible Entities with Shared Cyber Infrastructure (SCI) that supports a low impact BCS can utilize policies, procedures, and processes for their SCI supporting high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s).** Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

The defined term SCI applies when it hosts or provides storage resources required for system functionality for one or more Virtual Cyber Assets (VCAs) and one or more VCAs that are not included in, or associated with, BCS of the same impact categorization. Where a higher level of controls is applied to the SCI supporting low impact BCS, Entities should be able to use them to satisfy the requirements applicable to SCI in CIP-003-12, Attachment 1.

Likes 0	
Dislikes 0	

Response

TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	Yes
Document Name	

Comment

Southern Indiana Gas and Electric d/b/a CenterPoint Energy Indiana South (SIGE) has concerns that having multiple versions of the standard simultaneously working on modifications causing confusion. Without having approved versions prior to making proposed revisions seems a bit premature.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute for Question #6.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI. Black Hills Corporation has reviewed the redline of CIP-003-9 to CIP-003-12 and understands that the revisions make conforming changes in alignment with Project 2016-02 and is supportive of the alignment. EEI suggests the following clarification, which we feel is non-substantive and in alignment with the intention of the DT, in Attachment 1: Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). **Responsible Entities with Shared Cyber Infrastructure (SCI) that supports a low impact BCS can utilize policies, procedures, and processes for their SCI supporting high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s).** Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets. The defined term SCI applies when it hosts or provides storage resources required for system functionality for one or more Virtual Cyber Assets (VCAs) and one or more VCAs that are not included in, or associated with, BCS of the same impact categorization. Where a higher level of controls is applied to the SCI supporting low impact BCS, Entities should be able to use them to satisfy the requirements applicable to SCI in CIP-003-12, Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	

Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligned with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; Tyler Brun, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
Comments and ballots on CIP-003-11 and 12 are confusing> To avoid complications, the others should be abandoned and only one should be released.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	

NEE supports EEI's comments: "EEI has reviewed the redline of CIP-003-9 to CIP-003-12 and understands that the revisions make conforming changes in alignment with Project 2016-02 and is supportive of the alignment. EEI suggests the following clarification, which we feel is non-substantive and in alignment with the intention of the DT, in Attachment 1:

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). **Responsible Entities with Shared Cyber Infrastructure (SCI) that supports a low impact BCS can utilize policies, procedures, and processes for their SCI supporting high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s).** Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

The defined term SCI applies when it hosts or provides storage resources required for system functionality for one or more Virtual Cyber Assets (VCAs) and one or more VCAs that are not included in, or associated with, BCS of the same impact categorization. Where a higher level of controls is applied to the SCI supporting low impact BCS, Entities should be able to use them to satisfy the requirements applicable to SCI in CIP-003-12, Attachment 1."

Likes 0	
Dislikes 0	

Response

Michelle Pagano - Con Ed - Consolidated Edison Co. of New York - 5

Answer	Yes
Document Name	

Comment

Supporting EEI comments

Likes 0	
Dislikes 0	

Response

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1 - RF

Answer	Yes
Document Name	

Comment

Combining multiple versions of a Reliability Standard Under Development into one (1) ballot is proving to be overtly onerous. It would be more beneficial if CIP-003-11 and CIP-003-12 language were combined into one (1) version of the Standard to be evaluated and balloted upon.

Likes 0	
Dislikes 0	

Response

Matt Carden - Southern Company - Southern Company Services, Inc. - 1

Answer	Yes
Document Name	

Comment

Southern Company is in agreement with the EEI comments:

EEI has reviewed the redline of CIP-003-9 to CIP-003-12 and understands that the revisions make conforming changes in alignment with Project 2016-02 and is supportive of the alignment. EEI suggests the following clarification, which we feel is non-substantive and in alignment with the intention of the DT, in Attachment 1:

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). **Responsible Entities with Shared Cyber Infrastructure (SCI) that supports a low impact BCS can utilize policies, procedures, and processes for their SCI supporting high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s).** Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

The defined term SCI applies when it hosts or provides storage resources required for system functionality for one or more Virtual Cyber Assets (VCAs) and one or more VCAs that are not included in, or associated with, BCS of the same impact categorization. Where a higher level of controls is applied to the SCI supporting low impact BCS, Entities should be able to use them to satisfy the requirements applicable to SCI in CIP-003-12, Attachment 1.

Likes 0	
Dislikes 0	

Response

Robert Kerrigan - Los Angeles Department of Water and Power - 5

Answer	Yes
Document Name	

Comment

Comments: CIP-003-12 seems better developed than CIP-003-11, in that it includes more concepts. The main comment about CIP-003-12 is that it includes two terms, “VCA” and “SCI”, that are new per virtualization project – will the terms be added into the standard itself or will the DT ensure they be added to the NERC glossary of terms?

Likes 0	
Dislikes 0	
Response	
Fausto Serratos - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
CIP-003-12 seems better developed than CIP-003-11, in that it includes more concepts. The main comment about CIP-003-12 is that it includes two terms, “VCA” and “SCI”, that are new per virtualization project – will the terms be added into the standard itself or will the DT ensure they be added to the NERC glossary of terms?	
Likes 0	
Dislikes 0	
Response	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
It’s very confusing to review two separate versions of the same standard at the same time. Preferably one version should be reviewed at a time. Also having so many different projects working on one standard at the same time creates confusion.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
See FirstEnergy's response to Q1.	

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	Yes
Document Name	

Comment

Duke Energy supports the non-substantive revisions proposed by EEI.

Likes 0	
Dislikes 0	

Response

Carver Powers - Utility Services, Inc. - 4

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	

It’s very confusing to review two separate versions of the same standard at the same time. Preferably one version should be reviewed at a time. Also having so many different projects working on one standard at the same time creates confusion.

We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language. CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. TFIST recommends merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot.

Additionally, we have concerns with the use of the SCI term and the possibility the EACMS, PACS at High or Medium Facilities may also have to comply with CIP-003-12 requirements which may be different than High and Medium requirements. We observed that SCI devices at High or Medium locations may be subject to documenting all inbound communication at the location which could be a substantial burden at a High and Medium location which would include corporate and non-BCS communications. It is proposed that SCI devices be high water marked to High/Medium or Low requirements.

Likes 0	
Dislikes 0	

Response

The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering this question.

7. Do you have any concerns in the CIP-003-12 implementation plan that should be addressed?

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment

Tacoma Power has no concerns.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	No
Document Name	

Comment

NEE supports EEI's comments: "EEI supports the CIP-003-12 implementation plan."

Likes 0	
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	No
Document Name	

Comment

NA.

Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
SMUD agrees with the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The NAGF agrees with the proposed CIP-003-12 implementation plan.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Fausto Serratos - Los Angeles Department of Water and Power - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Kerrigan - Los Angeles Department of Water and Power - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carey Salisbury - Santee Cooper - 5, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	

Manitoba Hydro appreciates the standard drafting team's intent that the timeline set forth for CIP-003-12 be the later of 36-months from CIP-003-11 approval or 24-months from CIP-003-12 approval, giving entities at least 36-months of time to implement the changes. However, there is the possibility that CIP-003-11 does not receive governmental approval, and the version is "skipped" going straight to CIP-003-12. In this scenario, only 24-months of implementation would be afforded. This would not give entities enough time, especially if the standard changes require additional staff, hardware or architecture changes. Manitoba Hydro suggests that the implementation plan effective date for CIP-003-12 be revised to match CIP-003-11 and state that the standard become effective thirty-six (36) months after the effective date of the applicable governmental authority's order approving Reliability Standard CIP-003-12.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	Yes
Document Name	

Comment

Duke Energy supports EEI comments.

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

See FirstEnergy's response to Q3.

Likes 0	
Dislikes 0	

Response

Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
When looking at implementation of plans of CIP-003-10, CIP-003-11, and CIP-003-12 it becomes confusing to decipher what is the actual effective date of CIP-003-12. There are too many dependencies involved.	
Likes 0	
Dislikes 0	
Response	

Matt Carden - Southern Company - Southern Company Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Southern Company is in agreement with the EEI comments: EEI is concerned about the proposed effective date for CIP-003-12. CIP-003-12 is the alignment of the Project 2023-04 changes with conforming changes from Project 2016-02 Virtualization, which is pending FERC approval. Given its pending approval, it is difficult to understand if the 24-month period would provide a shorter implementation timeframe than the 36-month period proposed for CIP-003-11. EEI supports a 36-month implementation period for the draft revisions and asks for that timeframe regardless of the version of CIP-003 approved.	
Likes 0	
Dislikes 0	
Response	

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1 - RF	
Answer	Yes
Document Name	
Comment	
With multiple versions of implementation plans as they pertain to the different versions of a Reliability Standard Under Development, it is challenging to discern the applicable timelines and the organizational impacts of the implementation	
Likes 0	
Dislikes 0	

Response	
Michelle Pagano - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	Yes
Document Name	
Comment	
Supporting EEI comments	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; Tyler Brun, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
This should state 24 months after the implementation of CIP -003-11 not CIP 003-9. The way it is currently written, implementation would be required earlier than CIP-003-11.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligned with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI's comments: Black Hills Corporation is concerned about the proposed effective date for CIP-003-12. CIP-003-12 is the alignment of the Project 2023-04 changes with conforming changes from Project 2016-02 Virtualization, which is pending FERC approval. Given its pending approval, it is difficult to understand if the 24-month period would provide a shorter implementation timeframe than the 36-month period proposed for CIP-003-11. EEI supports a 36-month implementation period for the draft revisions and asks for that timeframe regardless of the version of CIP-003 approved.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
The NSRF appreciates the standard drafting team's intent that the timeline set forth for CIP-003-12 be the later of 36-months from CIP-003-11 approval or 24-months from CIP-003-12 approval, giving entities at least 36-months of time to implement the changes. However, there is the possibility that CIP-003-11 does not receive governmental approval, and the version is "skipped" going straight to CIP-003-12. In this scenario, only 24-months of implementation would be afforded. This would not give entities enough time, especially if the standard changes require additional staff, hardware or architecture changes. The NSRF suggests that the implementation plan effective date for CIP-003-12 be revised to match CIP-003-11 and state that the	

standard become effective thirty-six (36) months after the effective date of the applicable governmental authority's order approving Reliability Standard CIP-003-12.	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute and MRO NSRF for Question #7.	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Southern Indiana Gas and Electric d/b/a CenterPoint Energy Indiana South (SIGE) has the same concerns as addressed in question 6.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI is concerned about the proposed effective date for CIP-003-12. CIP-003-12 is the alignment of the Project 2023-04 changes with conforming changes from Project 2016-02 Virtualization, which is pending FERC approval. Given its pending approval, it is difficult to understand if the 24-month	

period would provide a shorter implementation timeframe than the 36-month period proposed for CIP-003-11. EEI supports a 36-month implementation period for the draft revisions and asks for that timeframe regardless of the version of CIP-003 approved.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	Yes
Document Name	

Comment

NST has the following two concerns about the CIP-003-12 implementation plan:

(1) We note the section, "Prerequisite Standards" lists only CIP-003-11. We believe it should also be necessary for CIP-003-10 to be approved before CIP-003-12 can become effective.

(2) We note the section, "Effective Date" identifies two possible scenarios (36 months after FERC approval of CIP-003-11 or 24 months after FERC approval of CIP-003-12) that seem to be based on an implicit assumption that by such time FERC approval is given to either Version 11 or Version 12, CIP-003-10 will have been previously approved. Although the NERC BoT has approved the "-10" version, it has not yet been approved by FERC, and NST believes this fact should be reflected in the current version of the "-12" implementation plan.

Likes 0	
Dislikes 0	

Response

Jeffrey Streifling - NB Power Corporation - 1

Answer	Yes
Document Name	

Comment

When looking at implementation of plans of CIP-003-10, CIP-003-11, and CIP-003-12 it becomes confusing to decipher what is the actual effective date of CIP-003-12. There are too many dependencies involved.

CIP-003-11 and CIP-003-12 implementation plan should be combined and repost after FERC approves CIP-003-10 in a new ballot. TFIST recommends only having one implementation timeframe and TFIST prefers 36-month timeframe.

Likes 0	
Dislikes 0	

Response	
Leshel Hutchings - AEP - 3	
Answer	Yes
Document Name	
Comment	
AEP has the same concerns as EEI--concerned about the proposed effective date for CIP-003-12. CIP-003-12 is the alignment of the Project 2023-04 changes with conforming changes from Project 2016-02 Virtualization, which is pending FERC approval. Given its pending approval, it is difficult to understand if the 24-month period would provide a shorter implementation timeframe than the 36-month period proposed for CIP-003-11. EEI supports a 36-month implementation period for the draft revisions and asks for that timeframe regardless of the version of CIP-003 approved.	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
WEC Energy Group supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	

Response	
Michael Moltane - International Transmission Company Holdings Corporation - 1	
Answer	Yes
Document Name	
Comment	
Support EEI	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See comments from EEI	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	Yes
Document Name	
Comment	
• Expecting responsible entities to understand the unintended consequences of multiple changes to the same standard without any implementation time or settling time is unreasonable.	
Likes 0	
Dislikes 0	
Response	

Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE requests the SDT consider adding verbiage to the Initial Performance of Periodic Requirements section to include initial performance expectations for newly registered entities and for entities for which CIP-003 did not previously apply.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC

Answer	
Document Name	

Comment

When looking at implementation of plans of CIP-003-10, CIP-003-11, and CIP-003-12 it becomes confusing to decipher what is the actual effective date of CIP-003-12. There are too many dependencies involved.

CIP-003-11 and CIP-003-12 implementation plan should be combined and repost after FERC approves CIP-003-10 in a new ballot. TFIST recommends only having one implementation timeframe and TFIST prefers 36-month timeframe.

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Chantal Mazza On Behalf of: Junji Yamaguchi, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza

Answer	
Document Name	

Comment	
This comment applies to all questions :It’s very confusing to review two separate versions of the same standard at the same time. Preferably one version should be reviewed at a time. Also having so many different projects working on one standard at the same time creates confusion.	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2023-04 Modifications to CIP-003 | Draft 3
Comment Period Start Date:	6/12/2024
Comment Period End Date:	7/11/2024
Associated Ballot(s):	2023-04 Modifications to CIP-003 CIP-003-A AB 3 ST 2023-04 Modifications to CIP-003 Implementation Plan AB 3 OT

There were 54 sets of responses, including comments from approximately 156 different people from approximately 92 companies representing 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, contact Manager of Standards Information, Nasheema Santos (via email) or at (404) 446-2564.

Questions

1. Do you agree with the language proposed in CIP-003-11 Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

2. Do you agree with the language proposed in CIP-003-11 Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

3. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-11. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.

4. The DT believes the language of CIP-003-11 addresses the issues outlined in the SAR in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical, or procedural justification.

5. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.

The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering this question.

6. Do you have any concerns in the way CIP-003-10 (Project 2016-02 changes) and CIP-003-11 (Project 2023-04 changes) were combined to create standard CIP-003-12?

The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering this question.

7. Do you have any concerns in the CIP-003-12 implementation plan that should be addressed?

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Husam Al-Hadidi	Manitoba Hydro (System Performance)	1,3,5,6	MRO
					Kimberly Bentley	Western Area Power Administration	1,6	MRO
					Jaimin Patal	Saskatchewan Power Corporation (SPC)	1	MRO
					George Brown	Pattern Operators LP	5	MRO
					Larry Heckert	Alliant Energy (ALTE)	4	MRO

					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Dane Rogers	Oklahoma Gas and Electric (OG&E)	1,3,5,6	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Ayotte	ITC Holdings	1	MRO
					Andrew Coffelt	Board of Public Utilities-Kansas (BPU)	1,3,5,6	MRO
					Peter Brown	Invenergy	5,6	MRO
					Angela Wheat	Southwestern Power Administration	1	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC

					Armando Rodriguez	Tennessee Valley Authority	6	SERC
					Nehtisha Rollis	Tennessee Valley Authority	5	SERC
Santee Cooper	Carey Salisbury	5		Santee Cooper	Rodger Blakely	Santee Cooper	1,3,5,6	SERC
					Christine Pope	Santee Cooper	1,3,5,6	SERC
					Lachelle Brooks	Santee Cooper	1,3,5,6	SERC
					Rene' Free	Santee Cooper	1,3,5,6	SERC
					Bob Rhett	Santee Cooper	1,3,5,6	SERC
					Bridget Coffman	Santee Cooper	1,3,5,6	SERC
					Wanda Williams	Santee Cooper	1,3,5,6	SERC
					Jordan Steele	Santee Cooper	1,3,5,6	SERC
WEC Energy Group, Inc.	Christine Kane	3		WEC Energy Group	Christine Kane	WEC Energy Group	3	RF
					Matthew Beilfuss	WEC Energy Group, Inc.	4	RF
					Clarice Zellmer	WEC Energy Group, Inc.	5	RF
					David Boeshaar	WEC Energy Group, Inc.	6	RF
Manitoba Hydro	Jay Sethi	1,3,5,6	MRO	Manitoba Hydro Group	Nazra Gladu	Manitoba Hydro	1	MRO
					Mike Smith	Manitoba Hydro	3	MRO

					Kristy-Lee Young	Manitoba Hydro	5	MRO
					Kelly Bertholet	Manitoba Hydro	6	MRO
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF

					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy- FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					Tyler Brun	Pacific Gas and Electric Company	5	WECC
Black Hills Corporation	Rachel Schuldt	6		Black Hills Corporation - All Segments	Micah Runner	Black Hills Corporation	1	WECC
					Josh Combs	Black Hills Corporation	3	WECC
					Rachel Schuldt	Black Hills Corporation	6	WECC
					Carly Miller	Black Hills Corporation	5	WECC
					Sheila Suurmeier	Black Hills Corporation	5	WECC

Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Deidre Altobell	Con Edison	1	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
					Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
					Randy Buswell	Vermont Electric Power Company	1	NPCC
					James Grant	NYISO	2	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					David Burke	Orange and Rockland	3	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC

Salvatore Spagnolo	New York Power Authority	1	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
David Kwan	Ontario Power Generation	4	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
Sean Cavote	PSEG	4	NPCC
Jason Chandler	Con Edison	5	NPCC
Tracy MacNicoll	Utility Services	5	NPCC
Shivaz Chopra	New York Power Authority	6	NPCC
Vijay Puran	New York State Department of Public Service	6	NPCC
David Kiguel	Independent	7	NPCC
Joel Charlebois	AESI	7	NPCC
Joshua London	Eversource Energy	1	NPCC

					Nicolas Turcotte	Hydro-Quebec (HQ)	1	NPCC
					Jeffrey Streifling	NB Power Corporation	1,4,10	NPCC
					Joel Charlebois	AESI	7	NPCC
					John Hastings	National Grid	1	NPCC
					Erin Wilson	NB Power	1	NPCC
					James Grant	NYISO	2	NPCC
					Michael Couchesne	ISO-NE	2	NPCC
					Kurtis Chong	IESO	2	NPCC
					Michele Pagano	Con Edison	4	NPCC
					Bendong Sun	Bruce Power	4	NPCC
					Carvers Powers	Utility Services	5	NPCC
					Wes Yeomans	NYSRC	7	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable

					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC

1. Do you agree with the language proposed in CIP-003-11 Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy finds the scope is too great for larger utilities to be successfully accomplished as well as within the timeframe suggested by these proposals.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Drafting Team (DT) has taken efforts to not prescribe any specific technological configurations throughout the modified requirement language. It is important to note that the SDT considered language requirements to include capabilities for centralized (or decentralized) electronic access capabilities between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) and using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s) – which simplifies the implementation of electronic access controls. In doing so, the DT has allowed the Responsible Entities flexibility in how they choose to implement controls and methods to accomplish said requirements. The DT is operating within the bounds of the SAR provided to it that was approved by the Standards Committee based upon recommendations from the LICRT Report.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
Although section 3.1.2 is within the scope of the SAR BPA still believes it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. The proposed language requires detection of known/suspected malicious communications for "inbound and outbound electronic remote access." There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5). BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS or the applicability be changed to bring it in-line with other requirements.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. Per your comments, the basis for the enhancements to CIP-003 are from the October 2022 Low Impact Criteria Review Report – of which developed SARs based on FERC requests. The language used in section 3.1.2 is in the same vain as the approved language in Section 6.3 Vendor Electronic Remote Access Security Controls of CIP-003-9 with the scope being expanded to all electronic access that meets section 3.1 (i), (ii), and (iii), instead of being vendor specific.

Michael Johnson - Michael Johnson On Behalf of: Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; Tyler Brun, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment
Section 3.1.2 is requiring malicious communication detection which is not even required at medium sites (CIP-005-7 or CIP-005-8). It does not make sense to require it at lows unless there is going to be a change to require it for mediums as well.

Section 4 and Section 5 cannot be accomplished without knowing the individual assets that are part of the low impact Cyber Systems. The note that states a list of low assets in not required is a fallback that entities are using to justify not accomplishing the requirements of section 4 and 5. The requirement to classify individual assets should be required to accomplish all the changes in requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT understands this is a new requirement for lows, however overall there are more requirements associated with mediums than there are lows (please see the low impact report). The language used in section 3.1.2 is similar to the approved language in Section 6.3 Vendor Electronic Remote Access Security Controls of CIP-003-9 with the scope being expanded to all electronic access that meets section 3.1 (i), (ii), and (iii), instead of being vendor specific. The DT has not added proposed language that would require the identification of an asset's low impact BES Cyber Systems (BCS) or their collective BES Cyber Assets (BCA). Please refer to figures 4 and 5 of the Technical Rationale document for examples of how to accomplish Part 3.1.4 without knowing the individual BCSs or their BCAs. For Part 3.1.5, the DT has preserved the approved language under Section 6.1 Vendor Electronic Remote Access Security Controls of CIP-003-9 with the only change being removing it from Section 6 and appending it to Section 3. Part 3.1.5 is focused on documenting the method used to determine vendor remote access, but does not require a list of low impact BCSs or their BCAs.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1 - RF	
Answer	No
Document Name	
Comment	
The additional language in Section 3 does not fully mitigate the coordinated attack risk for LIBCS as the controls do not address distributed network accessibility from IBRs. Also, the suggested Requirements are more stringent than BCS classified as Medium Impact without ERC.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT understands this is a new requirement for lows, however overall there are more requirements associated with mediums than there are lows (please see the low impact report). The SDT is only allowed to work within the constraints of the SAR and cannot fully address distributed network accessibility from IBRs.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
CIP-003-11 Attachment 1, Section 3, Part 3.1.2 does not specify whether the requirement is to detect known or suspected malicious communications for ***both*** encrypted and/or unencrypted traffic. SMUD recommends changing the language to: 3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic ***unencrypted*** access;	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The language leaves open the possibility to use a variety of means to satisfy the action of detecting malicious communications. Section 3.1 Parts (i), (ii), and (iii) define the electronic access covered by Section 3. If those conditions are met then the controls must be implemented regardless if the is encrypted or unencrypted. The SDT left the standard open for entities to match their chosen technologic solution to their architecture.	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	

Comment	
We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language. CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. We recommend merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT created CIP-003-11 to specifically build upon the approved CIP-003-9 standard. The DT created CIP-003-12 to incorporate the CIP-003-10 modifications which have been approved by the NERC Board of Trustees as a way of wholistically incorporating both Project 2016-02 and Project 2023-04 changes to CIP-003, in the case that CIP-003-10 is approved by FERC before CIP-003-11. The Implementation Plan for this version also includes the provisions for both CIP-003-10 and CIP-003-11. For additional information please see the industry webinar recording.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
For Attachment 1, Part 3.1.2 – As proposed, this currently applies to all low impact BES Cyber Systems but does not apply to Medium Impact Facilities that are not Control Centers. The DT needs to ensure that the reliability risks of both low and medium impact facilities are appropriately and consistently applied.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT understands this is a new requirement for lows, however overall there are more requirements associated with mediums than there are lows (please see the low impact report). Per your comments, the basis for the enhancements to CIP-003 are from the October 2022 Low Impact Criteria Review Report – of which developed SARs based on FERC requests. The language used in section 3.1.2 is in the same vain as the approved language in Section 6.3 Vendor Electronic Remote Access Security Controls of CIP-003-9 with the scope being expanded to all electronic access that meets section 3.1 (i), (ii), and (iii), instead of being vendor specific.	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
Comments: Section 3.1.3 could be reworded to be less confusing. The intent appears to be requiring authentication of remote access into a LIBCS based on the verbiage "through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted". However, the Section 3.1 that is referenced may bring local access into question, as Section 3.1 includes both inbound (remote) and outbound access (local) from the LIBCS as it only mentions traffic "between a [LIBCS] and a Cyber Asset(s) outside the asset containing [LIBCS]" with no mention of traffic direction or origination point. This could require authentication in all cases of network access where traffic is leaving the site, if users could even be 100% aware of the destination of all information generated by their session and authentication may need to be implemented for all sessions. It may be difficult to implement an outbound access solution, and would potentially bring authentication prior to connecting to a non-CIP system into scope. The Technical Rationale section again supports the notion that the scope includes access "from a remote client outside the asset containing the LIBCS and destined for a LIBCS within the asset". This specifically notes an origination point and a traffic direction, which is missing in the language of the requirement. The requirement should specify traffic origination and direction for authentication if it is indeed scoped only to remote access. If local network access is intended to be included, then a requirement for remote access authentication and a separate requirement for local system access should be created and mirror the requirements of CIP-005 and CIP-007.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The intent of the language addresses authentication for remote access which sources outside of the low impact BES Cyber System and asset. The phrase, "through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted" is included in Section 3.1.3 to clarify scoping. As 3.1.3 is written at a different granularity of "network(s) containing" (which is not mentioned in the romanettes), this phrasing simply clarifies that the intended scope remains those networks through which the specific access described in the Section 3.1 romanettes is subsequently permitted. As 3.1.3 requires authentication of the user before access to the network(s) containing low impact BCS, it is not applicable to physically local logon to the low impact BCS and subsequent outbound access since the origin of the access is the network(s) containing the low impact BCS.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to NPCC Regional Standards Committee.	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	No
Document Name	
Comment	

Commented [AO1]: Jay to add about outbound

Commented [AO2R1]: Explain why the language is in 3.1

Commented [JC3R1]: SDT: check this response. It is a valid point made in the comment, but I think putting directionality into 3.1.3 will further complicate the requirement. Therefore, the response here rests on the fact that if the origin of the access IS the network containing, the requirement is just not applicable because there is no "prior to" point at which to perform it.

Commented [AO4R1]: complete

• The proposed changes to the language in section 1.1 of the “C. Compliance” area of the standard is problematic. What “Applicable Governmental Authority” could enforce compliance other than FERC, NERC or the Regional Entity in their “respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions”? How is “Applicable” defined? • Language in section 3, particularly 3.1.1 through 3.1.6 and 3.2, is perceived to be arduous and expensive to implement and maintain compliance with, and could result in negative results. More money and people will be required to ensure compliance rather than focus on the goal, which is to secure the systems against adversaries. Low impact assets are low impact or they are not. By adding the requirements to permit only necessary inbound and outbound access, detect known or suspected malicious communications, authenticate each user prior to permitting access, protecting user authentication information, determine vendor electronic access and disabling vendor access this is, in essence, raising the level of compliance requirements, and subsequently to the audit requirements thereof, to a state equivalent to Medium impact. • Recommendations: Leave it alone. Unless there are metrics to prove that the existing standards are not adequately protecting the critical infrastructure relating directly to root causes identifying these sections of the standards, then modifications to them should not be made, especially modifications that would result in an undue burden to the financial stability of the Responsible entity due to additional compliance requirements, labor, capital costs and potential fines for non-compliance. • Cancel all changes to CIP-003-9 and the SAR should be reviewed and recommendations made to change the criterion for Medium impact based on objective and measurable criteria rather than expect responsible entities to acquiesce to the recommendation by the LICRT to change all low impact requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The changes in the compliance area of the standard are to align with the new standard template. Per Appendix 2 of the ROP: ""“Applicable Governmental Authority” means the FERC within the United States and the appropriate governmental authority with subject matter jurisdiction over reliability in Canada and Mexico." The DT understands this is a new requirement for lows, however overall there are more requirements associated with mediums than there are lows (please see the low impact report). The SDT is only allowed to work within the constraints of the SAR and does not have the authority to cancel all changes to CIP-003-9.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	

Commented [AO5]: NERC to write a response
Commented [AO6R5]: Complete, team check

Answer	Yes
Document Name	
Comment	
Duke Energy supports the proposed language.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI's comments: "EEI supports the language proposed in CIP-003-11 Attachment 1."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Michelle Pagano - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	Yes
Document Name	
Comment	

Supporting EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, please see response to EEI.	
Matt Carden - Southern Company - Southern Company Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Southern Company is in agreement with EEI along with the following comment: Southern asks that a clarification as to intent be made at least in the Technical Rationale document that for 3.1.3 when it states "Authenticate each user" that it does not imply that every remote user must have an individual user account, precluding the use of shared accounts by valid and authorized users for remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The drafting team made clarifying changes to the Technical Rationale.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	

Commented [AO7]: Did we make these changes in the TR?

Exelon is aligned with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, please see response to EEI.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) supports the proposed language in CIP-003-11 Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments, please see response to EEI.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
TVA requests clarification that a list of users is not required to be maintained for vendor remote access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please refer to the note under requirement R2.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the language proposed in CIP-003-11 Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the proposed language in CIP-003-11 Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See comments from EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Michael Moltane - International Transmission Company Holdings Corporation - 1	
Answer	Yes
Document Name	

Comment	
Support EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Fausto Serratos - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Kerrigan - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Thank you for your support.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Leshel Hutchings - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Carey Salisbury - Santee Cooper - 5, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	

We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language. CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. We recommend merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT created CIP-003-11 to specifically build upon the approved CIP-003-9 standard. The DT created CIP-003-12 to incorporate the CIP-003-10 modifications which have been approved by the NERC Board of Trustees as a way of wholistically incorporating both Project 2016-02 and Project 2023-04 changes to CIP-003, in the case that CIP-003-10 is approved by FERC before CIP-003-11. The Implementation Plan for this version also includes the provisions for both CIP-003-10 and CIP-003-11. For additional information please see the industry webinar recording.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	
Document Name	
Comment	
WEC Energy Group supports the language proposed in CIP-003-11.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

2. Do you agree with the language proposed in CIP-003-11 Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	No
Document Name	
Comment	
• Suggested language changes throughout section 3 have completely vacated the approved CIP-003-8 and the changes are monumental. All changes are perceived to be arduous and expensive to implement and maintain compliance with, and could result in negative results. More money and people will be required to ensure compliance rather than focus on the goal, which is to secure the	

systems against adversaries. Low impact assets are low impact or they are not. By adding the requirements to show the ability to detect and authenticate, protect, determine and disable, this is, in essence, raising the level of compliance requirements, and subsequently the audit requirements thereof, to a state equivalent to a Medium impact facility. • Cancel all changes to CIP-003-9 and the SAR should be reviewed and recommendations made to change the criterion for Medium impact based on objective and measurable criteria rather than expect responsible entities to acquiesce to the recommendation by the LICRT to change all low impact requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT understands this is a new requirement for lows, however overall there are more requirements associated with mediums than there are lows (please see the low impact report). The SDT is only allowed to work within the constraints of the SAR and does not have the authority to cancel all changes to CIP-003-9.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to NPCC.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No

Document Name	
Comment	
Ameren suggests removing OEM sheets from the list of documentation. An OEM would not provide recommendations on how to use a device or consider what is necessary for electronic access by the entity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The use of a OEM is only a example of what may be used, but some may provide examples of ports and services that could be used for operational purposes.	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	
We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language. CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. We recommend merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT created CIP-003-11 to specifically build upon the approved CIP-003-9 standard. The DT created CIP-003-12 to incorporate the CIP-003-10 modifications which have been approved by the NERC Board of Trustees as a way of wholistically	

incorporating both Project 2016-02 and Project 2023-04 changes to CIP-003, in the case that CIP-003-10 is approved by FERC before CIP-003-11. The Implementation Plan for this version also includes the provisions for both CIP-003-10 and CIP-003-11. For additional information please see the industry webinar recording.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST suggests adding username/password to the list of user authentication mechanisms cited in Section 3, Item 3 as possible ways to address requirement 3.1.3 of Attachment 1, Section 3. We believe this addition to be justified by the fact the Technical Rationale document mentions username and password in its discussion of Attachment 1, Section 3.1.4.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. There are many possible ways to meet the requirements of Section 3.1.3, the examples listed are only a few and does not limit the implementation of the section if a mechanism is not listed.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1 - RF	
Answer	No
Document Name	
Comment	
Please refer to the comments provided in Question 1 above.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments, please see response in question 1.	
Michael Johnson - Michael Johnson On Behalf of: Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; Tyler Brun, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
Do not agree with 3.1.2 for Malware Detection unless it is going to be required at medium sites as well.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, this is not an exhaustive list but a sampling of options to meet the requirement.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Although section 3.1.2 is within the scope of the SAR BPA still believes it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. The proposed language requires detection of known/suspected malicious communications for “inbound and outbound electronic remote access.” There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5). BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS or the applicability be changed to bring it in-line with other requirements.	

BPA recommends the SDT include a documentation option outside of OEM spec sheets as, depending on equipment, these may not be available. BPA also believes internal proof of testing should be allowable in case OEM was not available.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT understands this is a new requirement for lows, however overall there are more requirements associated with mediums than there are lows (please see the low impact report). The use of a OEM is only a example of what may be used, but some may provide examples of ports and servcies that could be used for operational purposes.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy finds the scope is too great for larger utilities to be successfully accomplished as well as within the timeframe suggested by these proposals.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Attachment 2 is not inclusive of all measures and simply a finite list of examples.	
Michael Moltane - International Transmission Company Holdings Corporation - 1	
Answer	Yes
Document Name	
Comment	

Commented [AO8]: Circle back to this after discussing IP

Support EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for your support, please see response to EEI.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See comments from EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for your support, please see response to EEI.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the proposed language in CIP-003-11 Attachment 2.	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the language proposed in CIP-003-11 Attachment 2 as it conforms with the revised language in Attachment 1. EEI provides the non-substantive edit to change the case of the terms “Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)” and “Security Incident and Event Management (SIEM)” in Attachment 2, Section 3, part 2 to lowercase because they are not NERC Glossary defined terms and do not require capitalization.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. We have addressed the capitalization issue in the standard.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute for Question #2.	
Likes 0	

Commented [AO9]: Circle back to this, would be more changes than the two terms they mentioned

Commented [AO10R9]: Discussed with Kristine, might have changes in sections this team did not modify

Dislikes 0	
Response	
Thank you for your support, please see response to EEI.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support, please see response to EEI.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CEHE tentatively supports the proposed language in CIP-003-11 Attachment 2, but would like to request further clarification on Section 3, part 1, bullet 3 in the snippet included below: **Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:** **1. For Section 3.1.1, documentation showing the permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, such as:**	

• Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s); **• Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways); or** ***• Original Equipment Manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.*** CEHE requests further clarification on the process in determining how the inclusion of OEM specification sheets would be considered sufficient evidence for Electronic Access Controls. CEHE understands that the provided example is merely a suggestion but would like to request more clarification on how this could be utilized.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The use of a OEM is only a example of what may be used, but some may provide examples of ports and services that could be used for operational purposes.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligned with EEI in response to this question.	
Likes 0	
Dislikes 0	

Response	
Thank you for your support, please see response to EEI.	
Matt Carden - Southern Company - Southern Company Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Southern Company is in agreement with the EEEI comments: EEI supports the language proposed in CIP-003-11 Attachment 2 as it conforms with the revised language in Attachment 1. EEI provides the non-substantive edit to change the case of the terms “Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)” and “Security Incident and Event Management (SIEM)” in Attachment 2, Section 3, part 2 to lowercase because they are not NERC Glossary defined terms and do not require capitalization.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support, please see response to EEI.	
Michelle Pagano - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	Yes
Document Name	
Comment	
Supporting EEI comments	
Likes 0	

Dislikes 0	
Response	
Thank you for your support, please see response to EEI.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
EEI provides the non-substantive edit to change the case of the terms “Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)” and “Security Incident and Event Management (SIEM)” in Attachment 2, Section 3, part 2 to lowercase because they are not NERC Glossary defined terms and do not require capitalization.“	
Likes 0	
Dislikes 0	
Response	
Thank you for your support, please see response to EEI.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the proposed language and supports the non-substantive revisions proposed by EEI.	
Likes 0	
Dislikes 0	
Response	

Thank you for your support, please see response to EEI.	
Carey Salisbury - Santee Cooper - 5, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Leshel Hutchings - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Kerrigan - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Fausto Serratos - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	
We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language. CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. We recommend merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT created CIP-003-11 to specifically build upon the approved CIP-003-9 standard. The DT created CIP-003-12 to incorporate the CIP-003-10 modifications which have been approved by the NERC Board of Trustees as a way of wholistically incorporating both Project 2016-02 and Project 2023-04 changes to CIP-003, in the case that CIP-003-10 is approved by FERC before CIP-	

003-11. The Implementation Plan for this version also includes the provisions for both CIP-003-10 and CIP-003-11. For additional information please see the industry webinar recording.

3. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-11. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with detailed explanation.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy finds this an enormous undertaking for larger organizations/entities to meet expectations within the 3-year implementation plan. Considerations for network buildouts and firewalls as well as coordination with transmission planning and implementation must be taken into consideration. FirstEnergy requests the Drafting Team to consider a staged implementation plan to allow for planning, scheduling, budgeting, and implementing to ensure full compliance toward the scope of CIP-003 and protection of the BES. These required steps would necessitate a longer implementation that allows 18-24 months to develop an implementation plan, budget and staff for the implementation over time, and permit a number of years for staged implementations following CIP-003-09 based on reasonable criteria set by the utility which would, of course, be overseen by the RE.	
Likes 0	
Dislikes 0	
Response	
The DT thanks you for your comment, the team has made changes to the IP to ensure a full 36 months for the work needed to comply.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No

Document Name	
Comment	
Southern Indiana Gas and Electric d/b/a CenterPoint Energy Indiana South (SIGE) has concerns that having multiple versions of the standard and simultaneously working on modifications, is causing confusion. Without having approved versions, further proposed revisions seem a bit premature.	
Likes 0	
Dislikes 0	
Response	
The DT has worked to reduce the confusing with the next posting and will be posting a single version with a single implementation plan.	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	
CIP-003-11 and CIP-003-12 implementation plan should be combined and repost after FERC approves CIP-003-10 in a new ballot. NPCC recommends only having one implementation timeframe and TFIST prefers 36-month timeframe.	
Likes 0	
Dislikes 0	
Response	
The DT has worked to reduce the confusing with the next posting and will be posting a single version with a single implementation plan.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	

Comment	
Dominion Energy recommends a 5-year implementation plan with a phased approach for the implementation of devices required to achieve compliance with the IDS / IDP provisions in Part 3.1.2, The milestones and methodology for the implementation should be at the direction of the Registered Entity.	
Likes 0	
Dislikes 0	
Response	
The DT thanks you for your comment, the team has made changes to the IP to ensure a full 36 months for the work needed to comply.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to NPCC.	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	No
Document Name	
Comment	

• By adding the requirements to show the ability to detect and authenticate, protect, determine and disable, this is, in essence, raising the level of compliance requirements, and subsequently the audit requirements thereof, to a state equivalent to a Medium impact facility. • Cancel all changes to CIP-003-9 and the SAR should be reviewed and recommendations made to change the criterion for Medium impact based on objective and measurable criteria rather than expect responsible entities to acquiesce to the recommendation by the LICRT to change all low impact requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT understands this is a new requirement for lows, however overall there are more requirements associated with mediums than there are lows (please see the low impact report). The SDT is only allowed to work within the constraints of the SAR and does not have the authority to cancel all changes to CIP-003-9.	
Carey Salisbury - Santee Cooper - 5, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Santee Cooper would request a five-year implementation plan for the additional security controls listed in CIP-003-11. It would take time and money to implement these controls into over 100 low impact sites. Santee Cooper is in the process of rolling out routable communication to its low impact sites and this would require us to revisit each site to implement these additional security controls.	
Likes 0	
Dislikes 0	
Response	
The DT thanks you for your comment, the team has made changes to the IP to ensure a full 36 months for the work needed to comply.	

Commented [AO11]: This is the same response we have used above for this entity. Is it appropriate or should it be modified?

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
The implementation plan for CIP-003-11 includes a footnote that states: "1 On May 9, 2024, the NERC Board of Directors approved the retirement of Reliability Standard CIP-003-9, which *was* scheduled to take effect on April 1, 2026, when it approved revised Reliability Standard CIP-003-10. CIP-003-10 is pending regulatory approval. This implementation plan is intended to retire whichever version of the CIP-003 Reliability Standard that is then in effect." With many concurrent CIP-003 version projects, it is possible that CIP-003-11 gets approved before CIP-003-10. Regardless of which version gets approved first, the wording in the footnote states that CIP-003-9 *was* to take effect on April 1, 2026. Is CIP-003-9 still effective April 1, 2026, or will CIP-003-10 or CIP-003-11 (or CIP-003-12) supersede the effective date of CIP-003-9?	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment, the team has made changes to the IP to ensure a full 36 months for the work needed to comply and to remove confusion will be posting on a single standard and single IP.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI's comments: "EEI supports the proposed three-year implementation plan for CIP-003-11 and appreciates the drafting team's acknowledgement that the revisions proposed in CIP-003-11 do not conflict but build upon the implementation of CIP-003-9 which has an effective date of April 1, 2026, however, we recommend removing the footnote on page 1 of the implementation plan regarding the retirement of CIP-003-9. The effective dates and retirement dates of the different versions of CIP-003 are discussed clearly in the General Considerations section and Retirement Date Section. Including the information in a footnote has not been standard practice and the Implementation Plan is clearer without it."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Michelle Pagano - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	Yes
Document Name	
Comment	

Supporting EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Matt Carden - Southern Company - Southern Company Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Southern Company is in agreement with the EEI comments: EEI supports the proposed three-year implementation plan for CIP-003-11 and appreciates the drafting team's acknowledgement that the revisions proposed in CIP-003-11 do not conflict but build upon the implementation of CIP-003-9 which has an effective date of April 1, 2026, however, we recommend removing the footnote on page 1 of the implementation plan regarding the retirement of CIP-003-9. The effective dates and retirement dates of the different versions of CIP-003 are discussed clearly in the General Considerations section and Retirement Date Section. Including the information in a footnote has not been standard practice and the Implementation Plan is clearer without it.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes

Document Name	
Comment	
Exelon is aligned with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CEHE supports the comments as submitted by the Edison Electric Institute (EEI) EEI Comments: EEI supports the proposed three-year implementation plan for CIP-003-11 and appreciates the drafting team's acknowledgement that the revisions proposed in CIP-003-11 do not conflict but build upon the implementation of CIP-003-9 which has an effective date of April 1, 2026, however, we recommend removing the footnote on page 1 of the implementation plan regarding the retirement of CIP-003-9.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Daniel Gacek - Exelon - 1	

Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI's comments on question 7: Black Hills Corporation is concerned about the proposed effective date for CIP-003-12. CIP-003-12 is the alignment of the Project 2023-04 changes with conforming changes from Project 2016-02 Virtualization, which is pending FERC approval. Given its pending approval, it is difficult to understand if the 24-month period would provide a shorter implementation timeframe than the 36-month period proposed for CIP-003-11. EEI supports a 36-month implementation period for the draft revisions and asks for that timeframe regardless of the version of CIP-003 approved.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute for Question #3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed three-year implementation plan for CIP-003-11 and appreciates the drafting team's acknowledgement that the revisions proposed in CIP-003-11 do not conflict but build upon the implementation of CIP-003-9 which has an effective date of April 1, 2026, however, we recommend removing the footnote on page 1 of the implementation plan regarding the retirement of CIP-003-9. The effective dates and retirement dates of the different versions of CIP-003 are discussed clearly in the General Considerations section and Retirement Date Section. Including the information in a footnote has not been standard practice and the Implementation Plan is clearer without it.	
Likes 0	
Dislikes 0	

Response	
The DT thanks you for your comment, the team has made changes to the IP to ensure a full 36 months for the work needed to comply and to remove confusion will be posting on a single standard and single IP.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the proposed three (3) year implementation plan for CIP-003-11.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See comments from EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for your support, please see response to EEI.	

Michael Moltane - International Transmission Company Holdings Corporation - 1	
Answer	Yes
Document Name	
Comment	
Support EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for your support, please see response to EEI.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
WEC Energy Group supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support, please see response to EEI.	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Fausto Serratos - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Kerrigan - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michael Johnson - Michael Johnson On Behalf of: Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; Tyler Brun, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Leshel Hutchings - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	

CIP-003-11 and CIP-003-12 implementation plan should be combined and repost after FERC approves CIP-003-10 in a new ballot. NPCC recommends only having one implementation timeframe and TFIST prefers 36-month timeframe.	
Likes 0	
Dislikes 0	
Response	
The DT thanks you for your comment, the team has made changes to the IP to ensure a full 36 months for the work needed to comply and to remove confusion will be posting a single standard and single IP.	

4. The DT believes the language of CIP-003-11 addresses the issues outlined in the SAR in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical, or procedural justification.	
Carey Salisbury - Santee Cooper - 5, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Implementing CIP-003-11 would not be cost effective for Santee Cooper. We are installing routable communication at our low impact facilities. However, when developing the plans to roll out routable communication to our low impact facilities we didn't consider CIP-003-11. To comply with CIP-003-11 we would have to add additional support and incur significant cost in adding equipment or software licenses to comply.	
Likes 0	

Dislikes 0	

Response

The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of BES Cyber Systems against compromise. Considering this, cost effectiveness is achieved by the ability to implement changes with widely used industry tools and practices for securing network access to sensitive data, which makes them cost-effective. The required controls are common access controls in the current landscape of frequent and persistent cyber-attack attempts.

The DT intends that the proposed approach relies on common IT technical skills.

Required controls are not detailed for individual low-impact cyber systems, they allow authentication for a "network(s)," which can refer to one or several networks. This eliminates the need for repetitive or re-authentication for sub-networks. Instead, authentication is specified at the level of "networks containing" or "asset containing."

Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez

Answer	No
Document Name	

Comment

• Just the recommended changes to Appendix 2 make the DT claims that the language addresses the issues outlined in the SAR cost effectively objectively false. Just the technology needed to comply with the language makes that claim unreasonable, much less the cost of labor for implementation, maintenance, audit, troubleshooting and lifecycle replacement.

Likes 0	
Dislikes 0	

Response

The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of BES Cyber Systems against

compromise. Considering this, cost effectiveness is achieved by the ability to implement changes with widely used industry tools and practices for securing network access to sensitive data, which makes them cost-effective. The required controls are common access controls in the current landscape of frequent and persistent cyber-attack attempts. The DT intends that the proposed approach relies on common IT technical skills. The DT clarified to include "Intermediate System" implementations providing additional permitted options. The DT has clarified that "Intermediate System" implementations are included, allowing for additional authorized alternatives.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy does not think the methods listed in the SAR are cost effective. Any methods that require installation of devices that support IDS/IDP for Low Impact within larger Registered Entities is an expensive undertaking. Other methods that can be used to comply with the standard, such as manual reviews and SIEMs also have a significant cost associated with them.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of BES Cyber Systems against compromise. Considering this, cost effectiveness is achieved by the ability to implement changes with widely used industry tools and practices for securing network access to sensitive data, which makes them cost-effective. The required controls are common access controls in the current landscape of frequent and persistent cyber-attack attempts. The DT intends that the proposed approach relies on common IT technical skills.	

Required controls are not detailed for individual low-impact cyber systems, they allow authentication for a "network(s)," which can refer to one or several networks. This eliminates the need for repetitive or re-authentication for sub-networks. Instead, authentication is specified at the level of "networks containing" or "asset containing." The DT clarified to include "Intermediate System" implementations providing additional permitted options. The DT has clarified that "Intermediate System" implementations are included, allowing for additional authorized alternatives.	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	
We have no comments on the cost-effectiveness of CIP-003-11. We will note that the cost effectiveness of CIP-003-12 was not asked in this comment form.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
SMUD views the language in CIP-003-11 as neither cost effective nor cost ineffective. If CIP-003-11 Attachment 1, Section 3, Part 3.1.2 requires the detection of suspected malicious communications that is ***encrypted*** [emphasis added], then the language of CIP-003-11 would not be cost effective due to the additional cost of implementing the inspection of encrypted traffic.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT will take into consideration your comments. The DT intends that the proposed approach relies on common IT technical skills. Considering this, cost effectiveness is achieved by the ability to implement changes with widely used industry tools and practices for securing network access to sensitive data, which makes them cost-effective.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1 - RF	
Answer	No
Document Name	
Comment	

There will be costs associated with implementing additional IDS, monitoring, equipment upgrades, and resources to both implement and maintain. It is uncertain at this time if the language will provide a cost-effective solution.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT will take into consideration your comments. The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards.	
Michael Johnson - Michael Johnson On Behalf of: Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; Tyler Brun, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E will not comment on costs that have not been analyzed, there are too many factors that will go into this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	

Reclamation identifies that more information is needed to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
See FirstEnergy's comments above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

There will be costs associated with adding new software/technology and upgrading legacy equipment.	
Likes 0	
Dislikes 0	
Response	
The DT understands that implementing changes in the standard may incur costs in effort and implementation, as is the case with any changes made to standards. The proposed changes are suitable given the necessity to protect the reliability of BES Cyber Systems against compromise.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
It cannot be determined at this time if the language of CIP-003-11 addresses the issues in a cost effective manner.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the revisions and does not have any concerns regarding the cost effectiveness.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	

Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matt Carden - Southern Company - Southern Company Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Kerrigan - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Fausto Serratos - Los Angeles Department of Water and Power - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Michael Moltane - International Transmission Company Holdings Corporation - 1	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren has no comment on the cost effectiveness of the project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	

Document Name	
Comment	
We have no comments on the cost-effectiveness of CIP-003-11. We will note that the cost effectiveness of CIP-003-12 was not asked in this comment form.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	

CEHE does not comment on cost.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE does not comment on cost.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	

5. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
FirstEnergy thanks the DT for their work on these drafts but requests an increase in the implementation plan's timeline to ensure efficient and manageable protection of the Bulk Electric System.	
Likes 0	
Dislikes 0	
Response	
Thank you for the comment. The drafting team has kept 36 months in the Implementation Plan with one change for Attachment 1 Section 3.1.2.	

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	
Document Name	
Comment	
Duke Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Fausto Serratos - Los Angeles Department of Water and Power - 3	
Answer	
Document Name	
Comment	
CIP-003-11 references “Technical Rationale for Reliability Standard CIP-003-11 – Low Impact BES Cyber Security Criteria Revisions”. We recommend the following sentences be reviewed: 1) On page 1 of the Technical Rationale, please note that the following is not a complete sentence: “Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified.” 2) On page 6 of the Technical Rationale, under Section 3.1.3, says “(allowing, establishing, gaining)” after “permitting”. It is recommended that this phrase in the parentheses should just be deleted. It is unnecessary and confusing, given that these other words do not appear in the standard.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments, the team has addressed both of these issues in the draft TR.	
Robert Kerrigan - Los Angeles Department of Water and Power - 5	
Answer	
Document Name	
Comment	
Comments: CIP-003-11 references “Technical Rationale for Reliability Standard CIP-003-11 – Low Impact BES Cyber Security Criteria Revisions”. We recommend the following sentences be reviewed: 1) On page 1 of the Technical Rationale, please note that the following is not a complete sentence: “Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified.” 2) On page 6 of the Technical Rationale, under Section 3.1.3, says “(allowing, establishing, gaining)” after “permitting”. It is recommended that this phrase in the parentheses should just be deleted. It is unnecessary and confusing, given that these other words do not appear in the standard. The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering the following questions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, the team has addressed both of these issues in the draft TR.	
Richard Vendetti - NextEra Energy - 5	

Answer	
Document Name	
Comment	
NEE supports EEI's comments: "The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering the following questions."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Michael Johnson - Michael Johnson On Behalf of: Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; Tyler Brun, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	
Document Name	
Comment	
The rationale comments that jump host for low sites is not required, but in reality, there are limited ways to meet the requirements stated here other than using jump hosts. Since it is required in CIP 005, it should be here too. The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering the following questions.	
Likes 0	
Dislikes 0	
Response	

Thank you for the comment. The drafting team's intent was not to prescribe the need for a jump host and accommodate alternative methods for complying with the additional protections outlined in the SAR.	
Matt Carden - Southern Company - Southern Company Services, Inc. - 1	
Answer	
Document Name	
Comment	
Southern Company is in agreement with the EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligned with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Daniel Gacek - Exelon - 1	

Answer	
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	
Black Hills Corporation is concerned about having multiple CIP-003 projects and multiple virtualization projects occurring simultaneously as it is becoming difficult to maintain oversight of the changes to a degree that allows sufficient review. In addition, how is NERC ensuring that the direction of these multiple projects maintain alignment?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team has posted a draft CIP-003-11 that is this teams changes on top of NERC board approved CIP-003-10 (virtualization changes). This is also the path forward for the Implementation Plan. This version will contain all changes to date in one version.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	

Answer	
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	
Document Name	
Comment	
The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering the following questions.	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Thank you for your response.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	

Comment
NST considers it unfortunate that industry has been afforded only a single, up or down vote on two distinctly different implementation plans, one for CIP-003-11 and one for CIP-003-12. Our "Negative" vote reflects our concerns about only the "-12" implementation plan. Given the opportunity to vote on just the "-11" implementation plan, our vote would have been "Affirmative."

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The drafting team has posted a draft CIP-003-11 that is this teams changes on top of NERC board approved CIP-003-10 (virtualization changes). This is also the path forward for the Implementation Plan. This version will contain all changes to date in one version.

Carver Powers - Utility Services, Inc. - 4	
Answer	
Document Name	

Comment
In the Technical Rationale the information in figure 4 should be included in the diagram for figure 1 and figure 2. Figure 4 provides confusion because it does not meet the criteria listed in 3.1.1 and 3.1.2. Recommend that the Technical Rationale clearly states for each diagram if they are depicting compliance with only an individual subsection of the requirement. In figure 5 can the jump host now be part of an associated data center for a Control Center?

Likes 0	
Dislikes 0	

Response
Thank you for your comments, the drafting team has made edits to the Technical Rationale and Figure 5.

Commented [AO12]: I added this based on the work the team did, any additional details to include?

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	
Document Name	
Comment	
We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language. CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. We recommend merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The drafting team has posted a draft CIP-003-11 that is this teams changes on top of NERC board approved CIP-003-10 (virtualization changes). This is also the path forward for the Implementation Plan. This version will contain all changes to date in one version.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	
We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language. CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. We recommend merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team has posted a draft CIP-003-11 that is this teams changes on top of NERC board approved CIP-003-10 (virtualization changes). This is also the path forward for the Implementation Plan. This version will contain all changes to date in one version.	
Leshel Hutchings - AEP - 3	
Answer	
Document Name	
Comment	

VCA is used in the document but never defined as Virtual Cyber Asset anywhere, if an end user needs to look up acronym, it would be useful to define VCA in the Glossary of Terms.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Virtual Cyber Asset was a defined term developed under Project 2016-02 and was board approved in May 2024. The team has spelled out Virtual Cyber Asset during its first use in the standard prior to using the acronym. NERC has identified the problem of glossary terms only being included in the Glossary of Terms after FERC approval and will be adding a new section titled "Pending Regulatory Approval" where terms can be included prior to FERC approval.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
See comments from EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	

Commented [AO13]: Alison look into when terms get into glossary and add response

None.	
Likes 0	
Dislikes 0	
Response	
Michael Moltane - International Transmission Company Holdings Corporation - 1	
Answer	
Document Name	
Comment	
Support EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment, please see response to NPCC.	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	
Document Name	
Comment	
• Cancel all changes to CIP-003-9 and the SAR should be reviewed and recommendations made to change the criterion for Medium impact based on objective and measurable criteria rather than expect responsible entities to acquiesce to the recommendation by the LICRT to change all low impact requirements resulting in unreasonable technological and labor costs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT understands this is a new requirement for lows, however overall there are more requirements associated with mediums than there are lows (please see the low impact report). The SDT is only allowed to work within the constraints of the SAR and does not have the authority to cancel all changes to CIP-003-9.	

The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering this question. **6. Do you have any concerns in the way CIP-003-10 (Project 2016-02 changes) and CIP-003-11 (Project 2023-04 changes) were combined to create standard CIP-003-12?**	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
EACMS and PCAs have previously not been applicable for Low-Impact CIP Assets. However, SCI could be introducing an opportunity for EACMS and PCA requirements. Would a centralized engineering or cyber tool suite that is only used to support Low-Impact CIP assets from outside the ESP qualify as a SCI? If so, would EACMS or PCA requirements then apply to such a system even if such protections are not required for the BCS? Ameren suggests adding a statement to the SCI definition clarifying which requirements are for low, medium, and high impact BCS or SCI.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT asserts that shared Cyber Assets that support ONLY ONE impact category, such as low, do not meet the definition of SCI. As EACMS and PCAs are only associated with ESP's for medium and high impact BCS and if they are supported on the same SCI along with an engineering or cyber tool VCA that itself is only used for lows, then it would be SCI as it is supporting VCAs of differing impact levels (or associated with differing impact levels). The SCI itself would be subject to CIP requirements that have "SCI supporting…" in their applicability, and the individual VCAs would be subject to the requirements based on what the VCA is.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST has no concerns about the content of proposed CIP-003-12. We do, however, have concerns about the implementation plan, as explained below.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CEHE supports the comments as submitted by EEI.	

EEI has reviewed the redline of CIP-003-9 to CIP-003-12 and understands that the revisions make conforming changes in alignment with Project 2016-02 and is supportive of the alignment.	
Likes 0	
Dislikes 0	
Response	
Thank your for your comment. See response to EEI.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Tacoma Power has no concerns.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Carey Salisbury - Santee Cooper - 5, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	

Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	Yes
Document Name	
Comment	
• Expecting responsible entities to understand the unintended consequences of multiple changes to the same standard without any implementation time or settling time is unreasonable. Suggest following precedent set during changes to CIP-015 by making suggested changes in a new standard such as CIP-016, where CIP-003 would remain unchanged and requirements for low impact assets would be captured in the new standard. We do not agree that any changes should be made for Low Impact, but if forced to do so, the recommendation is to create a new standard. • Recommend canceling all changes to CIP-003-9 and the SAR should be reviewed and recommendations made to change the criterion for Medium impact based on objective and measurable criteria rather than expect responsible entities to acquiesce to the recommendation by the LICRT to change all low impact requirements.	
Likes 0	
Dislikes 0	
Response	

The SDT is completing its scope from the approved SAR as assigned by the Standards Committee. As to a new standard, the SDT asserts that from the beginning of V5, "low only" entities have been able to get all of their requirements from CIP-002 and CIP-003 (with CIP-012 if a Control Center). For lows, CIP-003 contains a requirement for a cyber security plan. The specifics of what must be included in that plan are in Attachment 1 and this SAR is adding 3 items to 1 of the 5 required sections of that plan. The SDT asserts there is not justification for a reorganization of every entity's low impact CIP programs and documentation by splitting the sections of the required cyber security plan for lows into multiple different standards.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
See comments from EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Michael Moltane - International Transmission Company Holdings Corporation - 1	
Answer	Yes
Document Name	
Comment	
Support EEI	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment, please see response to EEI.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to NPCC.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
WEC Energy Group supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Leshel Hutchings - AEP - 3	

Answer	Yes
Document Name	
Comment	

AEP has reviewed the redlines and concur with EEI's comments below understands that the revisions make conforming changes in alignment with Project 2016-02 and is supportive of the alignment. EEI suggests the following clarification, which we feel is non-substantive and in alignment with the intention of the DT, in Attachment 1:

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). **Responsible Entities with Shared Cyber Infrastructure (SCI) that supports a low impact BCS can utilize policies, procedures, and processes for their SCI supporting high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s).** Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

The defined term SCI applies when it hosts or provides storage resources required for system functionality for one or more Virtual Cyber Assets (VCAs) and one or more VCAs that are not included in, or associated with, BCS of the same impact categorization. Where a higher level of controls is applied to the SCI supporting low impact BCS, Entities should be able to use them to satisfy the requirements applicable to SCI in CIP-003-12, Attachment 1.

Likes 0	
Dislikes 0	
Response	

Thank you for your comment, please see response to EEI.

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	Yes
Document Name	
Comment	

Dominion Energy would like clarification on the SCI and the phrase from the technical rationale document for Project 2021-02, “However, network switches and other hardware that does enforce an ESP” specifically clarification on “other hardware”. Does this term include the firewall that is creating the ESP?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Unfortunately, this is a 2016-02 question regarding CIP-005 and therefore not within the scope of 2023-04’s scope to respond.	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	Yes
Document Name	
Comment	
It’s very confusing to review two separate versions of the same standard at the same time. Preferably one version should be reviewed at a time. Also having so many different projects working on one standard at the same time creates confusion. We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language. CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. TFIST recommends merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot. Additionally, we have concerns with the use of the SCI term and the possibility the EACMS, PACS at High or Medium Facilities may also have to comply with CIP-003-12 requirements which may be different than High and Medium requirements. We observed that SCI devices at High or Medium locations may be subject to documenting all inbound communication at the location which could be a	

substantial burden at a High and Medium location which would include corporate and non-BCS communications. It is proposed that SCI devices be high water marked to High/Medium or Low requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to similar comment under NPCC RSC.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI has reviewed the redline of CIP-003-9 to CIP-003-12 and understands that the revisions make conforming changes in alignment with Project 2016-02 and is supportive of the alignment. EEI suggests the following clarification, which we feel is non-substantive and in alignment with the intention of the DT, in Attachment 1: Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). **Responsible Entities with Shared Cyber Infrastructure (SCI) that supports a low impact BCS can utilize policies, procedures, and processes for their SCI supporting high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s).** Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets. The defined term SCI applies when it hosts or provides storage resources required for system functionality for one or more Virtual Cyber Assets (VCAs) and one or more VCAs that are not included in, or associated with, BCS of the same impact categorization. Where a higher level of controls is applied to the SCI supporting low impact BCS, Entities should be able to use them to satisfy the requirements applicable to SCI in CIP-003-12, Attachment 1.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments. The SDT agrees with the comments concerning SCI and the intent for such SCI that is already meeting high or medium impact requirements for the SCI itself should suffice for also meeting the CIP-003 low impact cyber security plan requirements. Therefore the SDT has modified CIP-003, Attachment 1 to that effect by specifically adding SCI to the paragraph in the header of Attachment 1.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Southern Indiana Gas and Electric d/b/a CenterPoint Energy Indiana South (SIGE) has concerns that having multiple versions of the standard simultaneously working on modifications causing confusion. Without having approved versions prior to making proposed revisions seems a bit premature.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to similar comment under NPCC RSC.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute for Question #6.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI. Black Hills Corporation has reviewed the redline of CIP-003-9 to CIP-003-12 and understands that the revisions make conforming changes in alignment with Project 2016-02 and is supportive of the alignment. EEI suggests the following clarification, which we feel is non-substantive and in alignment with the intention of the DT, in Attachment 1: Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). **Responsible Entities with Shared Cyber Infrastructure (SCI) that supports a low impact BCS can utilize policies, procedures, and processes for their SCI supporting high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s).** Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets. The defined term SCI applies when it hosts or provides storage resources required for system functionality for one or more Virtual Cyber Assets (VCAs) and one or more VCAs that are not included in, or associated with, BCS of the same impact categorization. Where a higher level of controls is applied to the SCI supporting low impact BCS, Entities should be able to use them to satisfy the requirements applicable to SCI in CIP-003-12, Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI.	
Daniel Gacek - Exelon - 1	

Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligned with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI.	
Michael Johnson - Michael Johnson On Behalf of: Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; Tyler Brun, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	

Comment
Comments and ballots on CIP-003-11 and 12 are confusing> To avoid complications, the others should be abandoned and only one should be released.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. Please see response to similar comment under NPCC RSC.

Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	

Comment
NEE supports EEI's comments: "EEI has reviewed the redline of CIP-003-9 to CIP-003-12 and understands that the revisions make conforming changes in alignment with Project 2016-02 and is supportive of the alignment. EEI suggests the following clarification, which we feel is non-substantive and in alignment with the intention of the DT, in Attachment 1: Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). **Responsible Entities with Shared Cyber Infrastructure (SCI) that supports a low impact BCS can utilize policies, procedures, and processes for their SCI supporting high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s).** Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets. The defined term SCI applies when it hosts or provides storage resources required for system functionality for one or more Virtual Cyber Assets (VCAs) and one or more VCAs that are not included in, or associated with, BCS of the same impact categorization. Where a higher

level of controls is applied to the SCI supporting low impact BCS, Entities should be able to use them to satisfy the requirements applicable to SCI in CIP-003-12, Attachment 1.“	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI.	
Michelle Pagano - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	Yes
Document Name	
Comment	
Supporting EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1 - RF	
Answer	Yes
Document Name	
Comment	

Combining multiple versions of a Reliability Standard Under Development into one (1) ballot is proving to be overtly onerous. It would be more beneficial if CIP-003-11 and CIP-003-12 language were combined into one (1) version of the Standard to be evaluated and balloted upon.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to similar comment under NPCC RSC.	
Matt Carden - Southern Company - Southern Company Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Southern Company is in agreement with the EEI comments:

EEI has reviewed the redline of CIP-003-9 to CIP-003-12 and understands that the revisions make conforming changes in alignment with Project 2016-02 and is supportive of the alignment. EEI suggests the following clarification, which we feel is non-substantive and in alignment with the intention of the DT, in Attachment 1:

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). **Responsible Entities with Shared Cyber Infrastructure (SCI) that supports a low impact BCS can utilize policies, procedures, and processes for their SCI supporting high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s).** Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

The defined term SCI applies when it hosts or provides storage resources required for system functionality for one or more Virtual Cyber Assets (VCAs) and one or more VCAs that are not included in, or associated with, BCS of the same impact categorization. Where a higher level of controls is applied to the SCI supporting low impact BCS, Entities should be able to use them to satisfy the requirements applicable to SCI in CIP-003-12, Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see response to EEI.	
Robert Kerrigan - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	
Comment	
Comments: CIP-003-12 seems better developed than CIP-003-11, in that it includes more concepts. The main comment about CIP-003-12 is that it includes two terms, “VCA” and “SCI”, that are new per virtualization project – will the terms be added into the standard itself or will the DT ensure they be added to the NERC glossary of terms?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. NERC has identified the problem of glossary terms only being included in the Glossary of Terms after FERC approval and will be adding a new section titled “Pending Regulatory Approval” where terms can be included prior to FERC approval. The implementation plan for this project will be modified to make it dependent on the final approval of that version of CIP-003.	
Fausto Serratos - Los Angeles Department of Water and Power - 3	
Answer	Yes

Document Name	
Comment	
CIP-003-12 seems better developed than CIP-003-11, in that it includes more concepts. The main comment about CIP-003-12 is that it includes two terms, "VCA" and "SCI", that are new per virtualization project – will the terms be added into the standard itself or will the DT ensure they be added to the NERC glossary of terms?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Those glossary terms were created by Project 2016-02 and are Board approved and will be added to the NERC glossary. The implementation plan for this project will be modified to make it dependent on the final approval of that version of CIP-003 and its subsequent modifications to the NERC glossary.	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
It's very confusing to review two separate versions of the same standard at the same time. Preferably one version should be reviewed at a time. Also having so many different projects working on one standard at the same time creates confusion.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to similar comment under NPCC RSC.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	

Answer	Yes
Document Name	
Comment	
See FirstEnergy's response to Q1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response in Q1.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the non-substantive revisions proposed by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your response.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	

It's very confusing to review two separate versions of the same standard at the same time. Preferably one version should be reviewed at a time. Also having so many different projects working on one standard at the same time creates confusion.

We are confused with the foundation starting with CIP-003-9 which was modified based upon project 2016-02 virtualization creating CIP-003-10 which has not been approved by FERC. CIP-003-11 changes do not appear to align or clearly track the changes in the last approved CIP-003-9 language. CIP-003-12 attempts to combine CIP-003-10 and the proposed CIP-003-11 but does not seem to capture all changes. TFIST recommends merging the proposed language in CIP-003-11 and CIP-003-12, marge the implementation plans, and repost after FERC approves CIP-003-10 in a new ballot.

Additionally, we have concerns with the use of the SCI term and the possibility the EACMS, PACS at High or Medium Facilities may also have to comply with CIP-003-12 requirements which may be different than High and Medium requirements. We observed that SCI devices at High or Medium locations may be subject to documenting all inbound communication at the location which could be a substantial burden at a High and Medium location which would include corporate and non-BCS communications. It is proposed that SCI devices be high water marked to High/Medium or Low requirements.

Likes 0	
Dislikes 0	

Response

Thank you for the comments. The SDT agrees concerning the multiple simultaneous versions issue. It was driven by the potential for very close proximity in time filing of this and 2016-02 versions of CIP-003 and uncertainty as to future order of regulatory approvals and being prepared for any eventuality. However, the SDT now plans for this version of CIP-003 to be filed at a later date after a subsequent posting for approval of the entire package including implementation plan and is thus consolidating into a single version and implementation plan for that next posting. That version will be labelled as CIP-003-11 and it will consist of this DT's changes on top of the Board approved CIP-003-10 along with a simplified implementation plan.

The SDT agrees with the comments concerning SCI. We note that since SCI supports systems of differing impact levels, whatever the highest impact category is of the supported systems will bring the SCI in under the "SCI supporting an Applicable System in the Part" applicability throughout the CIP standards, thus effectively high-watermarking the SCI. We agree the intent for such SCI that is already meeting high or medium impact requirements for the SCI itself should suffice for also meeting the CIP-003 low impact cyber security plan requirements. Therefore the SDT has modified CIP-003, Attachment 1 to that effect by specifically adding SCI to the paragraph in the header of Attachment 1.

Summary Response to Question 7:

The drafting team is putting forward only one standard and Implementation plan in the next comment and ballot period, which will be CIP-003-11 and includes this team changes on top of the virtualization changes made in CIP-003-10. This proposed CIP-003-11 Implementation plan would allow entities to have, at a minimum, the 24 months that was established by Project 2016-02 for the CIP-003-10 revisions. Likewise, entities would be allowed, at least, the 36 months to comply with the CIP-003-11 changes, as previously proposed by the Project 2023-04 drafting team.

The DT created a CIP-003-12 standard, CIP-003-12 implementation plan and a summary of changes document for this posting. Please review these files prior to answering this question. **7. Do you have any concerns in the CIP-003-12 implementation plan that should be addressed?**	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	

Tacoma Power has no concerns.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NEE supports EEI's comments: "EEI supports the CIP-003-12 implementation plan."	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
NA.	

Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
SMUD agrees with the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The NAGF agrees with the proposed CIP-003-12 implementation plan.	
Likes 0	

Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Fausto Serratos - Los Angeles Department of Water and Power - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Kerrigan - Los Angeles Department of Water and Power - 5	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carey Salisbury - Santee Cooper - 5, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Manitoba Hydro appreciates the standard drafting team's intent that the timeline set forth for CIP-003-12 be the later of 36-months from CIP-003-11 approval or 24-months from CIP-003-12 approval, giving entities at least 36-months of time to implement the changes. However, there is the possibility that CIP-003-11 does not receive governmental approval, and the version is "skipped" going straight to CIP-003-12. In this scenario, only 24-months of implementation would be afforded. This would not give entities enough time, especially if the standard changes require additional staff, hardware or architecture changes. Manitoba Hydro suggests that the implementation plan effective date for CIP-003-12 be revised to match CIP-003-11 and state that the standard become effective thirty-six (36) months after the effective date of the applicable governmental authority's order approving Reliability Standard CIP-003-12.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	

Duke Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
See FirstEnergy's response to Q3.	
Likes 0	
Dislikes 0	
Response	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	

When looking at implementation of plans of CIP-003-10, CIP-003-11, and CIP-003-12 it becomes confusing to decipher what is the actual effective date of CIP-003-12. There are too many dependencies involved.	
Likes 0	
Dislikes 0	
Response	
Matt Carden - Southern Company - Southern Company Services, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Southern Company is in agreement with the EEI comments: EEI is concerned about the proposed effective date for CIP-003-12. CIP-003-12 is the alignment of the Project 2023-04 changes with conforming changes from Project 2016-02 Virtualization, which is pending FERC approval. Given its pending approval, it is difficult to understand if the 24-month period would provide a shorter implementation timeframe than the 36-month period proposed for CIP-003-11. EEI supports a 36-month implementation period for the draft revisions and asks for that timeframe regardless of the version of CIP-003 approved.	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1 - RF	
Answer	Yes

Document Name	
Comment	
With multiple versions of implementation plans as they pertain to the different versions of a Reliability Standard Under Development, it is challenging to discern the applicable timelines and the organizational impacts of the implementation	
Likes 0	
Dislikes 0	
Response	
Michelle Pagano - Con Ed - Consolidated Edison Co. of New York - 5	
Answer	Yes
Document Name	
Comment	
Supporting EEI comments	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; Tyler Brun, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	

This should state 24 months after the implementation of CIP -003-11 not CIP 003-9. The way it is currently written, implementation would be required earlier than CIP-003-11.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligned with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	

Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI's comments: Black Hills Corporation is concerned about the proposed effective date for CIP-003-12. CIP-003-12 is the alignment of the Project 2023-04 changes with conforming changes from Project 2016-02 Virtualization, which is pending FERC approval. Given its pending approval, it is difficult to understand if the 24-month period would provide a shorter implementation timeframe than the 36-month period proposed for CIP-003-11. EEI supports a 36-month implementation period for the draft revisions and asks for that timeframe regardless of the version of CIP-003 approved.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
The NSRF appreciates the standard drafting team's intent that the timeline set forth for CIP-003-12 be the later of 36-months from CIP-003-11 approval or 24-months from CIP-003-12 approval, giving entities at least 36-months of time to implement the changes. However,	

there is the possibility that CIP-003-11 does not receive governmental approval, and the version is "skipped" going straight to CIP-003-12. In this scenario, only 24-months of implementation would be afforded. This would not give entities enough time, especially if the standard changes require additional staff, hardware or architecture changes. The NSRF suggests that the implementation plan effective date for CIP-003-12 be revised to match CIP-003-11 and state that the standard become effective thirty-six (36) months after the effective date of the applicable governmental authority's order approving Reliability Standard CIP-003-12.	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute and MRO NSRF for Question #7.	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	

Southern Indiana Gas and Electric d/b/a CenterPoint Energy Indiana South (SIGE) has the same concerns as addressed in question 6.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI is concerned about the proposed effective date for CIP-003-12. CIP-003-12 is the alignment of the Project 2023-04 changes with conforming changes from Project 2016-02 Virtualization, which is pending FERC approval. Given its pending approval, it is difficult to understand if the 24-month period would provide a shorter implementation timeframe than the 36-month period proposed for CIP-003-11. EEI supports a 36-month implementation period for the draft revisions and asks for that timeframe regardless of the version of CIP-003 approved.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	

Comment	
NST has the following two concerns about the CIP-003-12 implementation plan: (1) We note the section, "Prerequisite Standards" lists only CIP-003-11. We believe it should also be necessary for CIP-003-10 to be approved before CIP-003-12 can become effective. (2) We note the section, "Effective Date" identifies two possible scenarios (36 months after FERC approval of CIP-003-11 or 24 months after FERC approval of CIP-003-12) that seem to be based on an implicit assumption that by such time FERC approval is given to either Version 11 or Version 12, CIP-003-10 will have been previously approved. Although the NERC BoT has approved the "-10" version, it has not yet been approved by FERC, and NST believes this fact should be reflected in the current version of the "-12" implementation plan.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	Yes
Document Name	
Comment	
When looking at implementation of plans of CIP-003-10, CIP-003-11, and CIP-003-12 it becomes confusing to decipher what is the actual effective date of CIP-003-12. There are too many dependencies involved. CIP-003-11 and CIP-003-12 implementation plan should be combined and repost after FERC approves CIP-003-10 in a new ballot. TFIST recommends only having one implementation timeframe and TFIST prefers 36-month timeframe.	
Likes 0	
Dislikes 0	

Response	
Leshel Hutchings - AEP - 3	
Answer	Yes
Document Name	
Comment	
AEP has the same concerns as EEI--concerned about the proposed effective date for CIP-003-12. CIP-003-12 is the alignment of the Project 2023-04 changes with conforming changes from Project 2016-02 Virtualization, which is pending FERC approval. Given its pending approval, it is difficult to understand if the 24-month period would provide a shorter implementation timeframe than the 36-month period proposed for CIP-003-11. EEI supports a 36-month implementation period for the draft revisions and asks for that timeframe regardless of the version of CIP-003 approved.	
Likes 0	
Dislikes 0	

Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
WEC Energy Group supports the comments of EEI.	
Likes 0	
Dislikes 0	

Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Michael Moltane - International Transmission Company Holdings Corporation - 1	
Answer	Yes
Document Name	
Comment	
Support EEI	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	

Answer	Yes
Document Name	
Comment	
See comments from EEI	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	Yes
Document Name	
Comment	
• Expecting responsible entities to understand the unintended consequences of multiple changes to the same standard without any implementation time or settling time is unreasonable.	
Likes 0	
Dislikes 0	
Response	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE requests the SDT consider adding verbiage to the Initial Performance of Periodic Requirements section to include initial performance expectations for newly registered entities and for entities for which CIP-003 did not previously apply.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	

Document Name	
Comment	
When looking at implementation of plans of CIP-003-10, CIP-003-11, and CIP-003-12 it becomes confusing to decipher what is the actual effective date of CIP-003-12. There are too many dependencies involved. CIP-003-11 and CIP-003-12 implementation plan should be combined and repost after FERC approves CIP-003-10 in a new ballot. TFIST recommends only having one implementation timeframe and TFIST prefers 36-month timeframe.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Chantal Mazza On Behalf of: Junji Yamaguchi, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza	
Answer	
Document Name	
Comment	
This comment applies to all questions :It's very confusing to review two separate versions of the same standard at the same time. Preferably one version should be reviewed at a time. Also having so many different projects working on one standard at the same time creates confusion.	
Likes 0	
Dislikes 0	
Response	

End of Report

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reminder
Standards Announcement
Project 2023-04 Modifications to CIP-003

Additional Ballots and Non-binding Poll Open through July 11, 2024

Now Available

Additional ballots for **CIP-003-11 – Cyber Security – Security Management Controls** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels are open through **8 p.m. Eastern, Thursday, July 11, 2024**.

The third draft of CIP-003 is being posted for a 30-day formal comment and ballot period per the Standard Processes Manual Section 4.12.

Based on recent board adopted standards for CIP-003-9, the posted versions for the 2023-04 Modifications to CIP-003 was updated to reflect CIP-003-11. The Standards Balloting and Commenting System (SBS) does not allow edits once a ballot pool has been formed. Even though the standard versioning within the SBS states CIP-003-A, the version numbers within this posting are correct and entities will be voting on CIP-003-11 and CIP-003-12 in the same ballot.

The standard drafting team's considerations of the responses received from the last comment period are reflected in this draft of the standard.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Balloting

Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here.

Note: Votes cast in previous ballots, will not carry over to additional ballots. It is the responsibility of the registered voter in the ballot pools to place votes again. To ensure a quorum is reached, if you do not want to vote affirmative or negative, cast an abstention.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Manager, Standards Development, Alison Oswald (via email) or at 404-275-9410. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003 observer list” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-04 Modifications to CIP-003

Formal Comment Period Open through July 11, 2024

Now Available

A **30-day** formal comment period for **CIP-003-11 – Cyber Security – Security Management Controls**, is open through **8 p.m. Eastern, Thursday, July 11, 2024**.

The third draft of CIP-003 is being posted for a 30-day formal comment and ballot period per the Standard Processes Manual Section 4.12.

Based on recent board adopted standards for CIP-003-9, the posted versions for the 2023-04 Modifications to CIP-003 was updated to reflect CIP-003-11. The Standards Balloting and Commenting System (SBS) does not allow edits once a ballot pool has been formed. Even though the standard versioning within the SBS states CIP-003-A, the version numbers within this posting are correct and entities will be voting on CIP-003-11 and CIP-003-12 in the same ballot.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in this draft of the standard.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*

- *Please be mindful of ballot and comment period closing dates. We ask to* ***allow at least 48 hours*** *for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts* ***prior to the last day*** *of a comment/ballot period.*

Next Steps

An additional ballot for the standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **July 2-11, 2024**.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Manager, Standards Development, Alison Oswald (via email) or at 404-275-9410. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003 observer list” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/333)
Ballot Name: 2023-04 Modifications to CIP-003 CIP-003-A AB 3 ST
Voting Start Date: 7/2/2024 12:01:00 AM
Voting End Date: 7/11/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 231
Total Ballot Pool: 292
Quorum: 79.11
Quorum Established Date: 7/11/2024 6:26:34 PM
Weighted Segment Value: 80.58

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	83	1	49	0.817	11	0.183	0	4	19
Segment: 2	6	0	0	0	0	0	0	5	1
Segment: 3	62	1	43	0.811	10	0.189	0	2	7
Segment: 4	16	1	9	0.818	2	0.182	0	2	3
Segment: 5	77	1	43	0.796	11	0.204	0	2	21
Segment: 6	40	1	20	0.69	9	0.31	0	3	8
Segment: 7	1	0	0	0	0	0	0	0	1
Segment: 8	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	5	0.5	0	0	0	1	1
Totals:	292	5.5	169	4.432	43	1.068	0	19	61

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Corn Belt Power Cooperative	Larry brusseau		None	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Negative	Comments Submitted
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	JEA	Joseph McClung		None	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	LS Power Transmission, LLC	Jennifer Richardson		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	None	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Daniel Valle		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		None	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Pedernales Electric Cooperative, Inc.	Bradley Collard		None	N/A
1	Platte River Power Authority	Marissa Archie		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Laura Somak	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Olivia Olson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southwestern Power Administration	Angela Wheat		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Unisource - Tucson Electric Power Co.	Jessica Cordero		None	N/A
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		Abstain	N/A
3	AEP	Leshel Hutchings		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	BC Hydro and Power Authority	Ming Jiang		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	None	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Negative	Comments Submitted
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	Manitoba Hydro	Mike Smith		Affirmative	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	Richard Machado		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		None	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Ryan Walter		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Austin Energy	Tony Hua		None	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Abstain	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Katrina Lyons		Affirmative	N/A
4	Illinois Municipal Electric Agency	Mary Ann Todd		Abstain	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Affirmative	N/A
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	None	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	AES - AES Corporation	Ruchi Shah		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	American Municipal Power	Amy Ritts		None	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Amanda Wangler		None	N/A
5	BC Hydro and Power Authority	Quincy Wang		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		Affirmative	N/A
5	Bonneville Power Administration	Juergen Bermejo		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar	Jamie Monette	Abstain	N/A
5	Cowlitz County PUD	Deanna Carlson		Negative	Third-Party Comments
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Decatur Energy Center LLC	Megan Melham		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Negative	Comments Submitted
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	None	N/A
5	Great River Energy	Jacalynn Bentz		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi	Chantal Mazza	Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	JEA	John Babik		None	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Robert Kerrigan		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		None	N/A
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	Muscatine Power and Water	Chance Back		Affirmative	N/A
5	National Grid USA	Robin Berry		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		None	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NextEra Energy	Richard Vendetti		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Reid Cashion	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		Affirmative	N/A
5	Pacific Gas and Electric Company	Tyler Brun	Michael Johnson	Negative	Comments Submitted
5	Pattern Operators LP	George E Brown		Affirmative	N/A
5	Pine Gate Renewables	Michiko Sell		None	N/A
5	Platte River Power Authority	Jon Osell		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Carey Salisbury		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	TransAlta Corporation	Ashley Scheelar	Adam Burlock	None	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Michelle Hribar		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Imane Mrini		None	N/A
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco	Jamie Monette	Abstain	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Brandin Stoesz		Affirmative	N/A
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer	Dane Rogers	Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Powerex Corporation	Raj Hundal		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		None	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 292 of 292 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/333)
Ballot Name: 2023-04 Modifications to CIP-003 Implementation Plan AB 3 OT
Voting Start Date: 7/2/2024 12:01:00 AM
Voting End Date: 7/11/2024 8:00:00 PM
Ballot Type: OT
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 231
Total Ballot Pool: 293
Quorum: 78.84
Quorum Established Date: 7/11/2024 6:29:34 PM
Weighted Segment Value: 64.01

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	84	1	36	0.61	23	0.39	0	5	20
Segment: 2	6	0	0	0	0	0	0	5	1
Segment: 3	63	1	34	0.63	20	0.37	0	2	7
Segment: 4	16	1	7	0.636	4	0.364	0	1	4
Segment: 5	77	1	32	0.593	22	0.407	0	2	21
Segment: 6	40	1	16	0.552	13	0.448	0	3	8
Segment: 7	1	0	0	0	0	0	0	0	1
Segment: 8	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.5	5	0.5	0	0	0	1	0
Totals:	293	5.5	130	3.52	82	1.98	0	19	62

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Micah Runner		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Abstain	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Corn Belt Power Cooperative	Larry brusseau		None	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Negative	Comments Submitted
1	Duke Energy	Katherine Street		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Negative	Comments Submitted
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	JEA	Joseph McClung		None	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Third-Party Comments
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	LS Power Transmission, LLC	Jennifer Richardson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Negative	Comments Submitted
1	MEAG Power	David Weekley	Rebika Yitna	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	None	N/A
1	Muscatine Power and Water	Andrew Kurriger		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Daniel Valle		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		None	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Third-Party Comments
1	Omaha Public Power District	Doug Peterchuck		Negative	Third-Party Comments
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pedernales Electric Cooperative, Inc.	Bradley Collard		None	N/A
1	Platte River Power Authority	Marissa Archie		Negative	Third-Party Comments
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Laura Somak	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Olivia Olson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southwestern Power Administration	Angela Wheat		Negative	Third-Party Comments
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Unisource - Tucson Electric Power Co.	Jessica Cordero		None	N/A
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		Abstain	N/A
3	AEP	Leshel Hutchings		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	BC Hydro and Power Authority	Ming Jiang		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Negative	Comments Submitted
3	Black Hills Corporation	Josh Combs		Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	None	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Negative	Third-Party Comments
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Negative	Comments Submitted
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Affirmative	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	Manitoba Hydro	Mike Smith		Negative	Comments Submitted
3	MEAG Power	Roger Brand	Rebika Yitna	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Negative	Third-Party Comments
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	Richard Machado		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	William Berry		None	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tri-State G and T Association, Inc.	Ryan Walter		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		None	N/A
4	Austin Energy	Tony Hua		None	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Katrina Lyons		Affirmative	N/A
4	Illinois Municipal Electric Agency	Mary Ann Todd		Abstain	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Affirmative	N/A
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	None	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	AEP	Thomas Foltz		Affirmative	N/A
5	AES - AES Corporation	Ruchi Shah		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	American Municipal Power	Amy Ritts		None	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Amanda Wangler		None	N/A
5	BC Hydro and Power Authority	Quincy Wang		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		Affirmative	N/A
5	Bonneville Power Administration	Juergen Bermejo		Affirmative	N/A
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar	Jamie Monette	Abstain	N/A
5	Cowlitz County PUD	Deanna Carlson		Negative	Third-Party Comments
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Decatur Energy Center LLC	Megan Melham		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Negative	Comments Submitted
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	None	N/A
5	Great River Energy	Jacalynn Bentz		Negative	Third-Party Comments
5	Hydro-Quebec (HQ)	Junji Yamaguchi	Chantal Mazza	Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	JEA	John Babik		None	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Brittany Millard		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Los Angeles Department of Water and Power	Robert Kerrigan		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		None	N/A
5	Manitoba Hydro	Kristy-Lee Young		Negative	Comments Submitted
5	Muscatine Power and Water	Chance Back		Negative	Third-Party Comments
5	National Grid USA	Robin Berry		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		None	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NextEra Energy	Richard Vendetti		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Reid Cashion	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Third-Party Comments
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		Negative	Third-Party Comments
5	Pacific Gas and Electric Company	Tyler Brun	Michael Johnson	Negative	Comments Submitted
5	Pattern Operators LP	George E Brown		Negative	Third-Party Comments
5	Pine Gate Renewables	Michiko Sell		None	N/A
5	Platte River Power Authority	Jon Osell		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Carey Salisbury		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	TransAlta Corporation	Ashley Scheelar	Adam Burlock	None	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Michelle Hribar		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Imane Mrini		None	N/A
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco	Jamie Monette	Abstain	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Brandin Stoesz		Negative	Comments Submitted
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer	Dane Rogers	Negative	Third-Party Comments
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Powerex Corporation	Raj Hundal		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Negative	Comments Submitted
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		None	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 293 of 293 entries

BALLOT RESULTS

Ballot Name: 2023-04 Modifications to CIP-003 CIP-003-A | Non-binding Poll AB 3 NB
Voting Start Date: 7/2/2024 12:01:00 AM
Voting End Date: 7/11/2024 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 214
Total Ballot Pool: 280
Quorum: 76.43
Quorum Established Date: 7/11/2024 6:40:48 PM
Weighted Segment Value: 82.22

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	41	0.82	9	0.18	10	20
Segment: 2	6	0	0	0	0	0	5	1
Segment: 3	59	1	39	0.848	7	0.152	5	8
Segment: 4	16	1	9	0.818	2	0.182	1	4
Segment: 5	74	1	38	0.826	8	0.174	5	23
Segment: 6	38	1	17	0.739	6	0.261	6	9
Segment: 7	1	0	0	0	0	0	0	1
Segment: 8	0	0	0	0	0	0	0	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	6	0.4	4	0.4	0	0	2	0
Totals:	280	5.4	148	4.451	32	0.949	34	66

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Corn Belt Power Cooperative	Larry brusseau		None	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Negative	Comments Submitted
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	JEA	Joseph McClung		None	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	LS Power Transmission, LLC	Jennifer Richardson		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	None	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Daniel Valle		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		None	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Abstain	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Pedernales Electric Cooperative, Inc.	Bradley Collard		None	N/A
1	Platte River Power Authority	Marissa Archie		Negative	Comments Submitted
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Laura Somak	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Olivia Olson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southwestern Power Administration	Angela Wheat		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	David Plumb		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Unisource - Tucson Electric Power Co.	Jessica Cordero		None	N/A
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
2	California ISO	Darcy O'Connell		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		Abstain	N/A
3	AEP	Leshel Hutchings		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	BC Hydro and Power Authority	Ming Jiang		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	None	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Affirmative	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	Richard Machado		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		None	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Ryan Walter		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		None	N/A
4	Austin Energy	Tony Hua		None	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Katrina Lyons		Affirmative	N/A
4	Illinois Municipal Electric Agency	Mary Ann Todd		Abstain	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Affirmative	N/A
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	None	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	AES - AES Corporation	Ruchi Shah		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Amanda Wangler		None	N/A
5	BC Hydro and Power Authority	Quincy Wang		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		Affirmative	N/A
5	Bonneville Power Administration	Juergen Bermejo		Affirmative	N/A
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar	Jamie Monette	Abstain	N/A
5	Cowlitz County PUD	Deanna Carlson		Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Decatur Energy Center LLC	Megan Melham		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Negative	Comments Submitted
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	None	N/A
5	Great River Energy	Jacalynn Bentz		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi	Chantal Mazza	Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	JEA	John Babik		None	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Brittany Millard		Abstain	N/A
5	Los Angeles Department of Water and Power	Robert Kerrigan		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		None	N/A
5	Muscatine Power and Water	Chance Back		Affirmative	N/A
5	National Grid USA	Robin Berry		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		None	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NextEra Energy	Richard Vendetti		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Reid Cashion	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pacific Gas and Electric Company	Tyler Brun	Michael Johnson	Negative	Comments Submitted
5	Pattern Operators LP	George E Brown		Affirmative	N/A
5	Pine Gate Renewables	Michiko Sell		None	N/A
5	Platte River Power Authority	Jon Osell		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Carey Salisbury		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	TransAlta Corporation	Ashley Scheelar	Adam Burlock	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tri-State G and T Association, Inc.	Sergio Banuelos		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Michelle Hribar		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Imane Mrini		None	N/A
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco	Jamie Monette	Abstain	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	New York Power Authority	Shelly Dineen		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer	Dane Rogers	Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Portland General Electric Co.	Stefanie Burke		Abstain	N/A
6	Powerex Corporation	Raj Hundal		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Abstain	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		None	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 280 of 280 entries

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard for a 30-day formal comment period with additional ballot. CIP-003-11 is built on Board Approved CIP-003-10 which was created by Project 2016-02's changes for virtualization.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023
45-day formal comment period with initial ballot	October 24 – December 7, 2023
45-day formal comment period with additional ballot	January 30 – March 14, 2024
30-day formal comment period with additional ballot	June 12 – July 11, 2024

Anticipated Actions	Date
30-day formal comment period with additional ballot	September 11 – October 10, 2024
10-day final ballot	November 2024
Board adoption	December 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-11

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-11:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-11.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high-level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR	impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	the previous approval. (Part 1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the	according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment	Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote	

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (Requirement R2)	access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of the change. (Requirement R3)			calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2023-04
- CIP-003-11 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
10	5/9/2024	Adopted by the NERC Board of Trustees.	Modifications made by Project 2016-02.

Version	Date	Action	Change Tracking
10	TBD	FERC approval pending in Docket No. RM24-8-000	
11	TBD	Modified by Project 2023-04	

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS including any supporting SCI to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need, as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or Virtual Cyber Asset (VCA), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, where electronic access is:

i. Between:
- a low impact BCS; or
- an SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:
- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems;

the Responsible Entity shall implement one or more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for

both inbound and outbound electronic access;

3.1.3 Authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted;

3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System(s) outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BCS or SCI that supports a low impact BCS;

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, the Responsible Entity shall implement one or more control(s) that authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security

Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. For Section 3.1.1, documentation showing the permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, such as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BCS or SCI that supports a low impact BCS and a Cyber System outside the asset containing low impact BCS.
   - Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways); or
   - Original equipment manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
    - Anti-malware technologies;
    - Intrusion detection system (IDS)/intrusion prevention system (IPS);
    - Monitor or alert for changes to communication baselines;
    - Logging and alerting configuration for security incident and event management (SIEM) systems or other event correlation systems;
    - Automated or manual log reviews;
    - Alerting; or
    - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted, such as:
    - Authentication mechanism(s) including but not limited to:
        - Utilization of public key infrastructure (PKI), lightweight directory access protocol (LDAP), remote authentication dial-in user service (RADIUS), and/or similar implemented solutions; or
        - Enforcement of multi-factor authentication (MFA).
    - Virtual private network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
    - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BCS; or
    - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System outside the asset containing low impact BCS or SCI that supports a low impact BCS and
    - The authentication system used to meet Section 3.1.3, or
    - The asset containing low impact BCS or SCI that supports a low impact BCS,

    such as protection mechanism(s) including, but not limited to:
    - Implementation of an encrypted protocol or service (hypertext transfer protocol secure (HTTPS), secure shell (SSH), etc.);
    - Implementation of an IPsec or secure sockets layer (SSL) VPN; or

- Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;
   - Security information management logging alerts;
   - Time-of-need session initiation;
   - Session recording;
   - System logs; or
   - Other operational, procedural, or technical controls.
6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Disabling vendor electronic access user or system accounts;
   - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, remote desktop, remote control, or other hardware or software used for providing vendor electronic access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or
   - Other operational, procedural, or technical controls.
7. For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard for a 30-day formal comment period with additional ballot. CIP-003-11 is built on Board Approved CIP-003-10 which was created by Project 2016-02's changes for virtualization.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023
45-day formal comment period with initial ballot	October 24 – December 7, 2023
45-day formal comment period with additional ballot	January 30 – March 14, 2024
30-day formal comment period with additional ballot	June 12 – July 11, 2024

Anticipated Actions	Date
30-day formal comment period with additional ballot	September 11 – October 10, 2024
10-day final ballot	November 2024
Board adoption	December 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-~~10~~11

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-~~10~~11:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See ~~"Project 2016-02 Modifications to CIP Standards~~ Implementation Plan~~."~~ for CIP-003-11.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

~~**1.2.6.** Vendor electronic remote access security controls; and~~

~~**1.2.7.**~~**1.2.6.** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS,

that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high-~~-~~level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-~~10~~11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-~~1~~011)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR	impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1. (~~R1~~Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of

R #	Violation Severity Levels (CIP-003-~~1~~011)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	the previous approval. (~~R1~~Part 1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-~~1~~011)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the	according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity ~~documented~~ failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Violation Severity Levels (CIP-003-~~1~~011)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment	Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote	

R #	Violation Severity Levels (CIP-003-~~1~~011)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (Requirement R2)	access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60

R #	Violation Severity Levels (CIP-003-~~10~~11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of the change. (Requirement R3)			calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project ~~2016-02~~2023-04
- CIP-003-~~10~~11 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and

Version	Date	Action	Change Tracking
			communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	

Version	Date	Action	Change Tracking
9	3/22/2023	Effective Date	April 1, 2026
10	~~TBD~~5/9/2024	~~Virtualization Modifications~~Adopted by the NERC Board of Trustees.	Modifications made by Project 2016-02.
10	TBD	FERC approval pending in Docket No. RM24-8-000	
11	TBD	Modified by Project 2023-04	

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS including any supporting SCI to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need, as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or Virtual Cyber Asset (VCA~~,~~), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact ~~BES Cyber System(s)~~BCS identified pursuant to CIP-002~~, the Responsible Entity shall implement~~ and for SCI that supports a low impact BCS, if any, where electronic access ~~controls to~~is:

~~**3.1** Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:~~

i. Between:
- ~~a~~ low impact BCS; or
- ~~An~~an SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:
- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems~~.~~;

~~Authenticate~~the Responsible Entity shall implement one or more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic access;

3.1.3 Authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted;

3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System(s) outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BCS or SCI that supports a low impact BCS;

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, the Responsible Entity shall implement one or more control(s) that authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security

Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

~~**Section 6.** Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:~~

~~**6.1** One or more method(s) for determining vendor electronic remote access;~~

~~**6.2** One or more method(s) for disabling vendor electronic remote access; and~~

~~**6.3** One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.~~

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. ~~Documentation~~ For Section 3.1.1, documentation showing ~~that at each asset or group of assets,~~ the ~~routable protocol communication as outlined in Section 3 is restricted by electronic access controls to permit~~permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, ~~except where an entity provides rationale that communications are used for time-sensitive communications of Protection Systems. Examples of~~ such ~~documentation may include, but are not limited to representative~~as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) ~~or lists~~between the low impact BCS or SCI that supports a low impact BCS and a Cyber System outside the asset containing low impact BCS.

- Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways~~)~~.); or
- ~~Documentation~~Original equipment manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Anti-malware technologies;
   - Intrusion detection system (IDS)/intrusion prevention system (IPS);
   - Monitor or alert for changes to communication baselines;
   - Logging and alerting configuration for security incident and event management (SIEM) systems or other event correlation systems;
   - Automated or manual log reviews;
   - Alerting; or
   - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted, such as:
   - Authentication mechanism(s) including but not limited to:
     - Utilization of public key infrastructure (PKI), lightweight directory access protocol (LDAP), remote authentication dial-in user service (RADIUS), and/or similar implemented solutions; or
     - Enforcement of multi-factor authentication (MFA).
   - Virtual private network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
   - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BCS; or
   - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System outside the asset containing low impact BCS or SCI that supports a low impact BCS and
   - The authentication system used to meet Section 3.1.3, or

- The asset containing low impact BCS or SCI that supports a low impact BCS, such as protection mechanism(s) including, but not limited to:
  - Implementation of an encrypted protocol or service (hypertext transfer protocol secure (HTTPS), secure shell (SSH), etc.);
  - Implementation of an IPsec or secure sockets layer (SSL) VPN; or
  - Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;
   - Security information management logging alerts;
   - Time-of-need session initiation;
   - Session recording;
   - System logs; or
   - Other operational, procedural, or technical controls.
6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Disabling vendor electronic access user or system accounts;
   - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, remote desktop, remote control, or other hardware or software used for providing vendor electronic access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or
   - Other operational, procedural, or technical controls.

~~1.~~7. For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back

modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to

mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

~~**Section 6.** Vendor Electronic Remote Access Security Controls: Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:~~

~~1. For Section 6.1, documentation showing:~~

- ~~steps to preauthorize access;~~
- ~~alerts generated by vendor log on;~~
- ~~session monitoring;~~
- ~~security information management logging alerts;~~
- ~~time-of-need session initiation;~~
- ~~session recording;~~
- ~~system logs; or~~
- ~~other operational, procedural, or technical controls.~~

~~2. For Section 6.2, documentation showing:~~

- ~~disabling vendor electronic remote access user or system accounts;~~
- ~~disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control,~~

~~or other hardware or software used for providing vendor electronic remote access;~~

- ~~disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;~~
- ~~Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);~~
- ~~administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or~~
- ~~other operational, procedural, or technical controls.~~

3. ~~For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:~~
   - ~~Anti-malware technologies;~~
   - ~~Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);~~
   - ~~Automated or manual log reviews;~~
   - ~~alerting; or~~
   - ~~other operational, procedural, or technical controls.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-04 Modifications to CIP-003
Reliability Standard CIP-003-11

Applicable Standard(s)

- CIP-003-11 – Cyber Security – Security Management Controls

Requested Retirement(s)

- CIP-003-10 – Cyber Security – Security Management Controls[1]

Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- Cyber System
- Shared Cyber Infrastructure
- Virtual Cyber Asset

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

New/Modified/Retired Terms in the NERC Glossary of Terms

- None

[1] If CIP-003-10 is not currently in effect, then the currently effective version of Reliability Standard CIP-003 shall be retired immediately prior to the effective date of CIP-003-11 in the jurisdiction in which the revised standard is becoming effective.

Background

Project 2023-04 addresses modifications to CIP-003-10 in response to recommendations from the Low Impact Criteria Review Team (LICRT), which was formed by the NERC Board of Trustees to consider the potential threat and risk posed by a coordinated cyber-attack on low impact Bulk Electric System (BES) Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommended actions to address those risks. The NERC Board of Trustees accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the standard authorization request (SAR) at its March 22, 2023 meeting. In response to the SAR, Project 2023-04 proposes merging Sections 3 and 6 of CIP-003, Attachments 1 and 2 to consolidate all electronic access requirements. These revisions are captured in Reliability Standard CIP-003-11.

This implementation plan provides additional time for entities to come into compliance with Requirement R2 for the expanded scope of communications that must be monitored to detect known or suspicious malicious communications, from vendor electric remote access in CIP-003-9, to all inbound and outbound electronic access in CIP-003-11 (Attachment 1 Section 3.1.2). In determining additional time was appropriate, the Project 2023-04 drafting team considered that CIP-003-9 will become effective April 1, 2026, and two versions of the CIP-003 standard will be pending regulatory approval (CIP-003-10, CIP-003-11). The drafting team also considered that entities may have already invested significant resources to implement system architecture to monitor vendor remote access in compliance with Reliability Standard CIP-003-9, and that implementing further changes across a large fleet of low impact BES Cyber Systems may require significant additional time and investments. This implementation plan ensures that entities will have at least three years from the effective date of Reliability Standard CIP-003-9 to implement the additional controls contemplated by CIP-003-11, regardless of the date proposed Reliability Standard CIP-003-11 is approved.

The CIP-003-11 changes were made to the NERC Board of Trustees approved version of CIP-003, CIP-003-10 (Virtualization Revisions), which has been filed with the applicable governmental authorities. The use of certain defined terms within CIP-003-11 requires that the definitions for Cyber Systems, Shared Cyber Infrastructure, and Virtual Cyber Asset be approved either concurrently with or before CIP-003-11.

General Considerations

This implementation plan applies only to the CIP-003-11 revisions to the Reliability Standard that have been made by the Project 2023-04 drafting team. The implementation plan does not modify the implementation plan(s) for any other version of CIP-003.

This implementation plan provides entities with thirty-six (36) months to become compliant with the revised Reliability Standard CIP-003-11. This implementation plan reflects the following considerations for entities to implement the new controls of Requirement R2, Attachment 1:

- Revise cyber security policy, plan, and procedures.
- Hire and train new staff to implement the new cyber security controls.
- Reconfigure system, network, or security architectures.
- Purchase, procure, and install new technologies.
- The effective date of CIP-003-9 is April 1, 2026.
- The requested effective date of CIP-003-10 is the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority.

Effective Date

Reliability Standard CIP-003-11

Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and Responsible Entities shall comply initially with those periodic requirements in CIP-003-11 as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.3 on or before the effective date of CIP-003-11. Responsible Entities shall initially comply with all other periodic requirements in CIP-003-11 within the periodic timeframes of their last performance under the version of the CIP-003 Reliability Standard then in effect.

Compliance Date for Requirement R2, Attachment 1 Section 3.1.2

Entities shall not be required to comply with Requirement R2 as it relates to the implementation of documented cyber security plan(s) addressing Attachment 1 Section 3.1.2[2] until the later of: (1) April 1, 2029; or (2) the effective date of Reliability Standard CIP-003-11.

Retirement Date

Reliability Standard CIP-003

Reliability Standard CIP-003-10, or the version of Reliability Standard CIP-003 then in effect, shall be retired immediately prior to the effective date of CIP-003-11 in the jurisdiction in which the revised standard is becoming effective.

[2] Attachment 1 Section 3.1.2: "Detect known or suspected malicious communications for both inbound and outbound electronic access."

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard
CIP-003-11 – Low Impact BES Cyber Security Criteria Revisions

Introduction
This document is the technical rationale and justification for Reliability Standard CIP-003-11 and includes the rationale for changes in the current proposed version, as well as previous versions of the standard.

It is intended to provide stakeholders and the ERO Enterprise with an understanding of the revisions, technology, and technical concepts of Reliability Standard CIP-003-11. This is not a Reliability Standard and should not be considered mandatory and enforceable.

Background
In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact Bulk Electric System (BES) Cyber Assets. Specifically, this includes the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts, representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber-attack on low impact BES Cyber Systems (LIBCS). In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommended actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the Standard Authorization Request (SAR) at its March 22, 2023 meeting.

The LICRT conclusions regarding LIBCS are as follows:

- Individually, LIBCS are truly low impact to BES reliability. This corresponds to the longstanding work of NERC and the stakeholders to design and operate the BES to withstand the loss of any of its individual assets. A medium or high impact BES Cyber System is more than an impact to a typical single BES Element/Facility. Therefore, the LICRT does not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems.
- LIBCS may introduce BES reliability risks of a higher impact where distributed LIBCS are used for a coordinated attack. The LICRT recommends enhancing the existing low impact category to further mitigate the coordinated attack risk.

The LICRT report recommendations are as follows:

- Requirement(s) for authentication of remote users before granting and subsequently gaining electronic access to networks containing LIBCS at assets containing those systems that have external routable connectivity.

- Requirement(s) for protection of user authentication information in transit for remote electronic access to LIBCS at assets containing those systems that have external routable connectivity.
- Requirement(s) for detection of malicious communications to/between assets containing LIBCS with external routable connectivity.

Rationale for Attachment 1, Section 3 and Section 6

The drafting team's (DT) review of the SAR and industry comment initiated a discussion about the placement of requirements within CIP-003-11. Attachment 1, Section 3 and Attachment 1, Section 6 were identified as ideal locations to integrate the requirements due to their focus on electronic access controls and vendor electronic remote access security controls. The DT investigated two options:

Option A: Modify Sections 3 and 6, integrating the requirements, but keeping the sections separate.
Option B: Merge Sections 3 and 6.

The DT agreed to Option B: Merge Sections 3 and 6. Merging Section 3 and Section 6 would present a single section for all electronic access with sub-sections providing additional requirements based on the type of access (vendor, dial-up, local, etc.). This allows entities to look in one place for all of the electronic access control requirements needed for their assets containing low impact systems, rather than having very similar, and in some cases, overlapping requirements in multiple places within the standard.

While merging Section 3 and 6, the DT made conforming changes to the language. The DT uses the phrase "implement controls" to replace "implement a process" or "implement one or more method(s)". The DT believes a "control" can include an operation, process, procedure, or technology as described in the examples of Attachment 2. Additionally, the word "remote" was removed from the phrase "electronic remote access" as the section now covers all electronic access as described in Section 3, Part 3.1, (i), (ii), and (iii) as those define more specifically the remote nature of the in-scope access.

To clarify scope of requirements for industry and regulators alike, the DT placed the requirements in Attachment 1 Section 3.1 into a logical "if, then" order to further clarify the three identifying low impact asset characteristics or conditions (romanettes i, ii, iii) when implementing controls.

Section 3.1

The objective of the modifications within Section 3.1 is to maintain the original language used in CIP-003-10, Section 3.1, Subsections (i) - (iii). There is one revision to 3.1(iii) replacing the previous language concerning "intelligent electronic devices" with reference to the existing glossary term "Protection Systems" which is a conforming change to the change made by Project 2016-02, CIP-003-10. Figure 1 provides a graphical representation of Section 3.1, Subsections (i)-(iii).

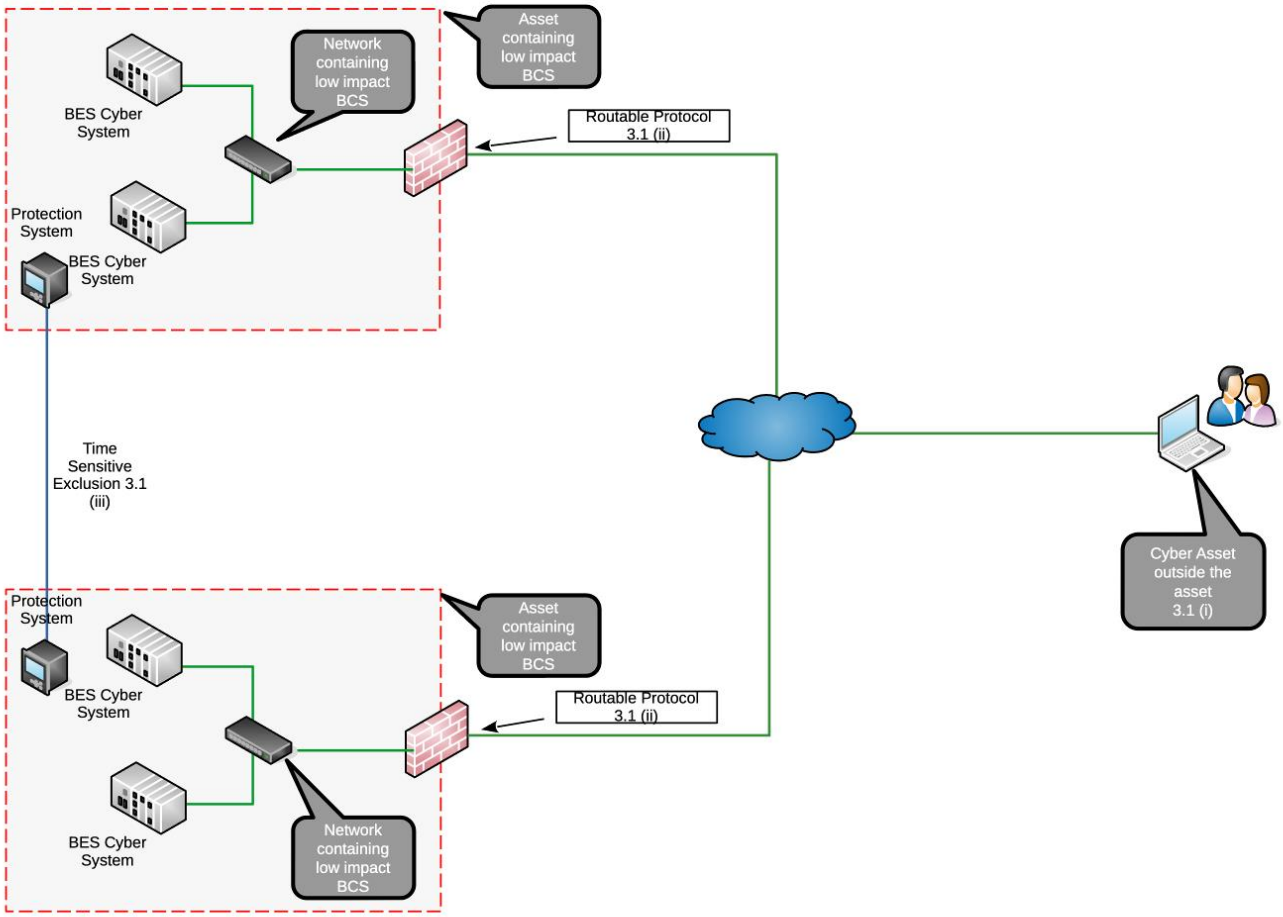


Figure 1

Section 3.1.1

The objective of Section 3.1.1 is to maintain the original language used in CIP-003-10, Section 3.1.

Section 3.1.2

This is an expanded cyber security control outlined in the SAR. The scope is expanded from CIP-003-10, Section 6.3 to include all communications rather than vendor specific communications. The objective of the modifications within Attachment 1 Section 3.1.2 is for entities to mitigate the risk posed by malicious communications to or from LIBCS. The detection of known or suspected malicious communications can be accomplished in several ways. For example, Figure 2 below depicts implementing the control (e.g., Intrusion Detection System (IDS)) in a centralized location (e.g., at a corporate hub site) rather than at every distributed "asset containing LIBCS" such as substations in this example "hub and spoke" model. The obligation in Section 3.1.2 requires that entities implement controls to detect known or suspected inbound and outbound malicious communications between a low impact BES Cyber System and a Cyber

Asset(s) outside the asset containing low impact BES Cyber System(s) thus allowing entity flexibility in where the control is implemented based on their architecture.

The DT considered entities that may use encryption to protect communications between hosts and the impact to the ability to detect known or suspected malicious communications. Because of the differences in entity programs, architectures, technologies and processes, the DT did not prescribe that encrypted communications must be decrypted for deep packet inspection when detecting known or suspected malicious communication. Requiring decryption/inspection/re-encryption may in some cases increase risk through introducing single points of failure or jeopardizing sensitive timing of communications. Entities may detect known or suspected malicious communications through other methods, such as detecting the appearance of abnormal new destination addresses or ports. The DT provided several other examples in Attachment 2. Entities may also choose to perform detection before or after the encryption tunnel occurs.

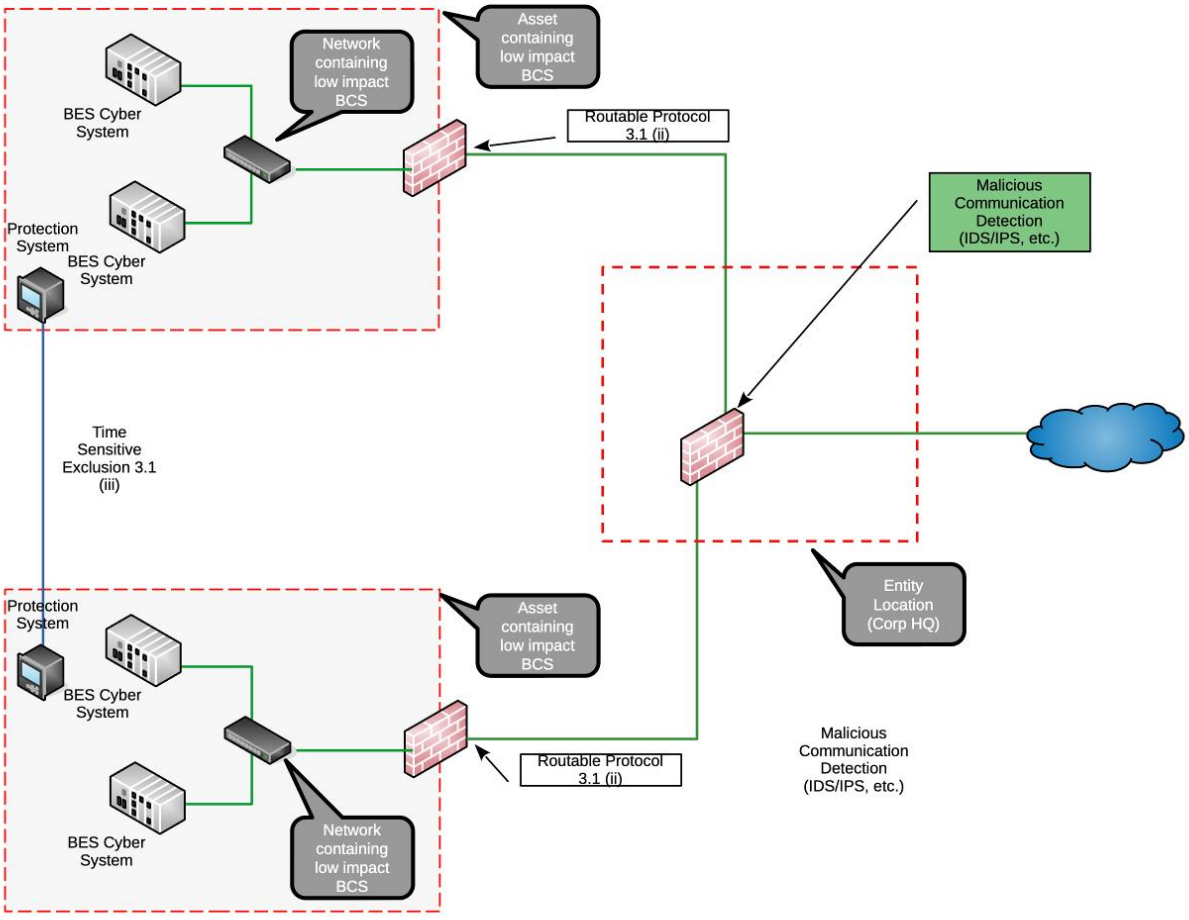


Figure 2

Section 3.1.3

This is a new cyber security control outlined in the SAR that requires entities to implement controls to authenticate users prior to permitting access to networks containing LIBCS. This control mitigates the risk of unauthenticated access to networks on which LIBCS reside. The intent is for each user to be authenticated (verifying a user) *before* they gain access to the "network containing low impact BES Cyber Systems"; thus, they have no ability to enumerate hosts on those networks, scan those networks for vulnerabilities, attempt logons to systems, or perform actions on those networks and systems before the entity has authenticated their user-initiated electronic access. It is important to note that Section 3.1.3 is not applicable to electronic access which sources (is connected) to the LIBCS network. For example, a laptop connected via an Ethernet cable to the LIBCS network would not be required to authenticate prior to accessing the LIBCS to which it is being connected. It is also important to note that the DT did not address specific account types (user or shared) used for authentication. While the intent is for entities to control each user prior to permitting electronic access, the SAR did not prescribe account types or passwords used by users to obtain (via authentication) electronic access. There are multiple methods to authenticate users for the responsible entity to choose.

Figure 3, below, depicts a situation where the authentication of the remote user is not occurring "prior to" but after the user already has access to the "network containing LIBCS" — as the authentication servers are on the same network with the LIBCS. The firewall in this scenario allows the user through to the network on which the LIBCS reside before the user is authenticated, and this does not meet the intent of the requirement.

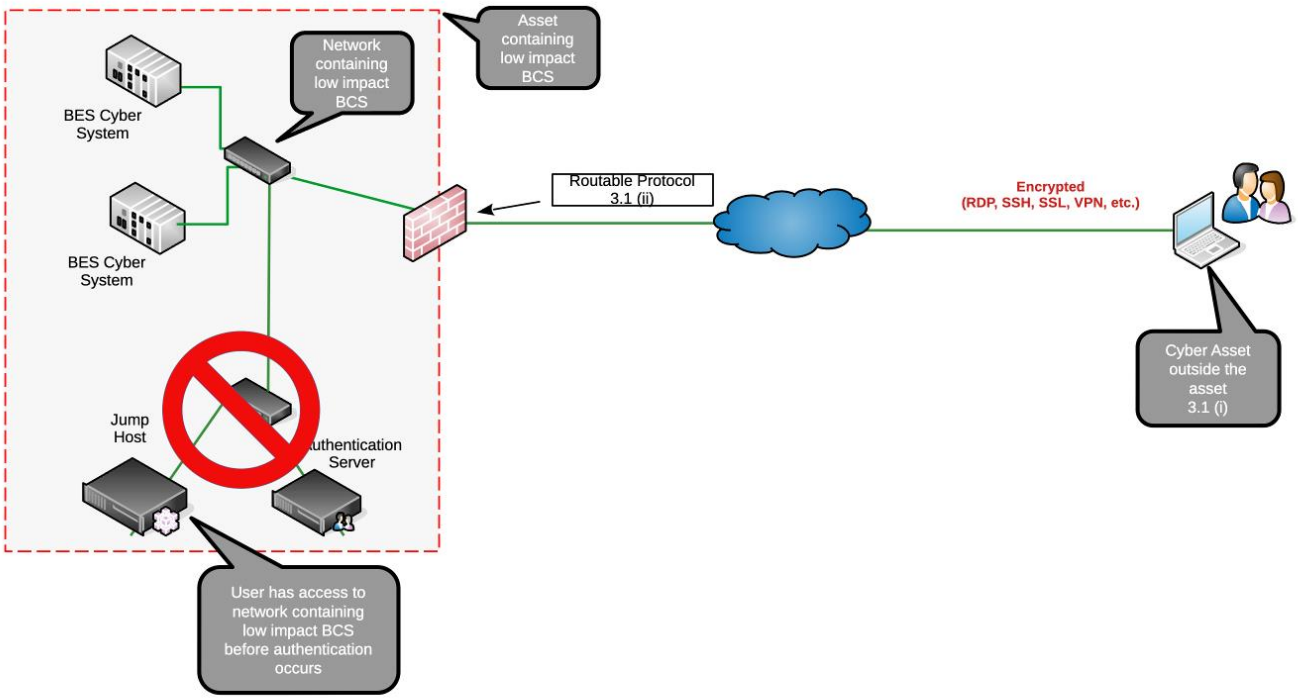


Figure 3

The intention of the phrase "each user prior to permitting access to a network(s)…" is meant to include the initial authentication and not all subsequent access to other downstream networks. If there is a collection of sub-networks or Cyber Assets within the network containing LIBCS, then multiple re-authentications at those levels would not be required by this specific requirement. Regardless of how many subsequent networks or BES Cyber Systems a user may access, as long as the entity's implemented control(s) have authenticated the user prior to their access to those subsequent networks, that meets the intent. This may include, but is not limited to, configurations where authentication is local device specific authentication or configurations consisting of centralized authentication using technologies such as an access, terminal, or proxy server ("Intermediate System") which processes authentication to the low impact asset networks through a centralized gateway.

The DT has not required the use of an "Intermediate System" as is prescribed in CIP-005 Requirement R2 for high and medium impact BES Cyber Systems. However, the DT's intent is that those entities who have established or implemented such infrastructure or technologies may use them for authenticating access

to the assets containing low impact BES Cyber Systems to satisfy these requirements. While prescribing such an architecture as in CIP-005 Requirement R2 would further clarify CIP-003's requirements, the DT has chosen not to prescribe such requirements due to the impact to a broad and diverse range of entities and their specific technologies and processes used to meet low impact BES Cyber Systems authentication requirements. For example, it would be excessive to require an entity with a single CIP-003 applicable renewable generation site to implement architectures and technologies (Intermediate Systems) to meet the CIP-005 Requirement R2 Interactive Remote Access requirements. Such an entity may only need a Secure Sockets Layer (SSL) Virtual Private Network (VPN) to an access control device (e.g., firewall) at the one site that authenticates the user prior to allowing access to the network containing low impact BES Cyber Systems on its inside interface. The entity may also choose to authenticate a local non-low impact BES Cyber Systems network first, then control access to the LIBCS from that access point. Conversely, an entity with many assets distributed over a large geographic area, with a variety of impact categorizations and supporting BES Cyber Systems, may want to use their existing CIP-005 Requirement R2 remote access solutions for all of their sites (centralized access controls). The DT's intent in the CIP-003 language is to allow flexibility for both cases.

The phrase, "through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted" is included in Section 3.1.3 to clarify scoping. As Section 3.1.3 is written at a different granularity of "network(s) containing", which is not mentioned in the romanettes, this phrasing simply clarifies that the intended scope remains those networks through which the specific access described in the Section 3.1 romanettes is subsequently permitted. The romanettes (i), (ii), and (iii) in Section 3.1 define the ultimate access that is in scope, which is from a remote client outside the asset containing the LIBCS and destined for a LIBCS within the asset.

Section 3.1.4

This is a new cyber security control outlined in the SAR. The objective of Attachment 1, Section 3.1.4 is for entities to protect the user authentication information (e.g., username, password, multi-factor authentication (MFA) information, session token, etc.) while in transit between the remote user's Cyber Asset and either the asset containing the low impact BES Cyber Systems or the entity's authentication system used to meet Section 3.1.3. This mitigates the risk of user authentication information being captured, especially as some BES equipment may still require protocols that transmit such information in clear text. The intent is not to specify authentication directly to a particular device but to allow entities that desire to use an existing compliant CIP-005 Requirement R2 Intermediate System, or similar architecture, access to networks containing LIBCS (Figure 4). For example, Figure 4 below depicts protection of the user authentication information to the asset containing a LIBCS.

Figure 5 depicts an alternative example of protecting the user authentication information to/from a central system (i.e. jump host) *before* accessing a network containing a LIBCS. This protection mitigates the unintended disclosure of authentication information for electronic access to low impact cyber systems.

Note that both Figure 4 and Figure 5 have a significant difference from Figure 3 above in that, although the authentication services are also within the asset containing the LIBCS, they are located on a separate network from those containing BES Cyber Systems. In this example, assuming the firewall is configured to only allow authenticated user sessions on the jump host through to the network containing the LIBCS, this would meet the intent of the Section 3.1.3.

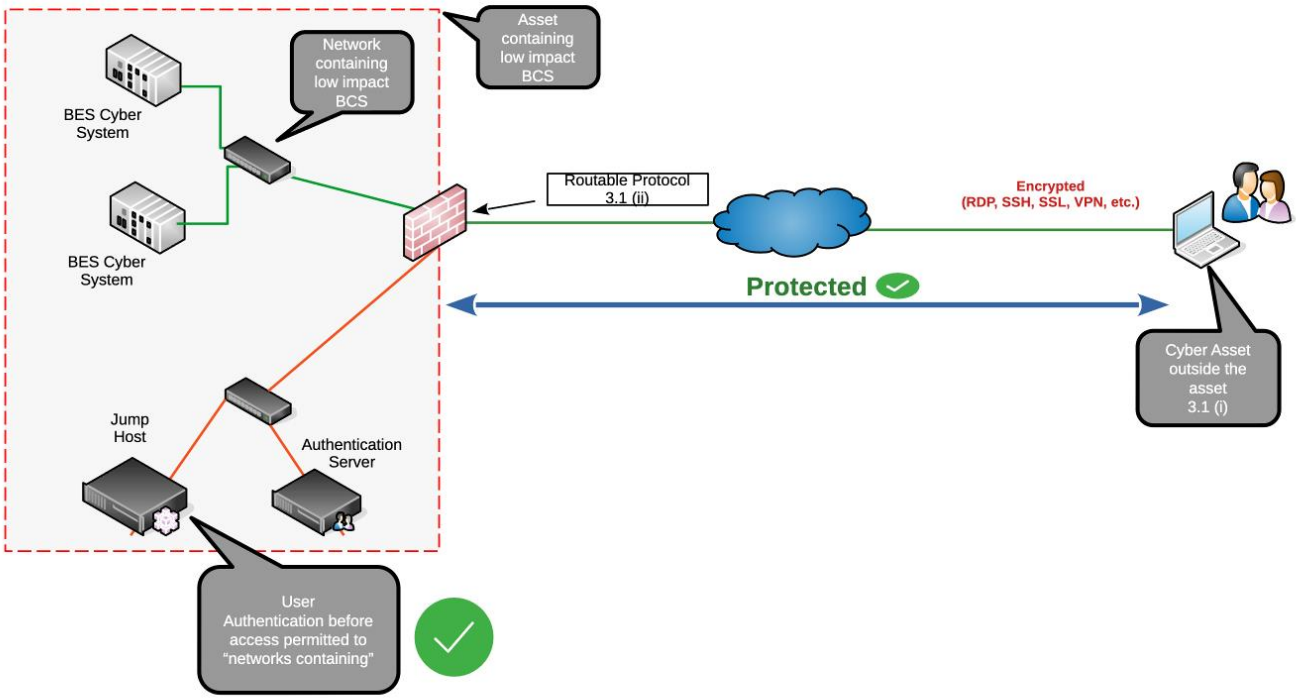


Figure 4

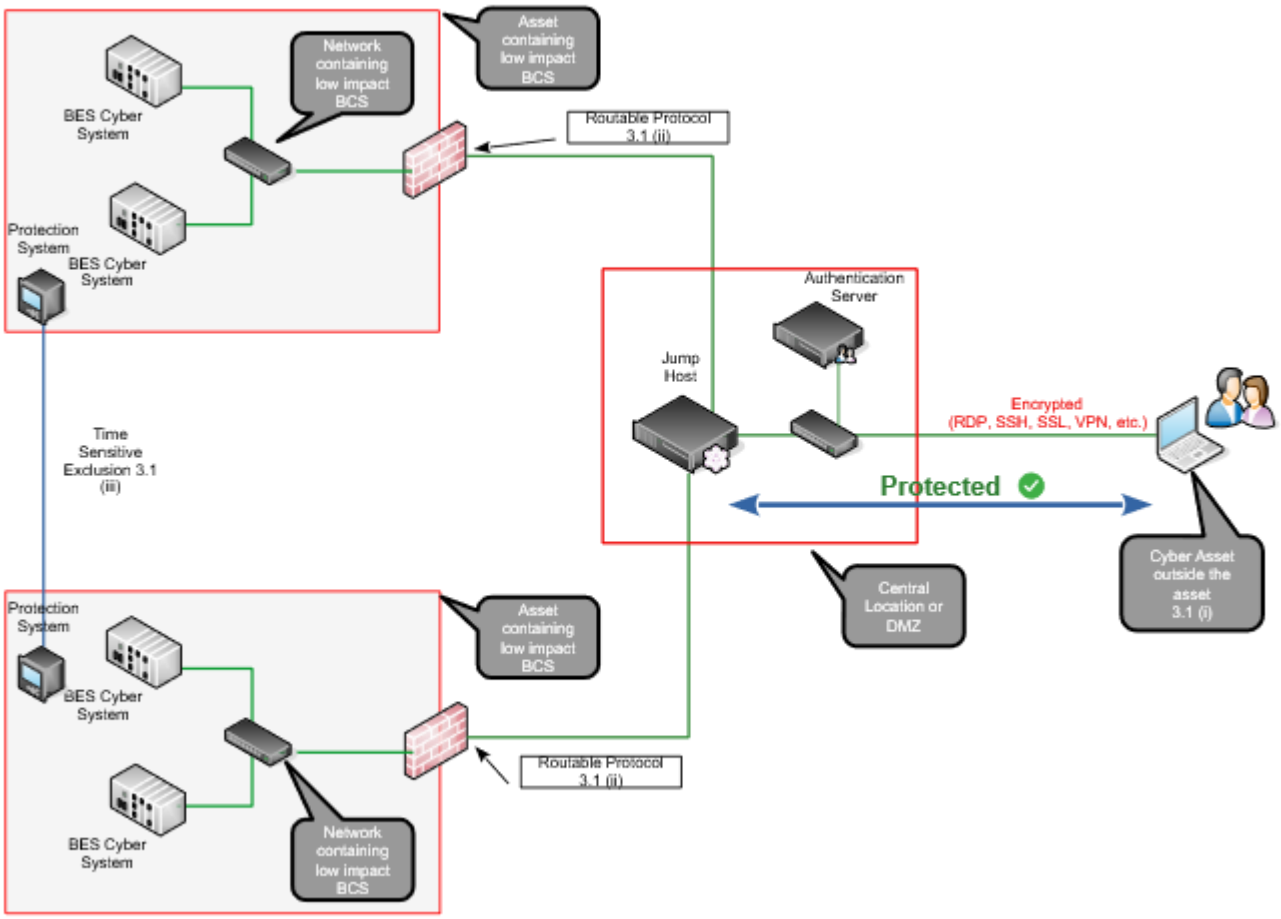


Figure 5

The DT has not required the use of an "Intermediate System" as is prescribed in CIP-005 Requirement R2 for high and medium impact BES Cyber Systems. However, the DT's intent is that those who have such infrastructures in place can, if they choose, use them for access to the assets containing low impact BES Cyber Systems to satisfy the intent of these requirements. While prescribing such an architecture as in CIP-005 Requirement R2 would make the target of CIP-003's requirements clearer to describe, the DT has chosen not to be this prescriptive due to the wide diversity of entities that may have only LIBCS. For example, an entity may have one small renewable generation site that falls under CIP-003 and implementing a full CIP-005 Requirement R2 "Interactive Remote Access with Intermediate System" architecture for access to one site may be excessive. That entity may only need an SSL VPN to an access control device (e.g., firewall) at the one site that authenticates the user and then allows access to the network containing LIBCS on its inside interface. However, an entity with 100 assets with BES Cyber Systems of varying impact categorization over a large geographic area may want to use their CIP-005 Requirement R2 remote access solution for all of their sites. The DT's intent in the CIP-003 language is to allow flexibility for both.

Section 3.1.5

The objective of Section 3.1.5 is to maintain the original language used in CIP-003-10, Section 6.1. One or more method(s) can be identified as part of this electronic access control. Entities must determine vendor electronic remote access, where permitted, to their LIBCS. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access.

Section 3.1.6

The objective of Section 3.1.6 is to maintain the original language used in CIP-003-10, Section 6.2. One or more method(s) can be identified as part of this electronic access control. Entities must have the ability to disable vendor electronic remote access, where permitted, for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing LIBCS.

Section 3.2

The DT made conforming changes to Section 3.2 with the objective to maintain the original intent of CIP-003-10, Section 3.2.

Special Scenarios

One low impact BES Cyber System across more than one asset containing that system.
In this scenario, a low impact BES Cyber System is not entirely located within one asset. For example, a generation resource has the majority of its BES Cyber System components within the site, but its network is extended full-time (e.g., over a dedicated circuit or dedicated VPN) to an operator console located at another site, and the console is part of the single BES Cyber System.

Since the components of the BES Cyber System are all located in "assets containing low impact BES Cyber System", just not a single asset, then this scenario is not in scope as it does not meet the condition of Section 3.1(i) of "between a low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber System(s)." The intent of Section 3.1.3 is authentication of users who are not located within any other "assets containing low impact BES Cyber System." This keeps CIP-003 analogous to the same concept in CIP-005 and the Interactive Remote Access definition that excludes from Interactive Remote Access user access that originates in another of the entity's Electronic Security Perimeters, such that operators in Control Centers are not required to implement CIP-005 Requirement R2 controls such as Intermediate Systems to operate field assets. It also avoids CIP-003 becoming circular when a local user at the BES Cyber System console would need to authenticate prior to permitting access to the extended network they are already on while seated at the console.

Rationale for Attachment 2

The DT made conforming changes to Attachment 2 merging Sections 3 and 6 and provided examples of compliance related activities.

Previous CIP-003 Versions Technical Rationale

Project 2020-03 Supply Chain Low Impact Revisions (CIP-003-9) Technical Rationale
Project 2016-02 Modifications to CIP Standards (CIP-003-10) Technical Rationale

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2023-04 Modifications to CIP-003

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on draft four of Reliability Standard **CIP-003-11 – Cyber Security – Security Management Controls** by **8 p.m. Eastern, Thursday, October 10, 2024.**

Additional information is available on the project page. If you have questions, contact Manager of Standards Development, Alison Oswald (via email), or at 404-275-9410.

Background

In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact Bulk Electric System (BES) Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts who were representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the Standard Authorization Request (SAR) at its March 22, 2023 meeting.

The LICRT report recognized that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The LICRT recommended enhancing the existing low impact category to further mitigate the coordinated attack risk. The proposed project will revise CIP-003-9 to add electronic access controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications for assets containing low impact BES Cyber Systems with external routable connectivity.

Please provide your responses to the questions listed below, along with any detailed comments.

Questions

1. Do you agree with the language proposed in CIP-003-11 Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

2. Do you agree with the language proposed in CIP-003-11 Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

3. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-11. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with a detailed explanation.

   ☐ Yes
   ☐ No

   Comments:

4. The DT believes the language of CIP-003-11 addresses the issues outlined in the SAR in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

5. Do you have any concerns in the way Project 2023-04 made conforming changes to CIP-003-11 to align with virtualization changes in Project 2016-02?

☐ Yes
☐ No
Comments:

6. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2023-04 Modifications to CIP-003

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2023-04 Modifications to CIP-003. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

Justification for VRFs and VSLs

- Requirement R1: There were no changes to VRFs from the previously FERC-approved CIP-003-9 Reliability Standard and only conforming or non-substantive changes to the VSLs.
- Requirement R2: The VRF did not change from the previously FERC-approved CIP-003-9 Reliability Standard. VSL changes are outlined below.
- Requirement R3: There were no changes to VRFs from the previously FERC-approved CIP-003-9 Reliability Standard and only conforming or non-substantive changes to the VSLs.
- Requirement R4: There were no changes to VRFs from the previously FERC-approved CIP-003-9 Reliability Standard and only conforming or non-substantive changes to the VSLs.

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document the electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2)	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security controls according to Requirement R2, Attachment 1,	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to implement three or more controls listed in Requirement R2, Attachment 1, Section 2. (Requirement R2)	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	Section 2. (Requirement R2) OR The Responsible Entity failed to implement one or two controls listed in Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code	OR The Responsible Entity failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code	

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

VSL Justifications for CIP-003-A, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSLs for Requirement R2 are similar to the previous VSLs of CIP-003-9, with a few revisions. Created Moderate and High VSL based on the number of controls implemented. Removed mentions of Attachment 1, Section 6, since Section 6 was merged with Section 3.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Requirement R2 is not a "binary" type requirement. Violation severity levels are clear, quantitative, and non-ambiguous.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The VSL level assignments are consistent with language in Requirement R2 and Attachment 1.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The violation severity levels relate to a single violation. A failure to do multiple portions of Requirement R2, Attachment 1 is considered a single violation.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-04 Modifications to CIP-003

Formal Comment Period Open through October 10, 2024

Now Available

A 30-day formal comment period for **CIP-003-11 – Cyber Security – Security Management Controls**, is open through **8 p.m. Eastern, Thursday, October 10, 2024**.

The fourth draft of CIP-003 is being posted for a 30-day formal comment and ballot period per the Standard Processes Manual Section 4.12.

Based on recent board adopted standards for CIP-003-9, the posted versions for the 2023-04 Modifications to CIP-003 was updated to reflect CIP-003-11. The Standards Balloting and Commenting System (SBS) does not allow edits once a ballot pool has been formed. Even though the standard versioning within the SBS states CIP-003-A, the version numbers within this posting are correct and entities will be voting on CIP-003-11.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in this draft of the standard.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*

- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Additional ballots for the standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **October 1-10, 2024**.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Manager, Standards Development, Alison Oswald (via email) or at 404-275-9410. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003 observer list” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2023-04 Modifications to CIP-003 | Draft 4
Comment Period Start Date:	9/11/2024
Comment Period End Date:	10/10/2024
Associated Ballots:	2023-04 Modifications to CIP-003 CIP-003-A AB 4 ST 2023-04 Modifications to CIP-003 Implementation Plan AB 4 OT

There were 47 sets of responses, including comments from approximately 102 different people from approximately 69 companies representing 7 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the language proposed in CIP-003-11 Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

2. Do you agree with the language proposed in CIP-003-11 Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

3. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-11. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with a detailed explanation.

4. The DT believes the language of CIP-003-11 addresses the issues outlined in the SAR in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical, or procedural justification.

5. Do you have any concerns in the way Project 2023-04 made conforming changes to CIP-003-11 to align with virtualization changes in Project 2016-02?

6. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Husam Al-Hadidi	Manitoba Hydro (System Preformance)	1,3,5,6	MRO
					Kimberly Bentley	Western Area Power Adminstration	1,6	MRO
					Jaimin Patal	Saskatchewan Power Coporation (SPC)	1	MRO
					George Brown	Pattern Operators LP	5	MRO
					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Dane Rogers	Oklahoma Gas and Electric (OG&E)	1,3,5,6	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Ayotte	ITC Holdings	1	MRO
					Andrew Coffelt	Board of Public Utilities-Kansas (BPU)	1,3,5,6	MRO
					Peter Brown	Invenergy	5,6	MRO

					Angela Wheat	Southwestern Power Administration	1	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Joshua Phillips	Southwest Power Pool	2	MRO
					Patrick Tuttle	Oklahoma Municipal Power Authority	4,5	MRO
Manitoba Hydro	Jay Sethi	1,3,5,6	MRO	Manitoba Hydro Group	Nazra Gladu	Manitoba Hydro	1	MRO
					Mike Smith	Manitoba Hydro	3	MRO
					Kristy-Lee Young	Manitoba Hydro	5	MRO
					Kelly Bertholet	Manitoba Hydro	6	MRO
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NPCC,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Jason Procuniar	Buckeye Power, Inc.	4	RF

					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1,3,4,5	WECC
					Nikki Carson-Marquis	Minnkota Power Cooperative, Inc.	1	MRO
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1,3,4,5	WECC
					Kylee Kropp	Sunflower Electric Power Corporation	1	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
Black Hills Corporation	Rachel Schuldt	6		Black Hills Corporation - All Segments	Travis Grablander	Black Hills Corporation	1	WECC
					Josh Combs	Black Hills Corporation	3	WECC
					Rachel Schuldt	Black Hills Corporation	6	WECC
					Carly Miller	Black Hills Corporation	5	WECC
					Sheila Suurmeier	Black Hills Corporation	5	WECC
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC

Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC

1. Do you agree with the language proposed in CIP-003-11 Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

FirstEnergy does not support this proposed language.

Lack of New Definitions
The standard contemplates new concepts for Low Impact BES Cyber Systems (LIBCS) but does not define what those concepts mean

3.1.2 and the Technical Rationale Makes Flawed Assumptions about Network Topology
FirstEnergy has long questioned the prevailing narrative from the SDT that the requirement from 3.1.2 is cost-effective and not overly burdensome.

Likes 0	
Dislikes 0	

Response

Ronald Hoover - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA reiterates its comments from the previous draft.

Although section 3.1.2 is within the scope of the SAR BPA still believes it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. The proposed language requires detection of known/suspected malicious communications for "inbound and outbound electronic remote access." There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5).

BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS or the applicability be changed to bring it in-line with other requirements.

Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	
Comment	

CenterPoint Energy Houston Electric, LLC (CEHE) has concerns that “User-initiated electronic access” is not clearly defined. This terminology is used in the NERC term Interactive Remote Access which more appropriately includes the term “person” in the definition. System to system access for support systems managing multiple sites typically utilize support accounts that could meet the vague description of “User-initiated electronic access”. This could enforce unnecessary requirements for systems that are already segmented from internet/corporate networks that monitor multiple sites. In section 3.1.3 of the technical rationale, the DT compares “user-initiated electronic access” to “CIP-005 Requirement R2 Interactive Remote Access”. Interactive Remote Access is clearly defined and includes the term “person”. We recommend clearly defining the term “user-initiated electronic access” and including the term “person”.

Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	

Southern Indiana Gas and Electric d/b/a CenterPoint Energy Indiana South (SIGE) has concerns that “User-initiated electronic access” is not clearly defined. This terminology is used in the NERC term Interactive Remote Access which more appropriately includes the term “person” in the definition. System to system access for support systems managing multiple sites typically utilize support accounts that could meet the vague description of “User-initiated electronic access”. This could enforce unnecessary requirements for systems that are already segmented from internet/corporate networks that monitor multiple sites. In section 3.1.3 of the technical rationale, the DT compares “user-initiated electronic access” to “CIP-005 Requirement R2 Interactive Remote Access”. Interactive Remote Access is clearly defined and includes the term “person”. We recommend clearly defining the term “user-initiated electronic access” and including the term “person”.

Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	

Attachment 1 section 3.1 can be misleading specifically “one or more controls.” It can appear that only one of the subsections is required as oppose to all. It is recommended to add “one or more controls” to each subsection and have it removed from 3.1.

Likes 0	
Dislikes 0	

Response

Jessica Cordero - Unisource - Tucson Electric Power Co. - 1

Answer	Yes
Document Name	

Comment

TEPC supports the language proposed in CIP-003-11 Attachment 1.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	Yes
Document Name	

Comment

The NAGF supports the language proposed in CIP-013-11 Attachment 1.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Ellese Murphy On Behalf of: John Sturgeon, Duke Energy , 5, 6, 1, 1; - Ellese Murphy

Answer	Yes
Document Name	

Comment

Duke Energy supports the proposed language in CIP-003-11 Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the language proposed in CIP-003-11 Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Minnesota Power supports MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC supports EEI's and NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Nick Leathers - Nick Leathers On Behalf of: David Jendras Sr, Ameren - Ameren Services, 3, 6, 1; - Nick Leathers	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Hayden Maples - Hayden Maples On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Hayden Maples	
Answer	Yes
Document Name	
Comment	

Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the Midwest Reliability Organization's NERC Standards Review Forum (MRO NSRF) on question 1	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
MRO NSRF thanks the drafting team for both their fidelity to the SAR and explicitly providing for the option of protecting user authentication information to an authentication system in part 3.1.4. instead of only requiring protection all the way to the low impact asset. This facilitates the Attachment 1 lead-in statement allowing for the use of “policies, procedures, and processes for their high or medium impact BCS” to satisfy Section 3.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Please see EEI comments	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

NV Energy thanks the drafting team for both their fidelity to the SAR and explicitly providing for the option of protecting user authentication information to an authentication system in part 3.1.4. instead of only requiring protection all the way to the low impact asset. This facilitates the Attachment 1 lead-in statement allowing for the use of “policies, procedures, and processes for their high or medium impact BCS” to satisfy Section 3.

Likes 0	
Dislikes 0	

Response

Matthew Nicklin - Southern Illinois Power Cooperative - 1,3,5 - SERC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Do you agree with the language proposed in CIP-003-11 Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	No
Document Name	

Comment

We are not clear on what the SDT is trying to say in the following:

From Section 4 of Attachment 2:

Section 3.1.4: documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- The asset containing low impact BCS or SCI that supports a low impact BCS,

It seems that the bullet is an exact duplicate of the body of the explanation above the bullet? Is the SDT trying to cover communications between two (2) different LIBCS with this statement?

Likes 0	
Dislikes 0	

Response

TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

Southern Indiana Gas and Electric d/b/a CenterPoint Energy Indiana South (SIGE) has the same concerns as addressed in question 1.

Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CEHE) has the same concerns addressed in question 1.

Likes 0	
Dislikes 0	

Response

Ronald Hoover - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA reiterates its comments from the previous draft.

Although section 3.1.2 is within the scope of the SAR BPA still believes it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. The proposed language requires detection of known/suspected malicious communications for "inbound and outbound electronic remote access." There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5).

BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS or the applicability be changed to bring it in-line with other requirements.

BPA recommends the SDT include a documentation option outside of OEM spec sheets as, depending on equipment, these may not be available. BPA also believes internal proof of testing should be allowable in case OEM was not available.

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

FirstEnergy does not support this proposed language.

Lack of New Definitions
The standard contemplates new concepts for Low Impact BES Cyber Systems (LIBCS) but does not define what those concepts mean

3.1.2 and the Technical Rationale Makes Flawed Assumptions about Network Topology
FirstEnergy has long questioned the prevailing narrative from the SDT that the requirement from 3.1.2 is cost-effective and not overly burdensome.

Likes 0	
Dislikes 0	

Response

Matthew Nicklin - Southern Illinois Power Cooperative - 1,3,5 - SERC

Answer	No
Document Name	

Comment

We are not clear on what the SDT is trying to say in the following:

From Section 4 of Attachment 2:

Section 3.1.4: documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System outside the asset containing low impact BCS or SCI that supports a low impact BCS and

• The asset containing low impact BCS or SCI that supports a low impact BCS,

It seems that the bullet is an exact duplicate of the body of the explanation above the bullet? Is the SDT trying to cover communications between two (2) different LIBCS with this statement?

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

NV Energy appreciates the additional effort expended by the drafting team to list so many examples of what can be cited by Registered Entities as evidence of compliance, while also acknowledging that the list of examples is not limiting or exclusive.

Likes 0	
Dislikes 0	

Response

Selene Willis - Edison International - Southern California Edison Company - 5

Answer	Yes
Document Name	
Comment	
Please see EEI comments	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
MRO NSRF appreciates the additional effort expended by the drafting team to list so many examples of what can be cited by Registered Entities as evidence of compliance, while also acknowledging that the list of examples is not limiting or exclusive.	
Likes 0	
Dislikes 0	
Response	
Hayden Maples - Hayden Maples On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Hayden Maples	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the Midwest Reliability Organization's NERC Standards Review Forum (MRO NSRF) on question 2	
Likes 0	
Dislikes 0	
Response	
Nick Leathers - Nick Leathers On Behalf of: David Jendras Sr, Ameren - Ameren Services, 3, 6, 1; - Nick Leathers	

Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC supports EEI's and NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment	
EEI supports the language proposed in CIP-003-11 Attachment 2 as it conforms with language in Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: John Sturgeon, Duke Energy , 5, 6, 1, 1; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the proposed language in CIP-003-11 Attachment 2.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	

The NAGF supports the language proposed in CIP-013-11 Attachment 2.	
Likes 0	
Dislikes 0	
Response	
Jessica Cordero - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
TEPC supports the language proposed in CIP-003-11 Attachment 2.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

3. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-11. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with a detailed explanation.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

FirstEnergy does not support this proposed language.

Lack of New Definitions
The standard contemplates new concepts for Low Impact BES Cyber Systems (LIBCS) but does not define what those concepts mean

3.1.2 and the Technical Rationale Makes Flawed Assumptions about Network Topology
FirstEnergy has long questioned the prevailing narrative from the SDT that the requirement from 3.1.2 is cost-effective and not overly burdensome.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	

Comment

Additional factors to consider include the number of projects affecting this standard, such as virtualization changes, given the limited time available to successfully transition and integrate all these updates.

Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

CEHE does not oppose the proposed implementation plan for CIP-003-11.

Likes 0	
Dislikes 0	
Response	
Jessica Cordero - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
TEPC supports the proposed implementation plan.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the proposed three (3) year implementation plan for CIP-003-11.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: John Sturgeon, Duke Energy , 5, 6, 1, 1; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the proposed Implementation Plan.	
Likes 0	
Dislikes 0	

Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed three-year implementation plan for CIP-003-11.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power’s implementation of the proposed rule changes is not expected to be as expansive as other utilities given that we already use LDAP, VPN and 2FA technologies for more than 75% of it’s Low Impact Assets; it is expected that we will implement additional security monitoring to ensure the security and reliability of the BES in relation to these standard changes.	
Likes 0	
Dislikes 0	
Response	

Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC supports EEI's and NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Nick Leathers - Nick Leathers On Behalf of: David Jendras Sr, Ameren - Ameren Services, 3, 6, 1; - Nick Leathers	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Hayden Maples - Hayden Maples On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Hayden Maples	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the Midwest Reliability Organization's NERC Standards Review Forum (MRO NSRF) on question 3	
Likes 0	
Dislikes 0	
Response	

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
MRO NSRF understands that three years is essentially the longest period NERC will approve for implementation. While industry was concerned with the large number of low impact assets affected, the additional time provided for the detection of malicious communications is greatly appreciated and eases implementation concerns.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Please see EEI comments	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy understands that three years is essentially the longest period NERC will approve for implementation. While industry was concerned with the large number of low impact assets affected, the additional time provided for the detection of malicious communications is greatly appreciated and eases implementation concerns.	
Likes 0	
Dislikes 0	
Response	

Matthew Nicklin - Southern Illinois Power Cooperative - 1,3,5 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Hoover - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

4. The DT believes the language of CIP-003-11 addresses the issues outlined in the SAR in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical, or procedural justification.

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

While acknowledging that the SDT was bound by the SAR in drafting this revision, NV Energy does not believe the expected cost to address the risk to the many assets containing low impact BES Cyber Systems is appropriate. The costs will especially impact those Registered Entities that do not have high or medium impact policies, procedures or infrastructure that can be scaled up (although also at significant expense) to cover low impact assets.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez

Answer	No
Document Name	

Comment

SRP believes that these proposed changes will result in strain on revised cyber security policies and procedures, hire and train new staff cyber security controls, purchase, procure, and install new technologies, and/or reconfigure system network or security architects.

Likes 0	
Dislikes 0	

Response

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	No
Document Name	

Comment

While acknowledging that the SDT was bound by the SAR in drafting this revision, the MRO NSRF does not believe the expected cost to address the risk to the many assets containing low impact BES Cyber Systems is appropriate. The costs will especially impact those Registered Entities that do not

have high or medium impact policies, procedures or infrastructure that can be scaled up (although also at significant expense) to cover low impact assets.	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ITC supports NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
IID believes that the language in CIP-003-11 will place additional pressure on our current compliance responsibilities, including the need to update our cybersecurity policies and procedures, potentially hire and train new personnel, implement new technologies, and reconfigure network systems.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	

While Minnesota Power has implemented SSLVPNs to many Low Impact Assets, and has existing authentications to Low Impact Generation Assets, there are costs associated with the procurement and implementation of the technologies.

Likes 0	
Dislikes 0	

Response

Jessica Cordero - Unisource - Tucson Electric Power Co. - 1

Answer	No
Document Name	

Comment

TEPC has not adressed if this is a cost-effective solution.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	No
Document Name	

Comment

Reclamation identifies that more information is needed to adequately assess the cost effectiveness of the proposed approach.

Likes 0	
Dislikes 0	

Response

Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna

Answer	No
Document Name	

Comment

It cannot be determined at this time if the language of CIP-003-11 addresses the issues in a cost effective manner.

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

FirstEnergy does not support this proposed language.

Lack of New Definitions
The standard contemplates new concepts for Low Impact BES Cyber Systems (LIBCS) but does not define what those concepts mean

3.1.2 and the Technical Rationale Makes Flawed Assumptions about Network Topology
FirstEnergy has long questioned the prevailing narrative from the SDT that the requirement from 3.1.2 is cost-effective and not overly burdensome.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Selene Willis - Edison International - Southern California Edison Company - 5

Answer	Yes
Document Name	

Comment

Please see EEI comments

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hayden Maples - Hayden Maples On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Hayden Maples	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: John Sturgeon, Duke Energy , 5, 6, 1, 1; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Hoover - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matthew Nicklin - Southern Illinois Power Cooperative - 1,3,5 - SERC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Nick Leathers - Nick Leathers On Behalf of: David Jendras Sr, Ameren - Ameren Services, 3, 6, 1; - Nick Leathers

Answer	
Document Name	

Comment

Ameren will not comment on the cost effectiveness of the project

Likes 0	
Dislikes 0	

Response

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	
Document Name	

Comment

GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.

Likes 0	
Dislikes 0	

Response
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments
Answer	
Document Name	
Comment
Black Hills Corporation will not comment on cost effectiveness.
Likes 0	
Dislikes 0	
Response
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE
Answer	
Document Name	
Comment
CEHE does not comment on costs.
Likes 0	
Dislikes 0	
Response
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP
Answer	
Document Name	
Comment
No comments on cost-effectiveness.
Likes 0	
Dislikes 0	
Response

5. Do you have any concerns in the way Project 2023-04 made conforming changes to CIP-003-11 to align with virtualization changes in Project 2016-02?

Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NextEra supports EEI comments below: EEI supports the way Project 2023-04 made conforming changes to CIP-003-11 to align with virtualization changes in Project 2016-02.	
Likes 0	
Dislikes 0	
Response	

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CEHE has no comments.	
Likes 0	
Dislikes 0	
Response	

Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI. EEI supports the way Project 2023-04 made conforming changes to CIP-003-11 to align with virtualization changes in Project 2016-02.	
Likes 0	

Dislikes 0	
Response	
Jessica Cordero - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
TEPC supports the DT edits to align with the virtualization changes.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI supports the way Project 2023-04 made conforming changes to CIP-003-11 to align with virtualization changes in Project 2016-02.	
Likes 0	
Dislikes 0	
Response	

Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ITC supports EEI's and NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Hayden Maples - Hayden Maples On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Hayden Maples	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the Midwest Reliability Organization's NERC Standards Review Forum (MRO NSRF) on question 5	
Likes 0	
Dislikes 0	
Response	

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
MRO NSRF believes this was a prudent move as NERC has already sent CIP-003-10 to FERC for approval.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy believes this was a prudent move as NERC has already sent CIP-003-10 to FERC for approval.	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy has no issues with these changes to align the virtualization changes from CIP-003-10 to CIP-003-11.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: John Sturgeon, Duke Energy , 5, 6, 1, 1; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
No, Duke Energy supports the confirming changes.	

Likes 0	
Dislikes 0	
Response	
Nick Leathers - Nick Leathers On Behalf of: David Jendras Sr, Ameren - Ameren Services, 3, 6, 1; - Nick Leathers	
Answer	Yes
Document Name	
Comment	
How would this change if we had virtual firewalls?	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Please see EEI comments	
Likes 0	
Dislikes 0	

Response	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Considering the number of projects impacting the standard, there is limited time available to effectively transition and successfully integrate all these changes.	
Likes 0	
Dislikes 0	
Response	
Matthew Nicklin - Southern Illinois Power Cooperative - 1,3,5 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

6. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see EEI comments	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	2023-04_Unofficial_Comment_Form_Additional_Ballot_3_091124_Final Comments.docx
Comment	
See comments submitted by the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	
Document Name	
Comment	
We want to thank the SDT for their hard work and allowing us to provide feedback.	
Likes 0	
Dislikes 0	
Response	

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	
Document Name	
Comment	
MRO NSRF appreciates the drafting team addressing industry's concern with the previous CIP-003-12 implementation plan that allowed for possibility of FERC bypassing the previously proposed CIP-003-11 and approving both CIP-003-10 and CIP-003-12 (or even just CIP-003-12) which would have reduced the implementation time from 36 months to 24 months. We are also very grateful for the additional time to implement detection of malicious communications.	
Likes 0	
Dislikes 0	
Response	
Hayden Maples - Hayden Maples On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Hayden Maples	
Answer	
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the Midwest Reliability Organization's NERC Standards Review Forum (MRO NSRF) on question 6	
Likes 0	
Dislikes 0	
Response	
Nick Leathers - Nick Leathers On Behalf of: David Jendras Sr, Ameren - Ameren Services, 3, 6, 1; - Nick Leathers	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	

Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	
Document Name	
Comment	
ITC supports EEI's and NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	
Document Name	
Comment	
Even though there weren't any redlines in section 5 of Attachment 1 for TCAs, we would like to point out that authentication is not required for assets registered as TCAs. For example, our field personnel are acquiring test equipment that will be inventoried and registered as a transient asset, but lacks strong authentication and is not integrated with any AD/LDAP services. Furthermore, we operate within a geographical region characterized by limited access of local academic enrichment opportunities for professionals in cybersecurity. Moreover, this project will require significant technical effort, substantial capital investment, and the augmentation of staffing resources.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
Minnesota Power feels that low impact security and response requirements should be moved to the respective CIP standard of which is already in-place for Medium and High Impact assets. For example, Cyber Security Awareness requirements should be rolled into CIP-004; Physical Security requirements should be rolled into CIP-006, Electronic Security Perimeter Requirements should be rolled into CIP-005, and Cyber Security Incident Response should be rolled into CIP-008, etc.	

This will align low impact with high and medium impacts and place all the specific requirements within one standard and not spread out across multiple standards. This will also allow CIP-003 to maintain its original purpose, “Security Management Controls”.

In addition, Minnesota Power supports EEI response and has concern with how section 1.1 and 1.3 are currently written. We support EEI’s version of this language.

Likes 0	
Dislikes 0	

Response

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	

Comment

EEI offers the following non-substantive changes for consideration:

CIP-003-11 Section C. Compliance includes modifications to the 1.1 Compliance Enforcement Authority definition that do not align with the definition in the Rules of Procedure that became effective June 27, 2024. Please modify the definition to align as follows:

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and/or enforcing compliance with **the NERC Reliability Standards**.

Additionally, 1.3 Compliance Monitoring and Enforcement Program in CIP-003-011 does not align with the defined term in the Rules of Procedure that became effective June 27, 2024. Please modify the definition to align as follows:

1.3 Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” **means, depending on the context (1) the NERC *Compliance Monitoring and Enforcement Program* (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities’ compliance with Reliability Standards**.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon in responding in support of the EEI to this question.

Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: John Sturgeon, Duke Energy , 5, 6, 1, 1; - Ellese Murphy	
Answer	
Document Name	
Comment	
Duke Energy does not have any additional comments.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF has no additional comments.	
Likes 0	
Dislikes 0	

Response	
James Keele - Entergy - 3	
Answer	
Document Name	
Comment	
Entergy is concerned that the proposed requirements for Low Impact Electronic Access Controls in some cases exceed the requirements for Medium Impact BCS (e.g. protecting authentication information if not identified as BCSI), or require controls that are explicitly excluded from some Medium Impact facility types. For example, proposed CIP-003-11 R2 Attachment 1 Section 3.1.2 requires entities to “detect known or suspected malicious communications for both inbound or outbound electronic access” for all Low Impact BCS including Control Centers, Generation Facilities, Substations, and more. However, this requirement reads nearly identically to CIP-005-7 R1.5 which is only applicable to Control Centers per the current definition of High Impact BCS and the specific use of “Medium Impact BES Cyber Systems at Control Centers”. Entergy’s concerned that this strays away from the risk-based approach that the impact ratings are meant to imply, and instead of a steady “trickle-down” of controls across risk levels would result in a more complicated control and process structure that could result in increased likelihood of confusion and human error.	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	
Document Name	
Comment	
The Violation Severity Levels for R2 contain references to Attachment 1, Section 6. Section 6 in Attachment 1 has been deleted.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	

Black Hills Corporation is concerned about having multiple CIP-003 projects and multiple virtualization projects occurring simultaneously as it is becoming difficult to maintain oversight of the changes to a degree that allows sufficient review. In addition, how is NERC ensuring that the direction of these multiple projects maintain alignment?

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker

Answer	
Document Name	

Comment

See EEI comments.

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group

Answer	
Document Name	

Comment

Manitoba Hydro appreciates the drafting team’s implementation of industry feedback and is supportive of the changes made.

Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	
Document Name	

Comment

CEHE has concerns about The Violation Severity Levels for R2 contain references to Attachment 1, Section 6. Section 6 in Attachment 1 has been deleted.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	
Document Name	

Comment

NextEra suports EEI's comments below:

EEI offers the following non-substantive changes for consideration:

CIP-003-11 Section C. Compliance includes modifications to the 1.1 Compliance Enforcement Authority definition that do not align with the definition in the Rules of Procedure that became effective June 27, 2024. Please modify the definition to align as follows:

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure,

“Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with **the NERC Reliability Standards** mandatory and enforceable Reliability Standards in their respective jurisdictions.

Additionally, 1.3 Compliance Monitoring and Enforcement Program in CIP-003-011 does not align with the defined term in the Rules of Procedure that became effective June 27, 2024. Please modify the definition to align as follows:

1.3 Compliance Monitoring and Enforcement Program: As defined in the NERC Rules

of Procedure, “Compliance Monitoring and Enforcement Program” **means, depending on the context (1) the NERC *Compliance Monitoring and Enforcement Program* (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities’ compliance with Reliability Standards** refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	
Document Name	

Comment

CPS Energy does not have any additional comments.

Likes 0	
Dislikes 0	

Response
Donald Lock - Talen Generation, LLC - 5
Answer	
Document Name	
Comment
R3.1.5, "Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted," is incomprehensible. Did you mean to say, "authorizing," instead of, "determining," i.e. giving approval for granting access? Please clarify this requirement in the final standard.
Likes 0	
Dislikes 0	
Response
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter
Answer	
Document Name	
Comment
See above comments on behalf of FirstEnergy.
Likes 0	
Dislikes 0	
Response
Matthew Nicklin - Southern Illinois Power Cooperative - 1,3,5 - SERC
Answer	
Document Name	
Comment
We want to thank the SDT for their hard work and allowing us to provide feedback.
Likes 0	
Dislikes 0	
Response

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2023-04 Modifications to CIP-003 | Draft 4
Comment Period Start Date:	9/11/2024
Comment Period End Date:	10/10/2024
Associated Ballot(s):	2023-04 Modifications to CIP-003 CIP-003-A AB 4 ST 2023-04 Modifications to CIP-003 Implementation Plan AB 4 OT

There were 47 sets of responses, including comments from approximately 102 different people from approximately 69 companies representing 7 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, contact Director, Standards Development Jamie Calderon (via email) or at (404) 446-9647.

Questions

1. Do you agree with the language proposed in CIP-003-11 Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

2. Do you agree with the language proposed in CIP-003-11 Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

3. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-11. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with a detailed explanation.

4. The DT believes the language of CIP-003-11 addresses the issues outlined in the SAR in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical, or procedural justification.

5. Do you have any concerns in the way Project 2023-04 made conforming changes to CIP-003-11 to align with virtualization changes in Project 2016-02?

6. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Husam Al-Hadidi	Manitoba Hydro (System Performance)	1,3,5,6	MRO
					Kimberly Bentley	Western Area Power Administration	1,6	MRO
					Jaimin Patal	Saskatchewan Power Corporation (SPC)	1	MRO
					George Brown	Pattern Operators LP	5	MRO
					Larry Heckert	Alliant Energy (ALTE)	4	MRO

Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
Dane Rogers	Oklahoma Gas and Electric (OG&E)	1,3,5,6	MRO
Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
Michael Ayotte	ITC Holdings	1	MRO
Andrew Coffelt	Board of Public Utilities-Kansas (BPU)	1,3,5,6	MRO
Peter Brown	Invenergy	5,6	MRO
Angela Wheat	Southwestern Power Administration	1	MRO
Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
Joshua Phillips	Southwest Power Pool	2	MRO
Patrick Tuttle	Oklahoma Municipal Power Authority	4,5	MRO

Manitoba Hydro	Jay Sethi	1,3,5,6	MRO	Manitoba Hydro Group	Nazra Gladu	Manitoba Hydro	1	MRO
					Mike Smith	Manitoba Hydro	3	MRO
					Kristy-Lee Young	Manitoba Hydro	5	MRO
					Kelly Bertholet	Manitoba Hydro	6	MRO
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NPCC,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy	1	RF

						Electric Cooperative		
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Jason Procuniar	Buckeye Power, Inc.	4	RF
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1,3,4,5	WECC
					Nikki Carson-Marquis	Minnkota Power Cooperative, Inc.	1	MRO
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1,3,4,5	WECC
					Kylee Kropp	Sunflower Electric Power Corporation	1	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF

					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy- FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
Black Hills Corporation	Rachel Schuldt	6		Black Hills Corporation - All Segments	Travis Grablander	Black Hills Corporation	1	WECC
					Josh Combs	Black Hills Corporation	3	WECC
					Rachel Schuldt	Black Hills Corporation	6	WECC
					Carly Miller	Black Hills Corporation	5	WECC
					Sheila Suurmeier	Black Hills Corporation	5	WECC
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC

					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC

1. Do you agree with the language proposed in CIP-003-11 Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy does not support this proposed language. Lack of New Definitions The standard contemplates new concepts for Low Impact BES Cyber Systems (LIBCS) but does not define what those concepts mean 3.1.2 and the Technical Rationale Makes Flawed Assumptions about Network Topology FirstEnergy has long questioned the prevailing narrative from the SDT that the requirement from 3.1.2 is cost-effective and not overly burdensome.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT kept concepts that were already in place and did not define a new term to continue to allow entities to develop their program based on their own unique circumstances. The team tried to explain various options in the TR but the document does not contain every scenario. The DT drafted the requirements as objectives and not prescribed methods so there are various ways of satisfying the requirement.	
Ronald Hoover - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA reiterates its comments from the previous draft.

Although section 3.1.2 is within the scope of the SAR BPA still believes it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. The proposed language requires detection of known/suspected malicious communications for “inbound and outbound electronic remote access.” There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5).

BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS or the applicability be changed to bring it in-line with other requirements.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT understands this is a new requirement for lows, however overall there are more requirements associated with mediums than there are lows (please see the October 2022 Low Impact Criteria Review Report).

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CEHE) has concerns that “User-initiated electronic access” is not clearly defined. This terminology is used in the NERC term Interactive Remote Access which more appropriately includes the term “person” in the definition. System to system access for support systems managing multiple sites typically utilize support accounts that could meet the vague description of “User-initiated electronic access”. This could enforce unnecessary requirements for systems that are already segmented from internet/corporate networks that monitor multiple sites. In section 3.1.3 of the technical rationale, the DT compares “user-initiated electronic access” to “CIP-005 Requirement R2 Interactive Remote Access”. Interactive Remote Access is clearly defined and includes the term “person”. We recommend clearly defining the term “user-initiated electronic access” and including the term “person”.

Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The DT believes by the construction of the Attachment 1 Section 3.1.3, the standard is meeting the objective to authenticate each user not authenticate user-initiated electronic access. The descriptor user-initiated electronic access was used to scope the access to user access as opposed to system-to-system access specifically for authentication subparts.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
Southern Indiana Gas and Electric d/b/a CenterPoint Energy Indiana South (SIGE) has concerns that “User-initiated electronic access” is not clearly defined. This terminology is used in the NERC term Interactive Remote Access which more appropriately includes the term “person” in the definition. System to system access for support systems managing multiple sites typically utilize support accounts that could meet the vague description of “User-initiated electronic access”. This could enforce unnecessary requirements for systems that are already segmented from internet/corporate networks that monitor multiple sites. In section 3.1.3 of the technical rationale, the DT compares “user-initiated electronic access” to “CIP-005 Requirement R2 Interactive Remote Access”. Interactive Remote Access is clearly defined and includes the term “person”. We recommend clearly defining the term “user-initiated electronic access” and including the term “person”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT believes by the construction of the Attachment 1 Section 3.1.3, the standard is meeting the objective to authenticate each user not authenticate user-initiated electronic access. The descriptor user-initiated electronic access was used to scope the access to user access as opposed to system-to-system access specifically for authentication subparts.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	

Comment	
Attachment 1 section 3.1 can be misleading specifically “one or more controls.” It can appear that only one of the subsections is required as opposed to all. It is recommended to add “one or more controls” to each subsection and have it removed from 3.1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT believes based on the sentence structure that “one or more controls” applies to all the subparts.	
Jessica Cordero - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
TEPC supports the language proposed in CIP-003-11 Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the language proposed in CIP-013-11 Attachment 1.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Ellese Murphy - Ellese Murphy On Behalf of: John Sturgeon, Duke Energy , 5, 6, 1, 1; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the proposed language in CIP-003-11 Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the language proposed in CIP-003-11 Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to MRO NSRF.	
Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	

ITC supports EEI's and NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI and NSRF.	
Nick Leathers - Nick Leathers On Behalf of: David Jendras Sr, Ameren - Ameren Services, 3, 6, 1; - Nick Leathers	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Hayden Maples - Hayden Maples On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Hayden Maples	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the Midwest Reliability Organization's NERC Standards Review Forum (MRO NSRF) on question 1	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI and MRO NSRF.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
MRO NSRF thanks the drafting team for both their fidelity to the SAR and explicitly providing for the option of protecting user authentication information to an authentication system in part 3.1.4. instead of only requiring protection all the way to the low impact asset. This facilitates the Attachment 1 lead-in statement allowing for the use of "policies, procedures, and processes for their high or medium impact BCS" to satisfy Section 3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Please see EEI comments	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment, please see response to EEI.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy thanks the drafting team for both their fidelity to the SAR and explicitly providing for the option of protecting user authentication information to an authentication system in part 3.1.4. instead of only requiring protection all the way to the low impact asset. This facilitates the Attachment 1 lead-in statement allowing for the use of “policies, procedures, and processes for their high or medium impact BCS” to satisfy Section 3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Matthew Nicklin - Southern Illinois Power Cooperative - 1,3,5 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gladys DeLaO - CPS Energy - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

2. Do you agree with the language proposed in CIP-003-11 Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	

We are not clear on what the SDT is trying to say in the following:

From Section 4 of Attachment 2:

Section 3.1.4: documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- The asset containing low impact BCS or SCI that supports a low impact BCS,

It seems that the bullet is an exact duplicate of the body of the explanation above the bullet? Is the SDT trying to cover communications between two (2) different LIBCS with this statement?

Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The language is not duplicative, it is trying to distinguish between the cyber system outside the low impact asset and within the low impact asset.

TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No

Document Name	
Comment	
Southern Indiana Gas and Electric d/b/a CenterPoint Energy Indiana South (SIGE) has the same concerns as addressed in question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to Question 1.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) has the same concerns addressed in question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to Question 1.	
Ronald Hoover - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA reiterates its comments from the previous draft.	

Although section 3.1.2 is within the scope of the SAR BPA still believes it creates a higher compliance bar for Low BCS than for Medium BCS outside of Control Centers and inconsistencies within the standards. The proposed language requires detection of known/suspected malicious communications for "inbound and outbound electronic remote access." There is no similar requirement for Medium BCS unless they are at a Control Center (see Draft 5 of CIP-005-8 R1.5). BPA suggests that this requirement be removed for better consistency with the requirements for Medium BCS or the applicability be changed to bring it in-line with other requirements. BPA recommends the SDT include a documentation option outside of OEM spec sheets as, depending on equipment, these may not be available. BPA also believes internal proof of testing should be allowable in case OEM was not available.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT understands this is a new requirement for lows, however overall there are more requirements associated with mediums than there are lows (please see the low impact report). The use of OEM specification sheets is only one example of what may be used. Other examples include, but are not limited to, examples of ports and services that could be used for operational purposes.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy does not support this proposed language. Lack of New Definitions The standard contemplates new concepts for Low Impact BES Cyber Systems (LIBCS) but does not define what those concepts mean	

3.1.2 and the Technical Rationale Makes Flawed Assumptions about Network Topology FirstEnergy has long questioned the prevailing narrative from the SDT that the requirement from 3.1.2 is cost-effective and not overly burdensome.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT kept concepts that were already in place and did not define a new term to continue to allow entities to develop their program based on their own unique circumstances. The team tried to explain various options in the TR but the document does not contain every scenario. The DT drafted the requirements as objectives and not prescribed methods so there are various ways of satisfying the requirement.	
Matthew Nicklin - Southern Illinois Power Cooperative - 1,3,5 - SERC	
Answer	No
Document Name	
Comment	
We are not clear on what the SDT is trying to say in the following: From Section 4 of Attachment 2: Section 3.1.4: documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System outside the asset containing low impact BCS or SCI that supports a low impact BCS and **• The asset containing low impact BCS or SCI that supports a low impact BCS,** It seems that the bullet is an exact duplicate of the body of the explanation above the bullet? Is the SDT trying to cover communications between two (2) different LIBCS with this statement?	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The language is not duplicative, it is trying to distinguish between the cyber system outside the low impact asset and within the low impact asset.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy appreciates the additional effort expended by the drafting team to list so many examples of what can be cited by Registered Entities as evidence of compliance, while also acknowledging that the list of examples is not limiting or exclusive.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Please see EEI comments	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment, please see response to EEI.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
MRO NSRF appreciates the additional effort expended by the drafting team to list so many examples of what can be cited by Registered Entities as evidence of compliance, while also acknowledging that the list of examples is not limiting or exclusive.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Hayden Maples - Hayden Maples On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Hayden Maples	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the Midwest Reliability Organization's NERC Standards Review Forum (MRO NSRF) on question 2	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI and MRO NSRF.	
Nick Leathers - Nick Leathers On Behalf of: David Jendras Sr, Ameren - Ameren Services, 3, 6, 1; - Nick Leathers	

Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC supports EEI's and NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI and MRO NSRF.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Minnesota Power supports MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to MRO NSRF.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the language proposed in CIP-003-11 Attachment 2 as it conforms with language in Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment, please see response to EEI.	
Ellese Murphy - Ellese Murphy On Behalf of: John Sturgeon, Duke Energy , 5, 6, 1, 1; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the proposed language in CIP-003-11 Attachment 2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the language proposed in CIP-013-11 Attachment 2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jessica Cordero - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes

Document Name	
Comment	
TEPC supports the language proposed in CIP-003-11 Attachment 2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gladys DeLaO - CPS Energy - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

3. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-11. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with a detailed explanation.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy does not support this proposed language. Lack of New Definitions The standard contemplates new concepts for Low Impact BES Cyber Systems (LIBCS) but does not define what those concepts mean 3.1.2 and the Technical Rationale Makes Flawed Assumptions about Network Topology FirstEnergy has long questioned the prevailing narrative from the SDT that the requirement from 3.1.2 is cost-effective and not overly burdensome.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT kept concepts that were already in place and did not define a new term to continue to allow entities to develop their program based on their own unique circumstances. The team tried to explain various options in the TR but the document	

does not contain every scenario. The DT drafted the requirements as objectives and not prescribed methods so there are various ways of satisfying the requirement.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Additional factors to consider include the number of projects affecting this standard, such as virtualization changes, given the limited time available to successfully transition and integrate all these updates.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT took into account the multiple versions of the standard in the Implementation Plan by making the version 11 effective date dependent upon the version 10 (virtualization changes) plan.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CEHE does not oppose the proposed implementation plan for CIP-003-11.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jessica Cordero - Unisource - Tucson Electric Power Co. - 1	

Answer	Yes
Document Name	
Comment	
TEPC supports the proposed implementation plan.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the proposed three (3) year implementation plan for CIP-003-11.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Ellese Murphy - Ellese Murphy On Behalf of: John Sturgeon, Duke Energy , 5, 6, 1, 1; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	

Duke Energy supports the proposed Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see the response to EEI.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed three-year implementation plan for CIP-003-11.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power’s implementation of the proposed rule changes is not expected to be as expansive as other utilities given that we already use LDAP, VPN and 2FA technologies for more than 75% of its Low Impact Assets; it is expected that we will implement additional security monitoring to ensure the security and reliability of the BES in relation to these standard changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC supports EEI's and NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI and MRO NSRF.	

Nick Leathers - Nick Leathers On Behalf of: David Jendras Sr, Ameren - Ameren Services, 3, 6, 1; - Nick Leathers	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Hayden Maples - Hayden Maples On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Hayden Maples	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the Midwest Reliability Organization's NERC Standards Review Forum (MRO NSRF) on question 3	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI and MRO NSRF.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes

Document Name	
Comment	
MRO NSRF understands that three years is essentially the longest period NERC will approve for implementation. While industry was concerned with the large number of low impact assets affected, the additional time provided for the detection of malicious communications is greatly appreciated and eases implementation concerns.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Please see EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

NV Energy understands that three years is essentially the longest period NERC will approve for implementation. While industry was concerned with the large number of low impact assets affected, the additional time provided for the detection of malicious communications is greatly appreciated and eases implementation concerns.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Matthew Nicklin - Southern Illinois Power Cooperative - 1,3,5 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ronald Hoover - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal	

Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gladys DeLaO - CPS Energy - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

4. The DT believes the language of CIP-003-11 addresses the issues outlined in the SAR in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical, or procedural justification.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
While acknowledging that the SDT was bound by the SAR in drafting this revision, NV Energy does not believe the expected cost to address the risk to the many assets containing low impact BES Cyber Systems is appropriate. The costs will especially impact those Registered Entities that do not have high or medium impact policies, procedures or infrastructure that can be scaled up (although also at significant expense) to cover low impact assets.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team acknowledges that there are costs for implementation, and believes the standard follows a risk-based methodology based on the SAR. By making broad recommendations and following the risk-based methodology, this should allow entities to choose the most cost-effective solution for their unique infrastructure.	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	No
Document Name	
Comment	

SRP believes that these proposed changes will result in strain on revised cyber security policies and procedures, hire and train new staff cyber security controls, purchase, procure, and install new technologies, and/or reconfigure system network or security architects.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team acknowledges that there are costs for implementation, and believes the standard follows a risk-based methodology based on the SAR. By making broad recommendations and following the risk-based methodology, this should allow entities to choose the most cost-effective solution for their unique infrastructure.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
While acknowledging that the SDT was bound by the SAR in drafting this revision, the MRO NSRF does not believe the expected cost to address the risk to the many assets containing low impact BES Cyber Systems is appropriate. The costs will especially impact those Registered Entities that do not have high or medium impact policies, procedures or infrastructure that can be scaled up (although also at significant expense) to cover low impact assets.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team acknowledges that there are costs for implementation, and believes the standard follows a risk-based methodology based on the SAR. By making broad recommendations and following the risk-based methodology, this should allow entities to choose the most cost-effective solution for their unique infrastructure.	
Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No

Document Name	
Comment	
ITC supports NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to MRO NSRF.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
IID believes that the language in CIP-003-11 will place additional pressure on our current compliance responsibilities, including the need to update our cybersecurity policies and procedures, potentially hire and train new personnel, implement new technologies, and reconfigure network systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team acknowledges that there are costs for implementation, and believes the standard follows a risk-based methodology based on the SAR. By making broad recommendations and following the risk-based methodology, this should allow entities to choose the most cost-effective solution for their unique infrastructure.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	

Comment	
While Minnesota Power has implemented SSLVPNs to many Low Impact Assets, and has existing authentications to Low Impact Generation Assets, there are costs associated with the procurement and implementation of the technologies.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The drafting team acknowledges that there are costs for implementation, and believes the standard follows a risk-based methodology based on the SAR. By making broad recommendations and following the risk-based methodology, this should allow entities to choose the most cost-effective solution for their unique infrastructure.	
Jessica Cordero - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
TEPC has not addressed if this is a cost-effective solution.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	

Reclamation identifies that more information is needed to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
It cannot be determined at this time if the language of CIP-003-11 addresses the issues in a cost-effective manner.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy does not support this proposed language. Lack of New Definitions The standard contemplates new concepts for Low Impact BES Cyber Systems (LIBCS) but does not define what those concepts mean	

3.1.2 and the Technical Rationale Makes Flawed Assumptions about Network Topology FirstEnergy has long questioned the prevailing narrative from the SDT that the requirement from 3.1.2 is cost-effective and not overly burdensome.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT kept concepts that were already in place and did not define a new term to continue to allow entities to develop their program based on their own unique circumstances. The team tried to explain various options in the TR but the document does not contain every scenario. The DT drafted the requirements as objectives and not prescribed methods so there are various ways of satisfying the requirement.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Please see EEI comments	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Hayden Maples - Hayden Maples On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Hayden Maples	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Ellese Murphy On Behalf of: John Sturgeon, Duke Energy , 5, 6, 1, 1; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gladys DeLaO - CPS Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Ronald Hoover - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Matthew Nicklin - Southern Illinois Power Cooperative - 1,3,5 - SERC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Nick Leathers - Nick Leathers On Behalf of: David Jendras Sr, Ameren - Ameren Services, 3, 6, 1; - Nick Leathers	
Answer	
Document Name	
Comment	
Ameren will not comment on the cost effectiveness of the project	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	

Comment	
CEHE does not comment on costs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No comments on cost-effectiveness.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

5. Do you have any concerns in the way Project 2023-04 made conforming changes to CIP-003-11 to align with virtualization changes in Project 2016-02?	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NextEra supports EEI comments below: EEI supports the way Project 2023-04 made conforming changes to CIP-003-11 to align with virtualization changes in Project 2016-02.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CEHE has no comments.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment.	
Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI. EEI supports the way Project 2023-04 made conforming changes to CIP-003-11 to align with virtualization changes in Project 2016-02.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jessica Cordero - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
TEPC supports the DT edits to align with the virtualization changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Daniel Gacek - Exelon - 1	
Answer	No

Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI supports the way Project 2023-04 made conforming changes to CIP-003-11 to align with virtualization changes in Project 2016-02.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ITC supports EEI's and NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Hayden Maples - Hayden Maples On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Hayden Maples	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the Midwest Reliability Organization's NERC Standards Review Forum (MRO NSRF) on question 5	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment, please see response to EEI and MRO NSRF.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
MRO NSRF believes this was a prudent move as NERC has already sent CIP-003-10 to FERC for approval.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy believes this was a prudent move as NERC has already sent CIP-003-10 to FERC for approval.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donald Lock - Talen Generation, LLC - 5	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy has no issues with these changes to align the virtualization changes from CIP-003-10 to CIP-003-11.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Ellese Murphy - Ellese Murphy On Behalf of: John Sturgeon, Duke Energy , 5, 6, 1, 1; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
No, Duke Energy supports the confirming changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Nick Leathers - Nick Leathers On Behalf of: David Jendras Sr, Ameren - Ameren Services, 3, 6, 1; - Nick Leathers	
Answer	Yes

Document Name	
Comment	
How would this change if we had virtual firewalls?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the DT believes the language of the standard allows for various implementation approaches as long as the objective is met.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to NPCC Regional Standards Committee.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	

Please see EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Israel Perez - Israel Perez On Behalf of: Laura Somak, Salt River Project, 3, 6, 5, 1; Mathew Weber, Salt River Project, 3, 6, 5, 1; Thomas Johnson, Salt River Project, 3, 6, 5, 1; Timothy Singh, Salt River Project, 3, 6, 5, 1; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Considering the number of projects impacting the standard, there is limited time available to effectively transition and successfully integrate all these changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT took into account the multiple versions of the standard in the Implementation Plan by making version 11 effective date dependent upon the version 10 (virtualization changes) plan.	
Matthew Nicklin - Southern Illinois Power Cooperative - 1,3,5 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Marvin Johnson - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carver Powers - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	

6. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please see EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	2023-04_Unofficial_Comment_Form_Additional_Ballot_3_091124_Final Comments.docx
Comment	
See comments submitted by the Edison Electric Institute (EEI)	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	
Document Name	
Comment	
We want to thank the SDT for their hard work and allowing us to provide feedback.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	
Document Name	
Comment	
MRO NSRF appreciates the drafting team addressing industry's concern with the previous CIP-003-12 implementation plan that allowed for possibility of FERC bypassing the previously proposed CIP-003-11 and approving both CIP-003-10 and CIP-003-12 (or even just CIP-003-12) which would have reduced the implementation time from 36 months to 24 months. We are also very grateful for the additional time to implement detection of malicious communications.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Hayden Maples - Hayden Maples On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Hayden Maples	

Answer	
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) and the Midwest Reliability Organization's NERC Standards Review Forum (MRO NSRF) on question 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI and MRO NSRF.	
Nick Leathers - Nick Leathers On Behalf of: David Jendras Sr, Ameren - Ameren Services, 3, 6, 1; - Nick Leathers	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	
Document Name	
Comment	

ITC supports EEI's and NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI and MRO NSRF.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	
Document Name	
Comment	
Even though there weren't any redlines in section 5 of Attachment 1 for TCAs, we would like to point out that authentication is not required for assets registered as TCAs. For example, our field personnel are acquiring test equipment that will be inventoried and registered as a transient asset, but lacks strong authentication and is not integrated with any AD/LDAP services. Furthermore, we operate within a geographical region characterized by limited access of local academic enrichment opportunities for professionals in cybersecurity. Moreover, this project will require significant technical effort, substantial capital investment, and the augmentation of staffing resources.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Revisions to Section 5 were not required to meet the objectives laid out in the SAR. The drafting team acknowledges that there are costs for implementation, and believes the standards follow a risk-based methodology based on the SAR. By making broad recommendations and following the risk-based methodology, this should allow entities to choose the most cost-effective solution for their unique infrastructure.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	

Answer	
Document Name	
Comment	

Minnesota Power feels that low impact security and response requirements should be moved to the respective CIP standard of which is already in-place for Medium and High Impact assets. For example, Cyber Security Awareness requirements should be rolled into CIP-004; Physical Security requirements should be rolled into CIP-006, Electronic Security Perimeter Requirements should be rolled into CIP-005, and Cyber Security Incident Response should be rolled into CIP-008, etc.

This will align low impact with high and medium impacts and place all the specific requirements within one standard and not spread out across multiple standards. This will also allow CIP-003 to maintain its original purpose, “Security Management Controls”.

In addition, Minnesota Power supports EEI response and has concern with how section 1.1 and 1.3 are currently written. We support EEI’s version of this language.

Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The DT asserts that this is beyond the scope of the SAR. The DT is not authorized in the SAR to revise all of the standards. By having the low impact contained in CIP-002 and CIP-003, this allows “low impact only Entities” to comply with those two standards. Please see response to EEI for concern with Section 1.1 and 1.3.

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	
Comment	

EEI offers the following non-substantive changes for consideration:

CIP-003-11 Section C. Compliance includes modifications to the 1.1 Compliance Enforcement Authority definition that do not align with the definition in the Rules of Procedure that became effective June 27, 2024. Please modify the definition to align as follows:

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and/or enforcing compliance with **the NERC Reliability Standards**.

Additionally, 1.3 Compliance Monitoring and Enforcement Program in CIP-003-011 does not align with the defined term in the Rules of Procedure that became effective June 27, 2024. Please modify the definition to align as follows:

1.3 Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" **means, depending on the context (1) the NERC *Compliance Monitoring and Enforcement Program* (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities' compliance with Reliability Standards**.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The definitions have been updated to align with the ROP.

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon in responding in support of the EEI to this question.

Likes 0	
Dislikes 0	

Response

Thank you for your comment, please see response to EEI.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Ellese Murphy - Ellese Murphy On Behalf of: John Sturgeon, Duke Energy , 5, 6, 1, 1; - Ellese Murphy	
Answer	
Document Name	
Comment	
Duke Energy does not have any additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	

Comment	
The NAGF has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
James Keele - Entergy - 3	
Answer	
Document Name	
Comment	
Entergy is concerned that the proposed requirements for Low Impact Electronic Access Controls in some cases exceed the requirements for Medium Impact BCS (e.g. protecting authentication information if not identified as BCSI), or require controls that are explicitly excluded from some Medium Impact facility types. For example, proposed CIP-003-11 R2 Attachment 1 Section 3.1.2 requires entities to "detect known or suspected malicious communications for both inbound or outbound electronic access" for all Low Impact BCS including Control Centers, Generation Facilities, Substations, and more. However, this requirement reads nearly identically to CIP-005-7 R1.5 which is only applicable to Control Centers per the current definition of High Impact BCS and the specific use of "Medium Impact BES Cyber Systems at Control Centers". Entergy's concerned that this strays away from the risk-based approach that the impact ratings are meant to imply, and instead of a steady "trickle-down" of controls across risk levels would result in a more complicated control and process structure that could result in increased likelihood of confusion and human error.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT understands this is a new requirement for lows, however overall there are more requirements associated with mediums than there are lows (please see the October 2022 Low Impact Criteria Review Report).	

TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	
Document Name	
Comment	
The Violation Severity Levels for R2 contain references to Attachment 1, Section 6. Section 6 in Attachment 1 has been deleted.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the incorrect references have been removed.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	
Black Hills Corporation is concerned about having multiple CIP-003 projects and multiple virtualization projects occurring simultaneously as it is becoming difficult to maintain oversight of the changes to a degree that allows sufficient review. In addition, how is NERC ensuring that the direction of these multiple projects maintain alignment?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The two DT's modifying CIP-003 were in constant communication to maintain alignment. As the virtualization project concluded, this project made edits on top of the version that was filed with FERC. Additionally, the DT took into account the multiple versions of the standard in the Implementation Plan by making the version 11 effective date dependent upon the version 10 (virtualization changes) plan.	

Clay Walker - Clay Walker On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; - Clay Walker	
Answer	
Document Name	
Comment	
See EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO, Group Name Manitoba Hydro Group	
Answer	
Document Name	
Comment	
Manitoba Hydro appreciates the drafting team's implementation of industry feedback and is supportive of the changes made.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	

CEHE has concerns about The Violation Severity Levels for R2 contain references to Attachment 1, Section 6. Section 6 in Attachment 1 has been deleted.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, the incorrect references have been removed.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NextEra supports EEI's comments below: EEI offers the following non-substantive changes for consideration:	

CIP-003-11 Section C. Compliance includes modifications to the 1.1 Compliance Enforcement Authority definition that do not align with the definition in the Rules of Procedure that became effective June 27, 2024. Please modify the definition to align as follows:

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure,

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with **the NERC Reliability Standards** mandatory and enforceable Reliability Standards in their respective jurisdictions.

Additionally, 1.3 Compliance Monitoring and Enforcement Program in CIP-003-011 does not align with the defined term in the Rules of Procedure that became effective June 27, 2024. Please modify the definition to align as follows:

1.3 Compliance Monitoring and Enforcement Program: As defined in the NERC Rules

of Procedure, "Compliance Monitoring and Enforcement Program" **means, depending on the context (1) the NERC *Compliance Monitoring and Enforcement Program* (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities' compliance with Reliability Standards** refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Likes 0	
Dislikes 0	

Response

Thank you for your comment, please see response to EEI.

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	
Document Name	
Comment	
CPS Energy does not have any additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Donald Lock - Talen Generation, LLC - 5	
Answer	
Document Name	
Comment	

R3.1.5, "Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted," is incomprehensible. Did you mean to say, "authorizing," instead of, "determining," i.e. giving approval for granting access? Please clarify this requirement in the final standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT moved this language from Section 6 to Section 3 in Attachment 1 but the wording was the same as previously approved from CIP-003-9.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
See above comments on behalf of FirstEnergy.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see previous responses to FirstEnergy.	
Matthew Nicklin - Southern Illinois Power Cooperative - 1,3,5 - SERC	
Answer	
Document Name	
Comment	
We want to thank the SDT for their hard work and allowing us to provide feedback.	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

End of Report

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reminder
Standards Announcement
Project 2023-04 Modifications to CIP-003

Additional Ballots and Non-binding Poll Open through October 10, 2024

Now Available

Additional ballots for **CIP-003-11 – Cyber Security – Security Management Controls** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels are open through **8 p.m. Eastern, Thursday, October 10, 2024**.

The fourth draft of CIP-003 is being posted for a 30-day formal comment and ballot period per the Standard Processes Manual Section 4.12.

Based on recent board adopted standards for CIP-003-9, the posted versions for the 2023-04 Modifications to CIP-003 was updated to reflect CIP-003-11. The Standards Balloting and Commenting System (SBS) does not allow edits once a ballot pool has been formed. Even though the standard versioning within the SBS states CIP-003-A, the version numbers within this posting are correct and entities will be voting on CIP-003-11.

The standard drafting team's considerations of the responses received from the last comment period are reflected in this draft of the standard.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Balloting

Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here.

Note: Votes cast in previous ballots, will not carry over to additional ballots. It is the responsibility of the registered voter in the ballot pools to place votes again. To ensure a quorum is reached, if you do not want to vote affirmative or negative, cast an abstention.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Manager, Standards Development, Alison Oswald (via email) or at 404-275-9410. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003 observer list” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-04 Modifications to CIP-003

Formal Comment Period Open through October 10, 2024

Now Available

A 30-day formal comment period for **CIP-003-11 – Cyber Security – Security Management Controls**, is open through **8 p.m. Eastern, Thursday, October 10, 2024**.

The fourth draft of CIP-003 is being posted for a 30-day formal comment and ballot period per the Standard Processes Manual Section 4.12.

Based on recent board adopted standards for CIP-003-9, the posted versions for the 2023-04 Modifications to CIP-003 was updated to reflect CIP-003-11. The Standards Balloting and Commenting System (SBS) does not allow edits once a ballot pool has been formed. Even though the standard versioning within the SBS states CIP-003-A, the version numbers within this posting are correct and entities will be voting on CIP-003-11.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in this draft of the standard.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*

- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Additional ballots for the standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **October 1-10, 2024**.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Manager, Standards Development, Alison Oswald (via email) or at 404-275-9410. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-04 Modifications to CIP-003 observer list” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/349)
Ballot Name: 2023-04 Modifications to CIP-003 CIP-003-A AB 4 ST
Voting Start Date: 10/1/2024 12:01:00 AM
Voting End Date: 10/10/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 256
Total Ballot Pool: 292
Quorum: 87.67
Quorum Established Date: 10/10/2024 2:11:06 PM
Weighted Segment Value: 93.89

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	83	1	65	0.956	3	0.044	0	7	8
Segment: 2	6	0	0	0	0	0	0	5	1
Segment: 3	62	1	48	0.941	3	0.059	0	5	6
Segment: 4	16	1	12	0.923	1	0.077	0	1	2
Segment: 5	77	1	52	0.929	4	0.071	0	5	16
Segment: 6	40	1	30	0.909	3	0.091	0	4	3
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	6	0.6	0	0	0	1	0
Totals:	292	5.6	213	5.258	14	0.342	0	29	36

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski	Brandon Smith	Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Travis Grablander		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Corn Belt Power Cooperative	Larry brusseau		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Steven Belle		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Evergy	Kevin Frick	Hayden Maples	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte	Chantal Mazza	Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	JEA	Joseph McClung		Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	LS Power Transmission, LLC	Jennifer Richardson		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Minnkota Power Cooperative Inc.	Theresa Allard	Nikki Carson-Marquis	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Daniel Valle		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Pedernales Electric Cooperative, Inc.	Bradley Collard		Abstain	N/A
1	Platte River Power Authority	Marissa Archie		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Laura Somak	Israel Perez	Affirmative	N/A
1	Santee Cooper	Chris Wagner		Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Olivia Olson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southwestern Power Administration	Angela Wheat		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Unisource - Tucson Electric Power Co.	Jessica Cordero		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Darcy O'Connell		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		Abstain	N/A
3	AEP	Leshel Hutchings		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr	Nick Leathers	Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez	Linda Henrickson	Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	BC Hydro and Power Authority	Ming Jiang		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Lincoln Burton		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Victoria Crider		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Hayden Maples	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Abstain	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	Manitoba Hydro	Mike Smith		Affirmative	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	Richard Machado		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Dane Rogers	Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Salt River Project	Mathew Weber	Israel Perez	Affirmative	N/A
3	Santee Cooper	Vicky Budreau		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Usama Tahir		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Ryan Walter		None	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		None	N/A
4	Austin Energy	Tony Hua		None	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Katrina Lyons		Affirmative	N/A
4	Illinois Municipal Electric Agency	Mary Ann Todd		Abstain	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Affirmative	N/A
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen	Kristen Eyman	Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Candace Morakinyo		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	AES - AES Corporation	Ruchi Shah		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer	Danielle Moskop	None	N/A
5	American Municipal Power	Amy Ritts		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Basin Electric Power Cooperative	Amanda Wangler		None	N/A
5	BC Hydro and Power Authority	Quincy Wang		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		Affirmative	N/A
5	Bonneville Power Administration	Milli Chennell		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar	Jamie Monette	Abstain	N/A
5	Cowlitz County PUD	Deanna Carlson		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Decatur Energy Center LLC	Megan Melham		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Barbara Marion		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Hayden Maples	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Negative	Comments Submitted
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	None	N/A
5	Great River Energy	Jacalynn Bentz		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi	Chantal Mazza	Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	JEA	John Babik		None	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Robert Kerrigan		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		None	N/A
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	Muscatine Power and Water	Chance Back		Affirmative	N/A
5	National Grid USA	Robin Berry		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Erin Wilson		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
5	NextEra Energy	Richard Vendetti		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	North Carolina Electric Membership Corporation	Reid Cashion	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Tyler Brun	Michael Johnson	Abstain	N/A
5	Pattern Operators LP	George E Brown		Negative	Third-Party Comments
5	Pine Gate Renewables	Michiko Sell		None	N/A
5	Platte River Power Authority	Jon Osell		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Loren Harbachuk		Affirmative	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Salt River Project	Thomas Johnson	Israel Perez	Affirmative	N/A
5	Santee Cooper	Carey Salisbury		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	TransAlta Corporation	Ashley Scheelar	Adam Burlock	None	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Michelle Hribar		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Imane Mrini		None	N/A
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler	Qinling Zheng	Affirmative	N/A
6	Constellation	Kimberly Turco	Jamie Monette	Abstain	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon	Ellese Murphy	Affirmative	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Evergy	Tiffany Lake	Hayden Maples	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Brandin Stoesz		Affirmative	N/A
6	New York Power Authority	Shelly Dineen		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Rebecca Blair		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Powerex Corporation	Raj Hundal		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Glen Pruitt		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Affirmative	N/A
6	Santee Cooper	Marty Watson		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Matthew O'neal		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Steve Szablya		None	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 292 of 292 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/349)
Ballot Name: 2023-04 Modifications to CIP-003 Implementation Plan AB 4 OT
Voting Start Date: 10/1/2024 12:01:00 AM
Voting End Date: 10/10/2024 8:00:00 PM
Ballot Type: OT
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 255
Total Ballot Pool: 293
Quorum: 87.03
Quorum Established Date: 10/10/2024 2:11:14 PM
Weighted Segment Value: 93.44

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	84	1	65	0.956	3	0.044	0	7	9
Segment: 2	6	0	0	0	0	0	0	5	1
Segment: 3	63	1	49	0.942	3	0.058	0	5	6
Segment: 4	16	1	12	0.923	1	0.077	0	1	2
Segment: 5	77	1	50	0.909	5	0.091	0	5	17
Segment: 6	40	1	30	0.909	3	0.091	0	4	3
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.5	5	0.5	0	0	0	1	0
Totals:	293	5.5	211	5.139	15	0.361	0	29	38

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski	Brandon Smith	Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Travis Grablander		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Corn Belt Power Cooperative	Larry brusseau		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Steven Belle		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Hayden Maples	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte	Chantal Mazza	Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	JEA	Joseph McClung		Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	LS Power Transmission, LLC	Jennifer Richardson		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Nikki Carson-Marquis	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Daniel Valle		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Pedernales Electric Cooperative, Inc.	Bradley Collard		Abstain	N/A
1	Platte River Power Authority	Marissa Archie		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Laura Somak	Israel Perez	Affirmative	N/A
1	Santee Cooper	Chris Wagner		Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Olivia Olson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southwestern Power Administration	Angela Wheat		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Unisource - Tucson Electric Power Co.	Jessica Cordero		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		Abstain	N/A
3	AEP	Leshel Hutchings		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr	Nick Leathers	Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez	Linda Henrickson	Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	BC Hydro and Power Authority	Ming Jiang		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Lincoln Burton		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Victoria Crider		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Hayden Maples	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	Manitoba Hydro	Mike Smith		Affirmative	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	Richard Machado		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Dane Rogers	Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Affirmative	N/A
3	Santee Cooper	Vicky Budreau		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Usama Tahir		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Ryan Walter		None	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		None	N/A
4	Austin Energy	Tony Hua		None	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Katrina Lyons		Affirmative	N/A
4	Illinois Municipal Electric Agency	Mary Ann Todd		Abstain	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Affirmative	N/A
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen	Kristen Eyman	Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Candace Morakinyo		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	AES - AES Corporation	Ruchi Shah		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer	Danielle Moskop	None	N/A
5	American Municipal Power	Amy Ritts		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Amanda Wangler		None	N/A
5	BC Hydro and Power Authority	Quincy Wang		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		Affirmative	N/A
5	Bonneville Power Administration	Milli Chennell		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar	Jamie Monette	Abstain	N/A
5	Cowlitz County PUD	Deanna Carlson		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Decatur Energy Center LLC	Megan Melham		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Barbara Marion		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Jeremy Harris	Hayden Maples	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Negative	Comments Submitted
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	None	N/A
5	Great River Energy	Jacalynn Bentz		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi	Chantal Mazza	Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	JEA	John Babik		None	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Robert Kerrigan		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		None	N/A
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	Muscatine Power and Water	Chance Back		Negative	Third-Party Comments
5	National Grid USA	Robin Berry		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Erin Wilson		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
5	NextEra Energy	Richard Vendetti		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Reid Cashion	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Tyler Brun	Michael Johnson	Abstain	N/A
5	Pattern Operators LP	George E Brown		Negative	Third-Party Comments
5	Pine Gate Renewables	Michiko Sell		None	N/A
5	Platte River Power Authority	Jon Osell		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Loren Harbachuk		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Affirmative	N/A
5	Santee Cooper	Carey Salisbury		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	TransAlta Corporation	Ashley Scheelar	Adam Burlock	None	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Michelle Hribar		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Imane Mrini		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler	Qinling Zheng	Affirmative	N/A
6	Constellation	Kimberly Turco	Jamie Monette	Abstain	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon	Ellese Murphy	Affirmative	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Evergy	Tiffany Lake	Hayden Maples	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Brandin Stoesz		Affirmative	N/A
6	New York Power Authority	Shelly Dineen		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Rebecca Blair		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Powerex Corporation	Raj Hundal		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Glen Pruitt		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Affirmative	N/A
6	Santee Cooper	Marty Watson		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Matthew O'neal		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Steve Szablya		None	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 293 of 293 entries

BALLOT RESULTS

Ballot Name: 2023-04 Modifications to CIP-003 CIP-003-A | Non-binding Poll AB 4 NB
Voting Start Date: 10/1/2024 12:01:00 AM
Voting End Date: 10/10/2024 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 238
Total Ballot Pool: 280
Quorum: 85
Quorum Established Date: 10/10/2024 2:54:04 PM
Weighted Segment Value: 92.75

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	55	0.948	3	0.052	13	9
Segment: 2	6	0	0	0	0	0	5	1
Segment: 3	59	1	40	0.93	3	0.07	9	7
Segment: 4	16	1	12	0.923	1	0.077	1	2
Segment: 5	74	1	44	0.917	4	0.083	8	18
Segment: 6	38	1	23	0.885	3	0.115	7	5
Segment: 7	1	0	0	0	0	0	1	0
Segment: 8	0	0	0	0	0	0	0	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	6	0.5	5	0.5	0	0	1	0
Totals:	280	5.5	179	5.103	14	0.397	45	42

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski	Brandon Smith	Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Travis Grablander		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Corn Belt Power Cooperative	Larry brusseau		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Steven Belle		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Hayden Maples	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte	Chantal Mazza	Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	JEA	Joseph McClung		Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	LS Power Transmission, LLC	Jennifer Richardson		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Nikki Carson-Marquis	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Daniel Valle		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Pedernales Electric Cooperative, Inc.	Bradley Collard		Abstain	N/A
1	Platte River Power Authority	Marissa Archie		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Laura Somak	Israel Perez	Affirmative	N/A
1	Santee Cooper	Chris Wagner		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	SaskPower	Wayne Guttormson		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Olivia Olson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southwestern Power Administration	Angela Wheat		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Unisource - Tucson Electric Power Co.	Jessica Cordero		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
2	California ISO	Darcy O'Connell		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		Abstain	N/A
3	AEP	Leshel Hutchings		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr	Nick Leathers	Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez	Linda Henrickson	Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	BC Hydro and Power Authority	Ming Jiang		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Lincoln Burton		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Victoria Crider		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Hayden Maples	Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Abstain	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	Richard Machado		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	North Carolina Electric Membership Corporation	Chris Dimisa	Scott Brame	Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Dane Rogers	Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Affirmative	N/A
3	Santee Cooper	Vicky Budreau		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Usama Tahir		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Ryan Walter		None	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		None	N/A
4	Austin Energy	Tony Hua		None	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Katrina Lyons		Affirmative	N/A
4	Illinois Municipal Electric Agency	Mary Ann Todd		Abstain	N/A
4	North Carolina Electric Membership Corporation	Richard McCall	Scott Brame	Affirmative	N/A
4	Northern California Power Agency	Marty Hostler	Chris Carnesi	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen	Kristen Eyman	Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Candace Morakinyo		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	AES - AES Corporation	Ruchi Shah		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer	Danielle Moskop	None	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Amanda Wangler		None	N/A
5	BC Hydro and Power Authority	Quincy Wang		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		Affirmative	N/A
5	Bonneville Power Administration	Milli Chennell		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar	Jamie Monette	Abstain	N/A
5	Cowlitz County PUD	Deanna Carlson		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Decatur Energy Center LLC	Megan Melham		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Barbara Marion		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Hayden Maples	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Negative	Comments Submitted
5	Florida Municipal Power Agency	Chris Gowder	LaKenya Vannorman	None	N/A
5	Great River Energy	Jacalynn Bentz		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi	Chantal Mazza	Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	JEA	John Babik		None	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Brittany Millard		Abstain	N/A
5	Los Angeles Department of Water and Power	Robert Kerrigan		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		None	N/A
5	Muscatine Power and Water	Chance Back		Affirmative	N/A
5	National Grid USA	Robin Berry		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Erin Wilson		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
5	NextEra Energy	Richard Vendetti		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Reid Cashion	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pacific Gas and Electric Company	Tyler Brun	Michael Johnson	Abstain	N/A
5	Pattern Operators LP	George E Brown		Negative	Comments Submitted
5	Pine Gate Renewables	Michiko Sell		None	N/A
5	Platte River Power Authority	Jon Osell		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Loren Harbachuk		Affirmative	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Affirmative	N/A
5	Santee Cooper	Carey Salisbury		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	TransAlta Corporation	Ashley Scheelar	Adam Burlock	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tri-State G and T Association, Inc.	Sergio Banuelos		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Michelle Hribar		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Imane Mrini		None	N/A
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler	Qinling Zheng	Affirmative	N/A
6	Constellation	Kimberly Turco	Jamie Monette	Abstain	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon	Ellese Murphy	Affirmative	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Evergy	Tiffany Lake	Hayden Maples	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Shelly Dineen		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Rebecca Blair		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	Powerex Corporation	Raj Hundal		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 2 of Grant County, Washington	Glen Pruitt		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Affirmative	N/A
6	Santee Cooper	Marty Watson		Abstain	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Matthew O'neal		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 280 of 280 entries

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final version of the proposed standard. The drafting team is posting the final documents but not conducting a final ballot per the Standard Processes Manual (SPM) section 4.13, which allows the drafting team to conclude the standards action without conducting a final ballot if: (1) the previous ballot achieved at least 85% weighted segment approval; (2) the drafting team made a good faith effort at resolving applicable objections; (3) the drafting team responded in writing to comments as required by section 4.12; and (4) the drafting team is proposing no further changes to the balloted documents. Consistent with these requirements, the last ballot received 93.89% approval. The drafting team has made a good faith effort to resolve objections and responded to comments in writing, including making minor corrections to two of the non-mandatory and enforceable sections of the standard. Per SPM section 2.5: "The only mandatory and enforceable components of a Reliability Standard are the: (1) applicability, (2) Requirements, and the (3) effective dates. The additional components are included in the Reliability Standard for informational purposes and to provide guidance to Functional Entities concerning how compliance will be assessed by the Compliance Enforcement Authority." CIP-003-11 is built on Board Approved CIP-003-10 which was created by Project 2016-02's changes for virtualization.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023
45-day formal comment period with initial ballot	October 24 – December 7, 2023
45-day formal comment period with additional ballot	January 30 – March 14, 2024
30-day formal comment period with additional ballot	June 12 – July 11, 2024
30-day formal comment period with additional ballot	September 11 – October 10, 2024

Anticipated Actions	Date
Board adoption	December 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-11

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-11:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-11.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high-level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. Compliance Monitoring and Enforcement Program: "Compliance Monitoring and Enforcement Program" or "CMEP" means, depending on the context (1) the NERC Compliance Monitoring and Enforcement Program (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities' compliance with Reliability Standards.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR	impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	the previous approval. (Part 1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the	according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment	Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2023-04
- CIP-003-11 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
10	5/9/2024	Adopted by the NERC Board of Trustees.	Modifications made by Project 2016-02.

Version	Date	Action	Change Tracking
10	TBD	FERC approval pending in Docket No. RM24-8-000	
11	TBD	Modified by Project 2023-04	

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS including any supporting SCI to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need, as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or Virtual Cyber Asset (VCA), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, where electronic access is:

i. Between:
- a low impact BCS; or
- an SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:
- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems;

the Responsible Entity shall implement one or more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for

both inbound and outbound electronic access;

3.1.3 Authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted;

3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System(s) outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BCS or SCI that supports a low impact BCS;

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, the Responsible Entity shall implement one or more control(s) that authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security

Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. For Section 3.1.1, documentation showing the permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, such as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BCS or SCI that supports a low impact BCS and a Cyber System outside the asset containing low impact BCS.
   - Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways); or
   - Original equipment manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
    - Anti-malware technologies;
    - Intrusion detection system (IDS)/intrusion prevention system (IPS);
    - Monitor or alert for changes to communication baselines;
    - Logging and alerting configuration for security incident and event management (SIEM) systems or other event correlation systems;
    - Automated or manual log reviews;
    - Alerting; or
    - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted, such as:
    - Authentication mechanism(s) including, but not limited to:
        - Utilization of public key infrastructure (PKI), lightweight directory access protocol (LDAP), remote authentication dial-in user service (RADIUS), and/or similar implemented solutions; or
        - Enforcement of multi-factor authentication (MFA).
    - Virtual private network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
    - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BCS; or
    - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System outside the asset containing low impact BCS or SCI that supports a low impact BCS and
    - The authentication system used to meet Section 3.1.3, or
    - The asset containing low impact BCS or SCI that supports a low impact BCS,

    such as protection mechanism(s) including, but not limited to:
    - Implementation of an encrypted protocol or service (hypertext transfer protocol secure (HTTPS), secure shell (SSH), etc.);
    - Implementation of an IPsec or secure sockets layer (SSL) VPN; or

- Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;
   - Security information management logging alerts;
   - Time-of-need session initiation;
   - Session recording;
   - System logs; or
   - Other operational, procedural, or technical controls.
6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Disabling vendor electronic access user or system accounts;
   - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, remote desktop, remote control, or other hardware or software used for providing vendor electronic access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or
   - Other operational, procedural, or technical controls.
7. For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final version of the proposed standard. The drafting team is posting the final documents but not conducting a final ballot per the Standard Processes Manual (SPM) section 4.13, which allows the drafting team to conclude the standards action without conducting a final ballot if: (1) the previous ballot achieved at least 85% weighted segment approval; (2) the drafting team made a good faith effort at resolving applicable objections; (3) the drafting team responded in writing to comments as required by section 4.12; and (4) the drafting team is proposing no further changes to the balloted documents. Consistent with these requirements, the last ballot received 93.89% approval, the drafting team has made a good faith effort to resolve objections and responded to comments in writing, including making minor corrections to two of the non-mandatory and enforceable sections of the standard. Per SPM section 2.5: "The only mandatory and enforceable components of a Reliability Standard are the: (1) applicability, (2) Requirements, and the (3) effective dates. The additional components are included in the Reliability Standard for informational purposes and to provide guidance to Functional Entities concerning how compliance will be assessed by the Compliance Enforcement Authority." CIP-003-11 is built on Board Approved CIP-003-10 which was created by Project 2016-02's changes for virtualization.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023
45-day formal comment period with initial ballot	October 24 – December 7, 2023
45-day formal comment period with additional ballot	January 30 – March 14, 2024
30-day formal comment period with additional ballot	June 12 – July 11, 2024
30-day formal comment period with additional ballot	September 11 – October 10, 2024

Anticipated Actions	Date

Board adoption	December 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-11

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-11:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-11.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high-level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

1.1. Compliance Enforcement Authority: ~~As defined in the NERC Rules of Procedure,~~ "Compliance Enforcement Authority" ~~(CEA)~~ means NERC or the Regional Entity in their respective roles~~, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles~~ of monitoring and~~/or~~ enforcing compliance ~~with mandatory and enforceable~~the NERC Reliability Standards ~~in their respective jurisdictions~~.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~CEA~~ Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The ~~Responsible Entity~~applicable entity shall keep data or evidence to show compliance as identified below unless directed by its ~~CEA~~ Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The ~~CEA~~ Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: ~~As defined in the NERC Rules of Procedure,~~ "Compliance Monitoring and Enforcement Program" or "CMEP" means, depending on the context (1) the NERC Compliance Monitoring and Enforcement Program (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities' compliance with Reliability Standards.~~refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR	impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	the previous approval. (Part 1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the	according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) ~~OR~~ ~~The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)~~	determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment	Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) ~~OR~~ ~~The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote~~	

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) ~~OR~~ ~~The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (Requirement R2)~~	~~access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)~~	
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of the change. (Requirement R3)			calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2023-04
- CIP-003-11 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
10	5/9/2024	Adopted by the NERC Board of Trustees.	Modifications made by Project 2016-02.

Version	Date	Action	Change Tracking
10	TBD	FERC approval pending in Docket No. RM24-8-000	
11	TBD	Modified by Project 2023-04	

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS including any supporting SCI to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need, as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or Virtual Cyber Asset (VCA), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, where electronic access is:

i. Between:
- a low impact BCS; or
- an SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:
- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems;

the Responsible Entity shall implement one or more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for

both inbound and outbound electronic access;

3.1.3 Authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted;

3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System(s) outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BCS or SCI that supports a low impact BCS;

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, the Responsible Entity shall implement one or more control(s) that authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security

Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. For Section 3.1.1, documentation showing the permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, such as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BCS or SCI that supports a low impact BCS and a Cyber System outside the asset containing low impact BCS.
   - Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways); or
   - Original equipment manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
    - Anti-malware technologies;
    - Intrusion detection system (IDS)/intrusion prevention system (IPS);
    - Monitor or alert for changes to communication baselines;
    - Logging and alerting configuration for security incident and event management (SIEM) systems or other event correlation systems;
    - Automated or manual log reviews;
    - Alerting; or
    - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted, such as:
    - Authentication mechanism(s) including, but not limited to:
        - Utilization of public key infrastructure (PKI), lightweight directory access protocol (LDAP), remote authentication dial-in user service (RADIUS), and/or similar implemented solutions; or
        - Enforcement of multi-factor authentication (MFA).
    - Virtual private network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
    - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BCS; or
    - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System outside the asset containing low impact BCS or SCI that supports a low impact BCS and
    - The authentication system used to meet Section 3.1.3, or
    - The asset containing low impact BCS or SCI that supports a low impact BCS,

    such as protection mechanism(s) including, but not limited to:
    - Implementation of an encrypted protocol or service (hypertext transfer protocol secure (HTTPS), secure shell (SSH), etc.);
    - Implementation of an IPsec or secure sockets layer (SSL) VPN; or

- Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;
   - Security information management logging alerts;
   - Time-of-need session initiation;
   - Session recording;
   - System logs; or
   - Other operational, procedural, or technical controls.
6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Disabling vendor electronic access user or system accounts;
   - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, remote desktop, remote control, or other hardware or software used for providing vendor electronic access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or
   - Other operational, procedural, or technical controls.
7. For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final version of the proposed standard. The drafting team is posting the final documents but not conducting a final ballot per the Standard Processes Manual (SPM) section 4.13, which allows the drafting team to conclude the standards action without conducting a final ballot if: (1) the previous ballot achieved at least 85% weighted segment approval; (2) the drafting team made a good faith effort at resolving applicable objections; (3) the drafting team responded in writing to comments as required by section 4.12; and (4) the drafting team is proposing no further changes to the balloted documents. Consistent with these requirements, the last ballot received 93.89% approval. The drafting team has made a good faith effort to resolve objections and responded to comments in writing, including making minor corrections to two of the non-mandatory and enforceable sections of the standard. Per SPM section 2.5: "The only mandatory and enforceable components of a Reliability Standard are the: (1) applicability, (2) Requirements, and the (3) effective dates. The additional components are included in the Reliability Standard for informational purposes and to provide guidance to Functional Entities concerning how compliance will be assessed by the Compliance Enforcement Authority." CIP-003-11 is built on Board Approved CIP-003-10 which was created by Project 2016-02's changes for virtualization.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	July 27, 2023
SAR posted for comment	March 31 – May 15, 2023
45-day formal comment period with initial ballot	October 24 – December 7, 2023
45-day formal comment period with additional ballot	January 30 – March 14, 2024
30-day formal comment period with additional ballot	June 12 – July 11, 2024
30-day formal comment period with additional ballot	September 11 – October 10, 2024

Anticipated Actions	Date

Board adoption	December 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-~~10~~11

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-~~10~~11:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See ~~"Project 2016-02 Modifications to CIP Standards~~ Implementation Plan~~."~~ for CIP-003-11.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

~~**1.2.6.** Vendor electronic remote access security controls; and~~

~~**1.2.7.**~~**1.2.6.** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS,

that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high-~~-~~level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

1.1. Compliance Enforcement Authority: ~~As defined in the NERC Rules of Procedure,~~ "Compliance Enforcement Authority" ~~(CEA)~~ means NERC or the Regional Entity ~~, or any entity as otherwise designated by an Applicable Governmental Authority,~~ in their respective roles of monitoring and~~/or~~ enforcing compliance with the NERC ~~mandatory and enforceable~~ Reliability Standards ~~in their respective jurisdictions~~.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~CEA~~ Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The ~~Responsible Entity~~applicable entity shall keep data or evidence to show compliance as identified below unless directed by its ~~CEA~~ Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The ~~CEA~~ Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: ~~As defined in the NERC Rules of Procedure,~~ "Compliance Monitoring and Enforcement Program" or "CMEP" means, depending on the context (1) the NERC Compliance Monitoring and Enforcement Program (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities' compliance with Reliability Standards. ~~refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-~~10~~11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-~~10~~11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR	impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1. (~~R1~~Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of

R #	Violation Severity Levels (CIP-003-~~1~~011)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	the previous approval. (~~R1~~Part 1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-~~1~~011)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the	according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity ~~documented~~ failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Violation Severity Levels (CIP-003-~~10~~11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) ~~OR~~ ~~The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)~~	determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment	Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) ~~OR~~ ~~The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote~~	

R #	Violation Severity Levels (CIP-003-~~1~~011)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) ~~OR~~ ~~The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (Requirement R2)~~	~~access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)~~	
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60

R #	Violation Severity Levels (CIP-003-~~10~~11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of the change. (Requirement R3)			calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project ~~2016-02~~2023-04
- CIP-003-~~10~~11 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and

Version	Date	Action	Change Tracking
			communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	

Version	Date	Action	Change Tracking
9	3/22/2023	Effective Date	April 1, 2026
10	~~TBD~~5/9/2024	~~Virtualization Modifications~~Adopted by the NERC Board of Trustees.	Modifications made by Project 2016-02.
10	TBD	FERC approval pending in Docket No. RM24-8-000	
11	TBD	Modified by Project 2023-04	

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS including any supporting SCI to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need, as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or Virtual Cyber Asset (VCA~~,~~), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact ~~BES Cyber System(s)~~BCS identified pursuant to CIP-002~~, the Responsible Entity shall implement~~ and for SCI that supports a low impact BCS, if any, where electronic access ~~controls to~~is:

~~**3.1** Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:~~

i. Between:
- ~~-~~a low impact BCS; or
- ~~An~~an SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:
- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems~~.~~;

~~Authenticate~~the Responsible Entity shall implement one or more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic access;

3.1.3 Authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted;

3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System(s) outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BCS or SCI that supports a low impact BCS;

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, the Responsible Entity shall implement one or more control(s) that authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security

Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

~~**Section 6.** Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:~~

~~**6.1** One or more method(s) for determining vendor electronic remote access;~~

~~**6.2** One or more method(s) for disabling vendor electronic remote access; and~~

~~**6.3** One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.~~

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. ~~Documentation~~ For Section 3.1.1, documentation showing ~~that at each asset or group of assets,~~ the ~~routable protocol communication as outlined in Section 3 is restricted by electronic access controls to permit~~permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, ~~except where an entity provides rationale that communications are used for time-sensitive communications of Protection Systems. Examples of~~ such ~~documentation may include, but are not limited to representative~~as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) ~~or lists~~between the low impact BCS or SCI that supports a low impact BCS and a Cyber System outside the asset containing low impact BCS.

- Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways~~)~~.); or
- ~~Documentation~~Original equipment manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Anti-malware technologies;
   - Intrusion detection system (IDS)/intrusion prevention system (IPS);
   - Monitor or alert for changes to communication baselines;
   - Logging and alerting configuration for security incident and event management (SIEM) systems or other event correlation systems;
   - Automated or manual log reviews;
   - Alerting; or
   - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted, such as:
   - Authentication mechanism(s) including, but not limited to:
     - Utilization of public key infrastructure (PKI), lightweight directory access protocol (LDAP), remote authentication dial-in user service (RADIUS), and/or similar implemented solutions; or
     - Enforcement of multi-factor authentication (MFA).
   - Virtual private network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
   - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BCS; or
   - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System outside the asset containing low impact BCS or SCI that supports a low impact BCS and
   - The authentication system used to meet Section 3.1.3, or

- The asset containing low impact BCS or SCI that supports a low impact BCS, such as protection mechanism(s) including, but not limited to:
  - Implementation of an encrypted protocol or service (hypertext transfer protocol secure (HTTPS), secure shell (SSH), etc.);
  - Implementation of an IPsec or secure sockets layer (SSL) VPN; or
  - Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;
   - Security information management logging alerts;
   - Time-of-need session initiation;
   - Session recording;
   - System logs; or
   - Other operational, procedural, or technical controls.
6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Disabling vendor electronic access user or system accounts;
   - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, remote desktop, remote control, or other hardware or software used for providing vendor electronic access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or
   - Other operational, procedural, or technical controls.

~~1.~~7. For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back

modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to

mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Section 6. Vendor Electronic Remote Access Security Controls: Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
   - steps to preauthorize access;
   - alerts generated by vendor log on;
   - session monitoring;
   - security information management logging alerts;
   - time-of-need session initiation;
   - session recording;
   - system logs; or
   - other operational, procedural, or technical controls.

2. For Section 6.2, documentation showing:
   - disabling vendor electronic remote access user or system accounts;
   - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control,

~~or other hardware or software used for providing vendor electronic remote access;~~

- ~~disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;~~
- ~~Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);~~
- ~~administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or~~
- ~~other operational, procedural, or technical controls.~~

3. ~~For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:~~
   - ~~Anti-malware technologies;~~
   - ~~Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);~~
   - ~~Automated or manual log reviews;~~
   - ~~alerting; or~~
   - ~~other operational, procedural, or technical controls.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-04 Modifications to CIP-003
Reliability Standard CIP-003-11

Applicable Standard(s)

- CIP-003-11 – Cyber Security – Security Management Controls

Requested Retirement(s)

- CIP-003-10 – Cyber Security – Security Management Controls[1]

Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- Cyber System
- Shared Cyber Infrastructure
- Virtual Cyber Asset

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

New/Modified/Retired Terms in the NERC Glossary of Terms

- None

[1] If CIP-003-10 is not currently in effect, then the currently effective version of Reliability Standard CIP-003 shall be retired immediately prior to the effective date of CIP-003-11 in the jurisdiction in which the revised standard is becoming effective.

Background

Project 2023-04 addresses modifications to CIP-003-10 in response to recommendations from the Low Impact Criteria Review Team (LICRT), which was formed by the NERC Board of Trustees to consider the potential threat and risk posed by a coordinated cyber-attack on low impact Bulk Electric System (BES) Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommended actions to address those risks. The NERC Board of Trustees accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the standard authorization request (SAR) at its March 22, 2023 meeting. In response to the SAR, Project 2023-04 proposes merging Sections 3 and 6 of CIP-003, Attachments 1 and 2 to consolidate all electronic access requirements. These revisions are captured in Reliability Standard CIP-003-11.

This implementation plan provides additional time for entities to come into compliance with Requirement R2 for the expanded scope of communications that must be monitored to detect known or suspicious malicious communications, from vendor electric remote access in CIP-003-9, to all inbound and outbound electronic access in CIP-003-11 (Attachment 1 Section 3.1.2). In determining additional time was appropriate, the Project 2023-04 drafting team considered that CIP-003-9 will become effective April 1, 2026, and two versions of the CIP-003 standard will be pending regulatory approval (CIP-003-10, CIP-003-11). The drafting team also considered that entities may have already invested significant resources to implement system architecture to monitor vendor remote access in compliance with Reliability Standard CIP-003-9, and that implementing further changes across a large fleet of low impact BES Cyber Systems may require significant additional time and investments. This implementation plan ensures that entities will have at least three years from the effective date of Reliability Standard CIP-003-9 to implement the additional controls contemplated by CIP-003-11, regardless of the date proposed Reliability Standard CIP-003-11 is approved.

The CIP-003-11 changes were made to the NERC Board of Trustees approved version of CIP-003, CIP-003-10 (Virtualization Revisions), which has been filed with the applicable governmental authorities. The use of certain defined terms within CIP-003-11 requires that the definitions for Cyber Systems, Shared Cyber Infrastructure, and Virtual Cyber Asset be approved either concurrently with or before CIP-003-11.

General Considerations

This implementation plan applies only to the CIP-003-11 revisions to the Reliability Standard that have been made by the Project 2023-04 drafting team. The implementation plan does not modify the implementation plan(s) for any other version of CIP-003.

This implementation plan provides entities with thirty-six (36) months to become compliant with the revised Reliability Standard CIP-003-11. This implementation plan reflects the following considerations for entities to implement the new controls of Requirement R2, Attachment 1:

- Revise cyber security policy, plan, and procedures.
- Hire and train new staff to implement the new cyber security controls.
- Reconfigure system, network, or security architectures.
- Purchase, procure, and install new technologies.
- The effective date of CIP-003-9 is April 1, 2026.
- The requested effective date of CIP-003-10 is the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority.

Effective Date

Reliability Standard CIP-003-11

Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Periodic requirements contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and Responsible Entities shall comply initially with those periodic requirements in CIP-003-11 as follows:

Responsible Entities shall initially comply with Requirement R1, Part 1.2.3 on or before the effective date of CIP-003-11. Responsible Entities shall initially comply with all other periodic requirements in CIP-003-11 within the periodic timeframes of their last performance under the version of the CIP-003 Reliability Standard then in effect.

Compliance Date for Requirement R2, Attachment 1 Section 3.1.2

Entities shall not be required to comply with Requirement R2 as it relates to the implementation of documented cyber security plan(s) addressing Attachment 1 Section 3.1.2[2] until the later of: (1) April 1, 2029; or (2) the effective date of Reliability Standard CIP-003-11.

[2] Attachment 1 Section 3.1.2: "Detect known or suspected malicious communications for both inbound and outbound electronic access."

Retirement Date

Reliability Standard CIP-003

Reliability Standard CIP-003-10, or the version of Reliability Standard CIP-003 then in effect, shall be retired immediately prior to the effective date of CIP-003-11 in the jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard
CIP-003-11 – Low Impact BES Cyber Security Criteria Revisions

Introduction
This document is the technical rationale and justification for Reliability Standard CIP-003-11 and includes the rationale for changes in the current proposed version, as well as previous versions of the standard.

It is intended to provide stakeholders and the ERO Enterprise with an understanding of the revisions, technology, and technical concepts of Reliability Standard CIP-003-11. This is not a Reliability Standard and should not be considered mandatory and enforceable.

Background
In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact Bulk Electric System (BES) Cyber Assets. Specifically, this includes the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts, representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber-attack on low impact BES Cyber Systems (LIBCS). In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommended actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the Standard Authorization Request (SAR) at its March 22, 2023 meeting.

The LICRT conclusions regarding LIBCS are as follows:

- Individually, LIBCS are truly low impact to BES reliability. This corresponds to the longstanding work of NERC and the stakeholders to design and operate the BES to withstand the loss of any of its individual assets. A medium or high impact BES Cyber System is more than an impact to a typical single BES Element/Facility. Therefore, the LICRT does not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems.
- LIBCS may introduce BES reliability risks of a higher impact where distributed LIBCS are used for a coordinated attack. The LICRT recommends enhancing the existing low impact category to further mitigate the coordinated attack risk.

The LICRT report recommendations are as follows:

- Requirement(s) for authentication of remote users before granting and subsequently gaining electronic access to networks containing LIBCS at assets containing those systems that have external routable connectivity.

- Requirement(s) for protection of user authentication information in transit for remote electronic access to LIBCS at assets containing those systems that have external routable connectivity.
- Requirement(s) for detection of malicious communications to/between assets containing LIBCS with external routable connectivity.

Rationale for Attachment 1, Section 3 and Section 6

The drafting team's (DT) review of the SAR and industry comment initiated a discussion about the placement of requirements within CIP-003-11. Attachment 1, Section 3 and Attachment 1, Section 6 were identified as ideal locations to integrate the requirements due to their focus on electronic access controls and vendor electronic remote access security controls. The DT investigated two options:

Option A: Modify Sections 3 and 6, integrating the requirements, but keeping the sections separate.
Option B: Merge Sections 3 and 6.

The DT agreed to Option B: Merge Sections 3 and 6. Merging Section 3 and Section 6 would present a single section for all electronic access with sub-sections providing additional requirements based on the type of access (vendor, dial-up, local, etc.). This allows entities to look in one place for all of the electronic access control requirements needed for their assets containing low impact systems, rather than having very similar, and in some cases, overlapping requirements in multiple places within the standard.

While merging Section 3 and 6, the DT made conforming changes to the language. The DT uses the phrase "implement controls" to replace "implement a process" or "implement one or more method(s)". The DT believes a "control" can include an operation, process, procedure, or technology as described in the examples of Attachment 2. Additionally, the word "remote" was removed from the phrase "electronic remote access" as the section now covers all electronic access as described in Section 3, Part 3.1, (i), (ii), and (iii) as those define more specifically the remote nature of the in-scope access.

To clarify scope of requirements for industry and regulators alike, the DT placed the requirements in Attachment 1 Section 3.1 into a logical "if, then" order to further clarify the three identifying low impact asset characteristics or conditions (romanettes i, ii, iii) when implementing controls.

Section 3.1

The objective of the modifications within Section 3.1 is to maintain the original language used in CIP-003-10, Section 3.1, Subsections (i) - (iii). There is one revision to 3.1(iii) replacing the previous language concerning "intelligent electronic devices" with reference to the existing glossary term "Protection Systems" which is a conforming change to the change made by Project 2016-02, CIP-003-10. Figure 1 provides a graphical representation of Section 3.1, Subsections (i)-(iii).

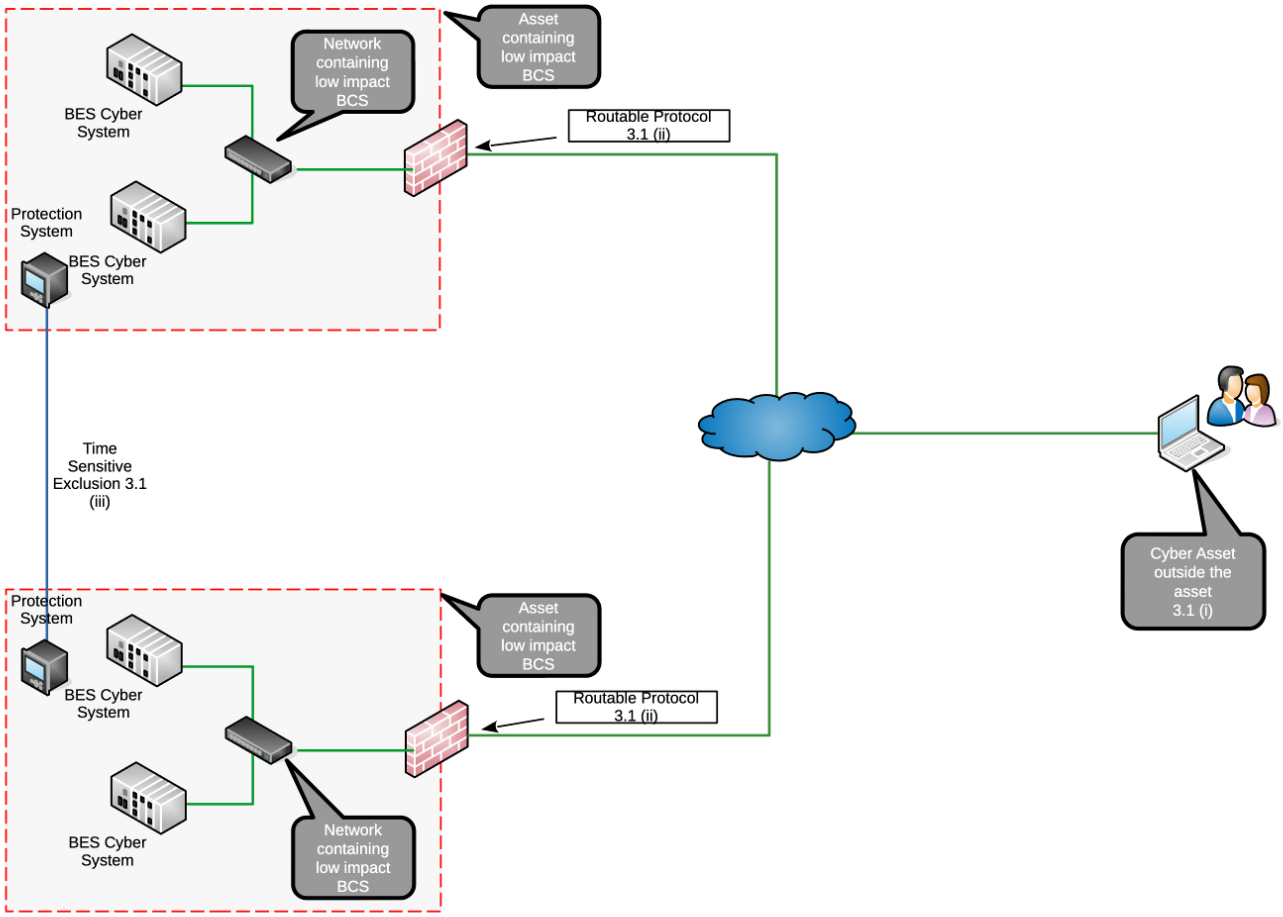


Figure 1

Section 3.1.1

The objective of Section 3.1.1 is to maintain the original language used in CIP-003-10, Section 3.1.

Section 3.1.2

This is an expanded cyber security control outlined in the SAR. The scope is expanded from CIP-003-10, Section 6.3 to include all communications rather than vendor specific communications. The objective of the modifications within Attachment 1 Section 3.1.2 is for entities to mitigate the risk posed by malicious communications to or from LIBCS. The detection of known or suspected malicious communications can be accomplished in several ways. For example, Figure 2 below depicts implementing the control (e.g., Intrusion Detection System (IDS)) in a centralized location (e.g., at a corporate hub site) rather than at every distributed "asset containing LIBCS" such as substations in this example "hub and spoke" model. The obligation in Section 3.1.2 requires that entities implement controls to detect known or suspected inbound and outbound malicious communications between a low impact BES Cyber System and a Cyber

Asset(s) outside the asset containing low impact BES Cyber System(s) thus allowing entity flexibility in where the control is implemented based on their architecture.

The DT considered entities that may use encryption to protect communications between hosts and the impact to the ability to detect known or suspected malicious communications. Because of the differences in entity programs, architectures, technologies and processes, the DT did not prescribe that encrypted communications must be decrypted for deep packet inspection when detecting known or suspected malicious communication. Requiring decryption/inspection/re-encryption may in some cases increase risk through introducing single points of failure or jeopardizing sensitive timing of communications. Entities may detect known or suspected malicious communications through other methods, such as detecting the appearance of abnormal new destination addresses or ports. The DT provided several other examples in Attachment 2. Entities may also choose to perform detection before or after the encryption tunnel occurs.

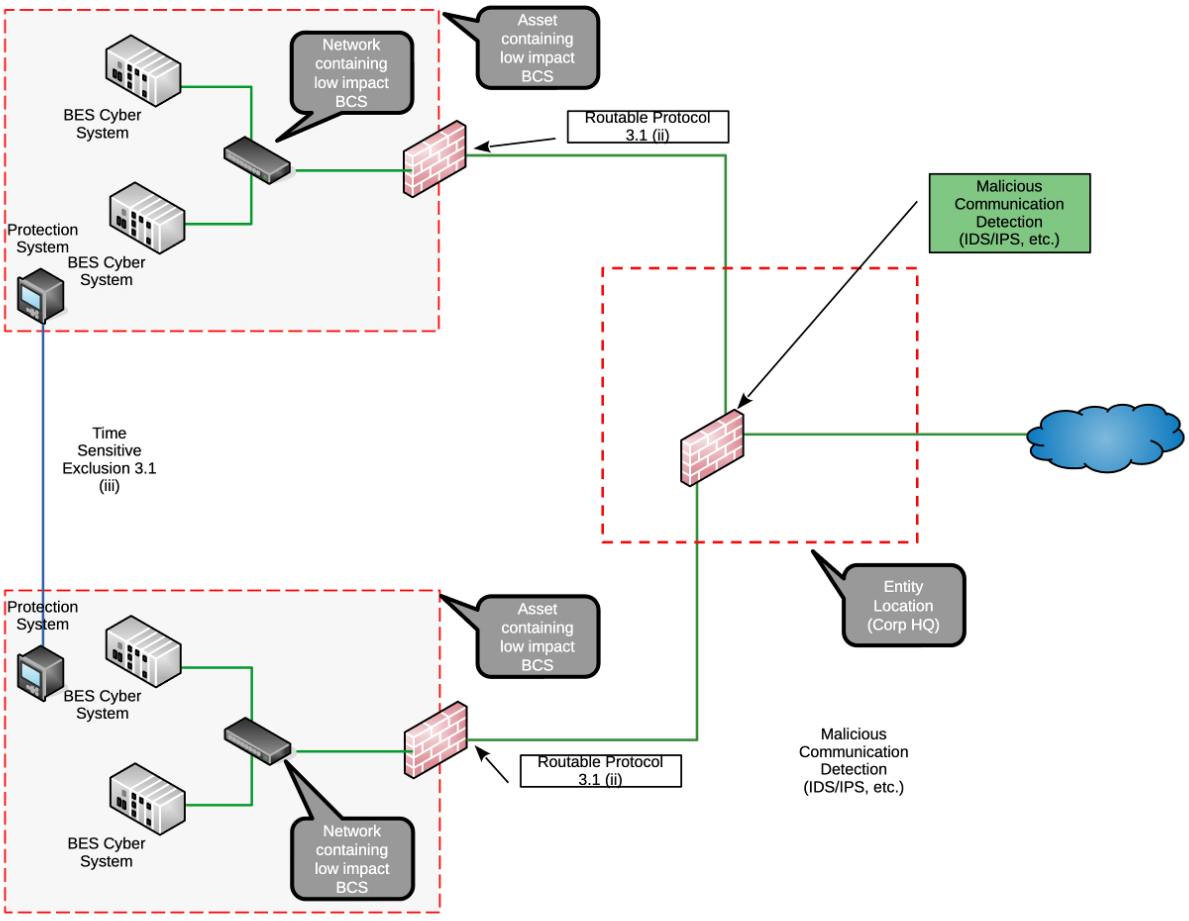


Figure 2

Section 3.1.3

This is a new cyber security control outlined in the SAR that requires entities to implement controls to authenticate users prior to permitting access to networks containing LIBCS. This control mitigates the risk of unauthenticated access to networks on which LIBCS reside. The intent is for each user to be authenticated (verifying a user) *before* they gain access to the "network containing low impact BES Cyber Systems"; thus, they have no ability to enumerate hosts on those networks, scan those networks for vulnerabilities, attempt logons to systems, or perform actions on those networks and systems before the entity has authenticated their user-initiated electronic access. It is important to note that Section 3.1.3 is not applicable to electronic access which sources (is connected) to the LIBCS network. For example, a laptop connected via an Ethernet cable to the LIBCS network would not be required to authenticate prior to accessing the LIBCS to which it is being connected. It is also important to note that the DT did not address specific account types (user or shared) used for authentication. While the intent is for entities to control each user prior to permitting electronic access, the SAR did not prescribe account types or passwords used by users to obtain (via authentication) electronic access. There are multiple methods to authenticate users for the responsible entity to choose.

Figure 3, below, depicts a situation where the authentication of the remote user is not occurring "prior to" but after the user already has access to the "network containing LIBCS" — as the authentication servers are on the same network with the LIBCS. The firewall in this scenario allows the user through to the network on which the LIBCS reside before the user is authenticated, and this does not meet the intent of the requirement.

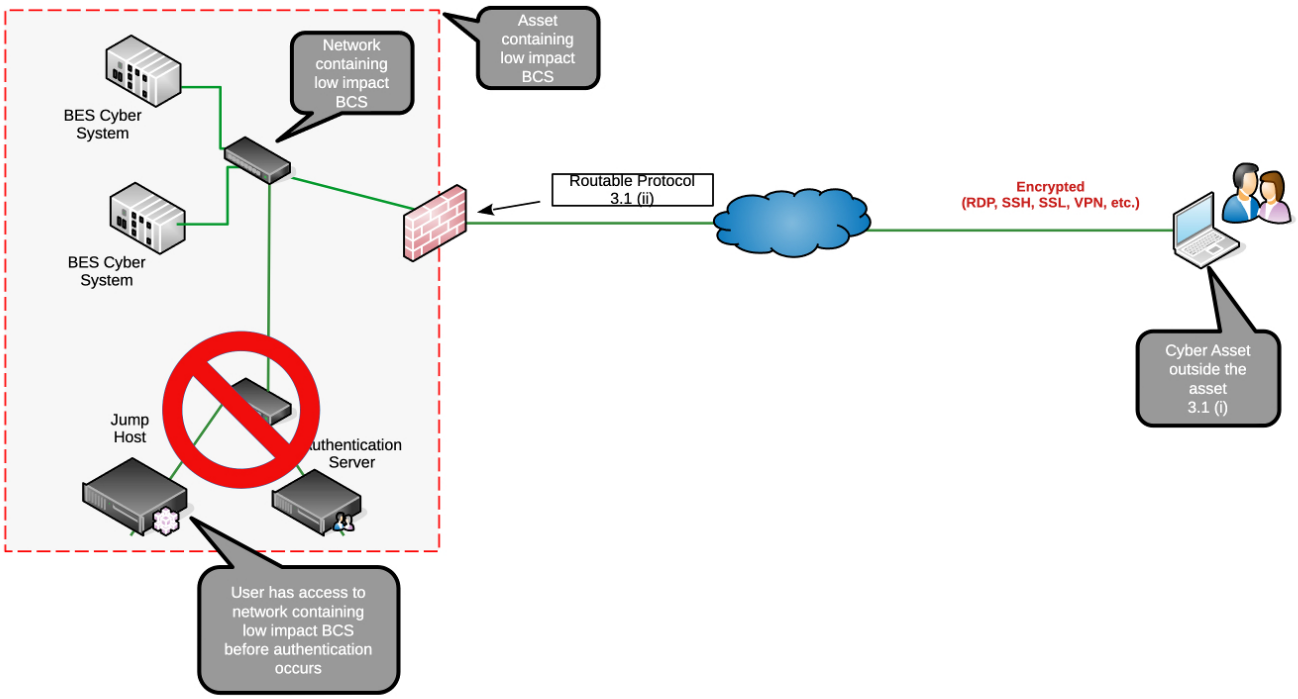


Figure 3

The intention of the phrase “each user prior to permitting access to a network(s)…” is meant to include the initial authentication and not all subsequent access to other downstream networks. If there is a collection of sub-networks or Cyber Assets within the network containing LIBCS, then multiple re-authentications at those levels would not be required by this specific requirement. Regardless of how many subsequent networks or BES Cyber Systems a user may access, as long as the entity’s implemented control(s) have authenticated the user prior to their access to those subsequent networks, that meets the intent. This may include, but is not limited to, configurations where authentication is local device specific authentication or configurations consisting of centralized authentication using technologies such as an access, terminal, or proxy server (“Intermediate System”) which processes authentication to the low impact asset networks through a centralized gateway.

The DT has not required the use of an “Intermediate System” as is prescribed in CIP-005 Requirement R2 for high and medium impact BES Cyber Systems. However, the DT’s intent is that those entities who have established or implemented such infrastructure or technologies may use them for authenticating access

to the assets containing low impact BES Cyber Systems to satisfy these requirements. While prescribing such an architecture as in CIP-005 Requirement R2 would further clarify CIP-003's requirements, the DT has chosen not to prescribe such requirements due to the impact to a broad and diverse range of entities and their specific technologies and processes used to meet low impact BES Cyber Systems authentication requirements. For example, it would be excessive to require an entity with a single CIP-003 applicable renewable generation site to implement architectures and technologies (Intermediate Systems) to meet the CIP-005 Requirement R2 Interactive Remote Access requirements. Such an entity may only need a Secure Sockets Layer (SSL) Virtual Private Network (VPN) to an access control device (e.g., firewall) at the one site that authenticates the user prior to allowing access to the network containing low impact BES Cyber Systems on its inside interface. The entity may also choose to authenticate a local non-low impact BES Cyber Systems network first, then control access to the LIBCS from that access point. Conversely, an entity with many assets distributed over a large geographic area, with a variety of impact categorizations and supporting BES Cyber Systems, may want to use their existing CIP-005 Requirement R2 remote access solutions for all of their sites (centralized access controls). The DT's intent in the CIP-003 language is to allow flexibility for both cases.

The phrase, "through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted" is included in Section 3.1.3 to clarify scoping. As Section 3.1.3 is written at a different granularity of "network(s) containing", which is not mentioned in the romanettes, this phrasing simply clarifies that the intended scope remains those networks through which the specific access described in the Section 3.1 romanettes is subsequently permitted. The romanettes (i), (ii), and (iii) in Section 3.1 define the ultimate access that is in scope, which is from a remote client outside the asset containing the LIBCS and destined for a LIBCS within the asset.

Section 3.1.4

This is a new cyber security control outlined in the SAR. The objective of Attachment 1, Section 3.1.4 is for entities to protect the user authentication information (e.g., username, password, multi-factor authentication (MFA) information, session token, etc.) while in transit between the remote user's Cyber Asset and either the asset containing the low impact BES Cyber Systems or the entity's authentication system used to meet Section 3.1.3. This mitigates the risk of user authentication information being captured, especially as some BES equipment may still require protocols that transmit such information in clear text. The intent is not to specify authentication directly to a particular device but to allow entities that desire to use an existing compliant CIP-005 Requirement R2 Intermediate System, or similar architecture, access to networks containing LIBCS (Figure 4). For example, Figure 4 below depicts protection of the user authentication information to the asset containing a LIBCS.

Figure 5 depicts an alternative example of protecting the user authentication information to/from a central system (i.e. jump host) *before* accessing a network containing a LIBCS. This protection mitigates the unintended disclosure of authentication information for electronic access to low impact cyber systems.

Note that both Figure 4 and Figure 5 have a significant difference from Figure 3 above in that, although the authentication services are also within the asset containing the LIBCS, they are located on a separate network from those containing BES Cyber Systems. In this example, assuming the firewall is configured to only allow authenticated user sessions on the jump host through to the network containing the LIBCS, this would meet the intent of the Section 3.1.3.

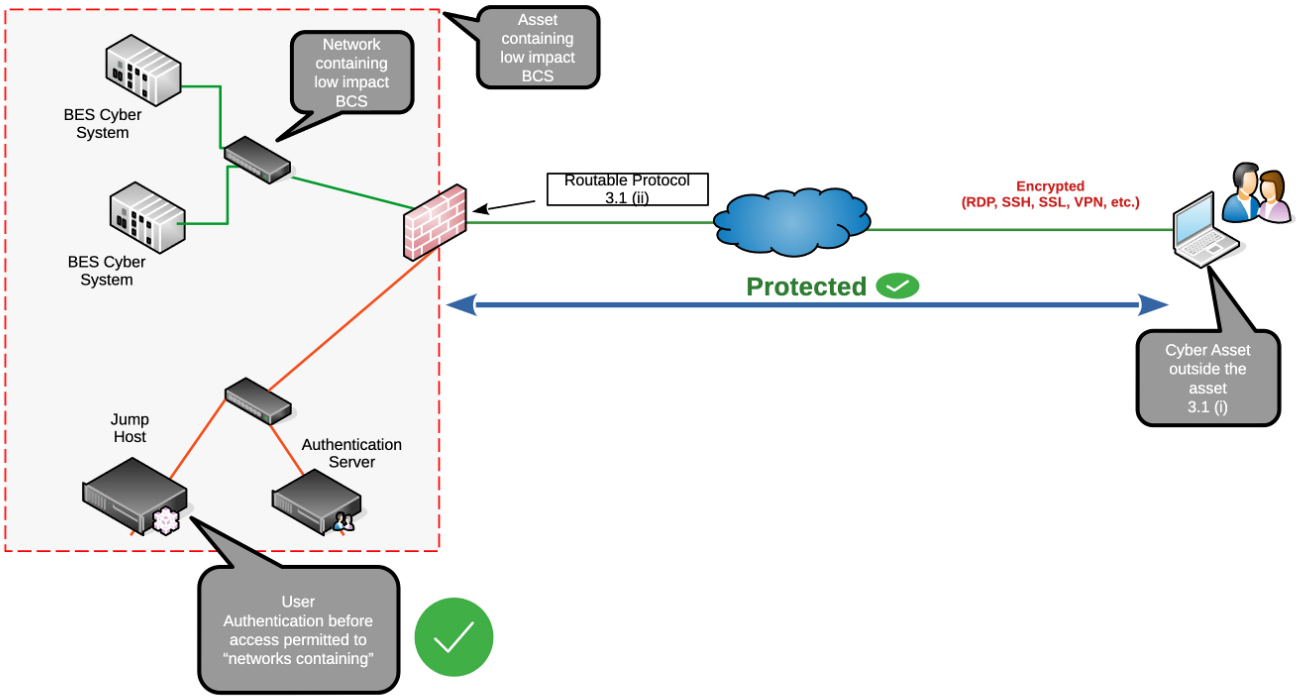


Figure 4

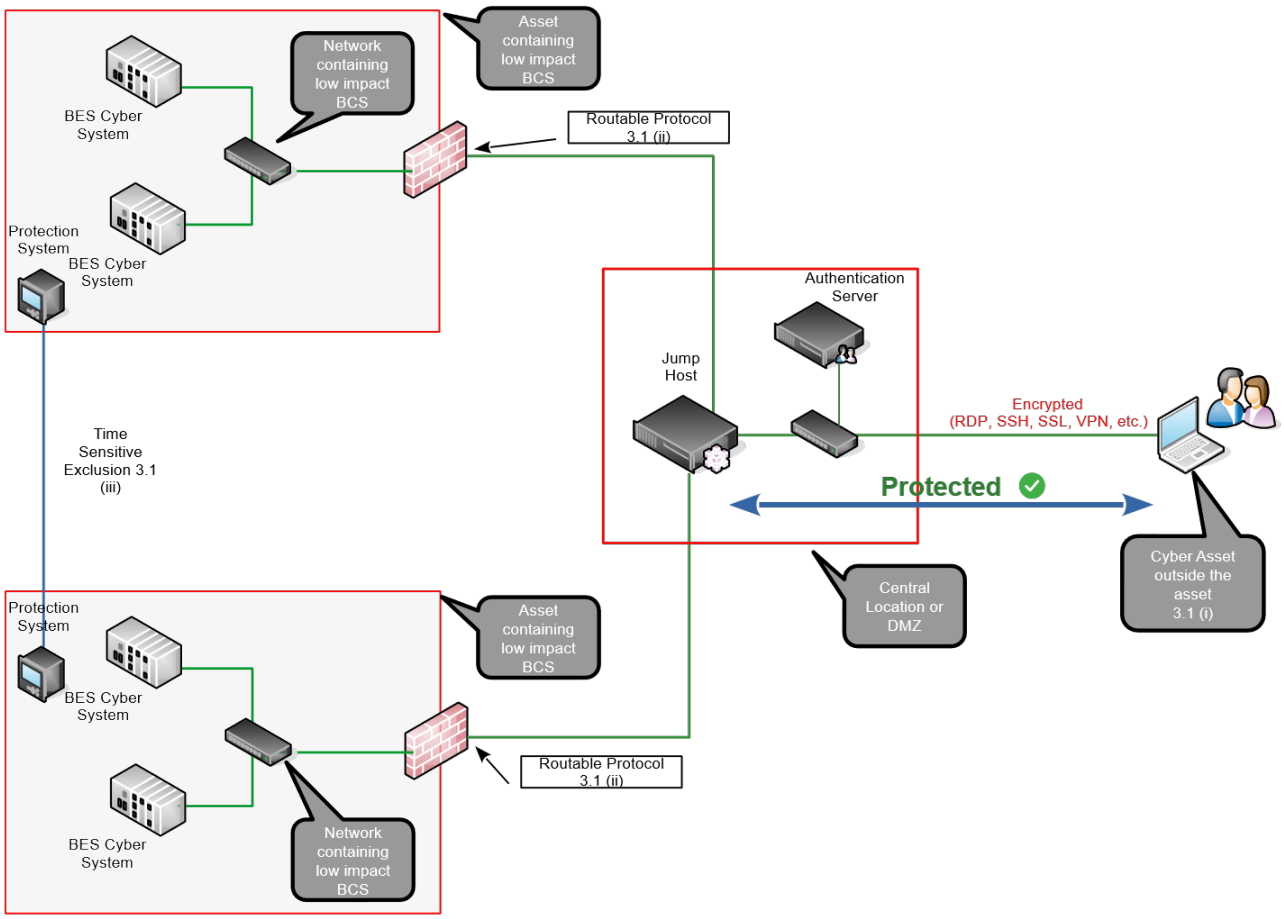


Figure 5

The DT has not required the use of an "Intermediate System" as is prescribed in CIP-005 Requirement R2 for high and medium impact BES Cyber Systems. However, the DT's intent is that those who have such infrastructures in place can, if they choose, use them for access to the assets containing low impact BES Cyber Systems to satisfy the intent of these requirements. While prescribing such an architecture as in CIP-005 Requirement R2 would make the target of CIP-003's requirements clearer to describe, the DT has chosen not to be this prescriptive due to the wide diversity of entities that may have only LIBCS. For example, an entity may have one small renewable generation site that falls under CIP-003 and implementing a full CIP-005 Requirement R2 "Interactive Remote Access with Intermediate System" architecture for access to one site may be excessive. That entity may only need an SSL VPN to an access control device (e.g., firewall) at the one site that authenticates the user and then allows access to the network containing LIBCS on its inside interface. However, an entity with 100 assets with BES Cyber Systems of varying impact categorization over a large geographic area may want to use their CIP-005 Requirement R2 remote access solution for all of their sites. The DT's intent in the CIP-003 language is to allow flexibility for both.

Section 3.1.5

The objective of Section 3.1.5 is to maintain the original language used in CIP-003-10, Section 6.1. One or more method(s) can be identified as part of this electronic access control. Entities must determine vendor electronic remote access, where permitted, to their LIBCS. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access.

Section 3.1.6

The objective of Section 3.1.6 is to maintain the original language used in CIP-003-10, Section 6.2. One or more method(s) can be identified as part of this electronic access control. Entities must have the ability to disable vendor electronic remote access, where permitted, for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing LIBCS.

Section 3.2

The DT made conforming changes to Section 3.2 with the objective to maintain the original intent of CIP-003-10, Section 3.2.

Special Scenarios

One low impact BES Cyber System across more than one asset containing that system.
In this scenario, a low impact BES Cyber System is not entirely located within one asset. For example, a generation resource has the majority of its BES Cyber System components within the site, but its network is extended full-time (e.g., over a dedicated circuit or dedicated VPN) to an operator console located at another site, and the console is part of the single BES Cyber System.

Since the components of the BES Cyber System are all located in "assets containing low impact BES Cyber System", just not a single asset, then this scenario is not in scope as it does not meet the condition of Section 3.1(i) of "between a low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber System(s)." The intent of Section 3.1.3 is authentication of users who are not located within any other "assets containing low impact BES Cyber System." This keeps CIP-003 analogous to the same concept in CIP-005 and the Interactive Remote Access definition that excludes from Interactive Remote Access user access that originates in another of the entity's Electronic Security Perimeters, such that operators in Control Centers are not required to implement CIP-005 Requirement R2 controls such as Intermediate Systems to operate field assets. It also avoids CIP-003 becoming circular when a local user at the BES Cyber System console would need to authenticate prior to permitting access to the extended network they are already on while seated at the console.

Rationale for Attachment 2

The DT made conforming changes to Attachment 2 merging Sections 3 and 6 and provided examples of compliance related activities.

Previous CIP-003 Versions Technical Rationale

Project 2020-03 Supply Chain Low Impact Revisions (CIP-003-9) Technical Rationale
Project 2016-02 Modifications to CIP Standards (CIP-003-10) Technical Rationale

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2023-04 Modifications to CIP-003

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2023-04 Modifications to CIP-003. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

Justification for VRFs and VSLs

- Requirement R1: There were no changes to VRFs from the previously FERC-approved CIP-003-9 Reliability Standard and only conforming or non-substantive changes to the VSLs.
- Requirement R2: The VRF did not change from the previously FERC-approved CIP-003-9 Reliability Standard. VSL changes are outlined below.
- Requirement R3: There were no changes to VRFs from the previously FERC-approved CIP-003-9 Reliability Standard and only conforming or non-substantive changes to the VSLs.
- Requirement R4: There were no changes to VRFs from the previously FERC-approved CIP-003-9 Reliability Standard and only conforming or non-substantive changes to the VSLs.

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document the electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2)	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security controls according to Requirement R2, Attachment 1,	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to implement three or more controls listed in Requirement R2, Attachment 1, Section 2. (Requirement R2)	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	Section 2. (Requirement R2) OR The Responsible Entity failed to implement one or two controls listed in Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code	OR The Responsible Entity failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code	

R #	Violation Severity Levels (CIP-003-A, Requirement R2)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

VSL Justifications for CIP-003-A, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSLs for Requirement R2 are similar to the previous VSLs of CIP-003-9, with a few revisions. Created Moderate and High VSL based on the number of controls implemented. Removed mentions of Attachment 1, Section 6, since Section 6 was merged with Section 3.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Requirement R2 is not a "binary" type requirement. Violation severity levels are clear, quantitative, and non-ambiguous.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The VSL level assignments are consistent with language in Requirement R2 and Attachment 1.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The violation severity levels relate to a single violation. A failure to do multiple portions of Requirement R2, Attachment 1 is considered a single violation.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-003-11 – Cyber Security — Security Management Controls

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	*	X	X		X			X	X		
R2	X	*	X	X		X			X	X		
R3	X	*	X	X		X			X	X		
R4	X	*	X	X		X			X	X		

* CIP-003-11 is only applicable to DPs that own certain UFLS, UVLS, RAS, Protection Systems, or Cranking Paths. See CIP-003-11 Section 4, Applicability, for details.

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request additional evidence from the registered entity that is not included in this RSAW. This RSAW may include excerpts from FERC Orders and other regulatory references which are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			
R3			
R4			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1.** For its high impact and medium impact (BCS), if any:
  - **1.1.1.** Personnel and training (CIP-004);
  - **1.1.2.** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
  - **1.1.3.** Physical security of BCS (CIP-006);
  - **1.1.4.** System security management (CIP-007);
  - **1.1.5.** Incident reporting and response planning (CIP-008);
  - **1.1.6.** Recovery plans for BCS (CIP-009);
  - **1.1.7.** Configuration change management and vulnerability assessments (CIP-010);
  - **1.1.8.** Information protection (CIP-011); and
  - **1.1.9.** Declaring and responding to CIP Exceptional Circumstances.
- **1.2.** For its assets identified in CIP-002 containing low impact BCS, if any:
  - **1.2.1.** Cyber security awareness;
  - **1.2.2.** Physical security controls;
  - **1.2.3.** Electronic access controls;
  - **1.2.4.** Cyber Security Incident response;
  - **1.2.5.** Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and
  - **1.2.6.** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-003-11, R1

This section to be completed by the Compliance Enforcement Authority

	For its high impact and medium impact BCS, if any, verify the Responsible Entity has documented one or more cyber security policies that collectively address the following topics: 1. Personnel and training (CIP-004); 2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access; 3. Physical security of BCS (CIP-006); 4. System security management (CIP-007); 5. Incident reporting and response planning (CIP-008); 6. Recovery plans for BCS (CIP-009); 7. Configuration change management and vulnerability assessments (CIP-010); 8. Information protection (CIP-011); and 9. Declaring and responding to CIP Exceptional Circumstances.
	For its assets identified in CIP-002 containing low impact BCS, if any, verify the Responsible Entity has documented one or more cyber security policies that collectively address the following topics: 1. Cyber security awareness; 2. Physical security controls; 3. Electronic access controls; 4. Cyber Security Incident response; 5. TCA and Removable Media malicious code risk mitigation; and 6. Declaring and responding to CIP Exceptional Circumstances.
	Verify each policy used to meet this Requirement has been reviewed at least once every 15 calendar months.
	Verify the CIP Senior Manager has approved each policy used to meet this Requirement at least once every 15 calendar months.
	Verify the Responsible Entity has achieved the security objective of instituting cyber security policies that will preserve the availability, integrity, and confidentiality of systems that support the reliable operation of the BES.
Note to Auditor: Per Attachment 1, "Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets."	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-003-11, R2

This section to be completed by the Compliance Enforcement Authority

	Attachment 1, Section 1 For each asset containing a low impact BCS, verify that the Responsible Entity has documented a plan to reinforce cyber security practices (which may include associated physical security practices) at least once every 15 calendar months.
	Attachment 1, Section 1 For each asset containing a low impact BCS, verify that the Responsible Entity has implemented its plan to reinforce cyber security practices (which may include associated physical security practices) at least once every 15 calendar months.
	Attachment 1, Section 1 For each asset containing a low impact BCS, verify that the Responsible Entity has achieved the security objective of ensuring personnel with access to low impact BCS remain aware of cyber security practices.
	Attachment 1, Section 2 For each asset containing a low impact BCS, verify that the Responsible Entity has documented a plan to control physical access, based on need as determined by the Responsible Entity, to: 1. The asset or the locations of the low impact BCS within the asset; and 2. The Cyber Asset(s) or Virtual Cyber Asset (VCA), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1.1, if any.
	Attachment 1, Section 2 For each asset containing a low impact BCS, verify that the Responsible Entity has implemented its plan to control physical access.
	Attachment 1, Section 2 For each asset containing a low impact BCS, verify that the Responsible Entity has achieved the security objective of controlling physical access to: 1. The asset or the locations of the low impact BCS within the asset; and 2. The Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.
	Attachment 1, Section 3.1 For each asset containing a low impact BCS and for SCI that supports a low impact BCS, if any, verify that the Responsible Entity has documented a plan to control electronic access as outlined below: i. Between: • a low impact BCS; or • an SCI that supports a low impact BCS; and a Cyber System(s) outside the asset containing: • the low impact BCS(s); or • the SCI that supports a low impact BCS. ii. Using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

	iii. Not used for time-sensitive communications of Protection Systems.
	Attachment 1, Section 3.1 For each asset containing a low impact BCS, and for SCI that supports a low impact BCS, if any, verify that the Responsible Entity has implemented one or more controls, where Section 3.1 Parts (i), (ii), and (iii) are met that: 3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity; 3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic access; 3.1.3 Authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS, through which user-initiated electronic access appliable to Section 3.1 is subsequently permitted; 3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System(s) outside the asset containing low impact BCS or SCI that supports a low impact BCS and • the authentication system used to meet Section 3.1.3, or • the asset containing low impact BCS or SCI that supports a low impact BCS; 3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and 3.1.6 Include one or more methods for disabling vendor electronic access where vendor electronic access is permitted.
	Attachment 1, Section 3.1 For each asset containing a low impact BCS, and for SCI that supports a low impact BCS, if any, verify that the Responsible Entity has achieved the security objective of implementing one or more controls for Section 3.1, where Section 3.1. Parts (i), (ii), and (iii) are met.
	Attachment 1, Section 3.2 For each asset containing a low impact BCS and for SCI that supports a low impact BCS, if any, verify that the Responsible Entity has documented a plan to authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.
	Attachment 1, Section 3.2 For each asset containing a low impact BCS and for SCI that supports a low impact BCS, if any, verify that the Responsible Entity has implemented the plan to authenticate Dial-up Connectivity.
	Attachment 1, Section 3.2 For each asset containing a low impact BCS and for SCI that supports a low impact BCS, if any, verify that the Responsible Entity has achieved the security objective of authenticating all Dial-up Connectivity, per system capability, where such connectivity permits access to its low impact BCS or SCI that supports a low impact BCS.
	Attachment 1, Section 4 For each asset containing a low impact BCS, verify that the Responsible Entity has

	documented one or more Cyber Security Incident response plan(s) that include: 1. Identification, classification, and response to Cyber Security Incidents; 2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law; 3. Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals; 4. Incident handling for Cyber Security Incidents; 5. Testing each Cyber Security Incident response plan at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and 6. Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.
	Attachment 1, Section 4 For each asset containing a low impact BCS, if the Responsible Entity responded to a Cyber Security Incident, verify the Responsible Entity implemented the Cyber Security Incident response plan.
	Attachment 1, Section 4.5 Verify the Responsible Entity tested each Cyber Security Incident response plan at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident.
	Attachment 1, Section 4.6 Verify the Responsible Entity updated each Cyber Security Incident response plan, if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.
	Attachment 1, Section 4 Verify the Responsible Entity is prepared to achieve the security objective of minimizing the adverse impact to the BES of a possible Cyber Security Incident affecting low impact BCS.
	Attachment 1, Section 5.1, 5.2, 5.2.1 Verify the Responsible Entity has documented one or more plans to mitigate the risk of the introduction of malicious code to low impact BCS through the use of TCA.
	Attachment 1, Section 5.1, 5.2, 5.2.1 Verify the Responsible Entity has implemented its plans to mitigate the risk of the introduction of malicious code to low impact BCS through the use of TCA.
	Attachment 1, Section 5.1, 5.2, 5.2.1 Verify the Responsible Entity has achieved the objective of mitigating the risk of the introduction of malicious code to low impact BCS through the use of

	TCA.
	Attachment 1, Section 5.2.2 For any method used pursuant to 5.2.1, verify the Responsible Entity has determined whether any additional mitigation actions are necessary and has implemented such actions prior to connecting the TCA.
	Attachment 1, Section 5.3.1 Verify the Responsible Entity has documented one or more plans to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS.
	Attachment 1, Section 5.3.2 Verify the Responsible Entity has documented one or more plans to mitigate the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.
	Attachment 1, Section 5.3 Verify the Responsible Entity has implemented its plans to mitigate the risk of the introduction of malicious code to low impact BCS or SCI that supports a low impact BCS through the use of Removable Media.
	Attachment 1, Section 5.3 Verify the Responsible Entity has achieved the objective of mitigating the risk of the introduction of malicious code to low impact BCS or SCI that supports a low impact BCS through the use of Removable Media.

Note to Auditor:

Attachment 1, Section 3

1. For each asset identified as containing a low impact BCS per CIP-002, the list of assets should identify those assets that have routable protocol communications between low impact BCS; or an SCI that supports a low impact BCS and a Cyber System(s) outside the asset containing: the low impact BCS(s); or the SCI that supports a low impact BCS when entering or leaving the asset and not used for time-sensitive protection or time-sensitive control functions.
    a. For these identified assets, obtain as evidence the devices used to control electronic access and the low impact BCS for which they control access.
2. For each asset identified as containing a low impact BCS per CIP-002, the Responsible Entity has an obligation to determine the necessary inbound and outbound routable protocol communications between low impact BCS and SCI that supports a low impact BCS outside the asset containing: the low impact BCS when entering or leaving the asset and not used for time-sensitive protection or time-sensitive control functions. The Responsible Entity must be able to provide a technically sound explanation as to how its electronic access permissions and controls are consistent with the security objective of permitting only necessary inbound and outbound access to low impact BCS.
3. The audit team should assess the effectiveness of the Responsible Entity's electronic

access control plan as well as the Responsible Entity's adherence to its electronic access control plan.

4. For the inbound and outbound communications that the Responsible Entity has determined to be necessary, the Responsible Entity must identify the electronic access controls used to effectively control access to and from the low impact BCS.

Attachment 1, Section 5

1. The means of verifying the mitigation of the introduction of malicious code to a low impact BCS differs depending on whether a TCA is managed by the Responsible Entity in an ongoing or an on-demand manner. The verification for a TCA managed in an ongoing manner focuses on the process of preventing malware from being introduced to the TCA. The verification for a TCA managed in an on-demand manner focuses on the process used to ensure the TCA may be safely used in a low impact BCS environment prior to such use. If the TCA is managed in both an ongoing and an on-demand manner, then both verification techniques should be employed.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high-level official designating the name of the individual identified as the CIP Senior Manager.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-003-11, R3

This section to be completed by the Compliance Enforcement Authority

	Verify the CIP Senior Manager has been identified by name.
	Verify that any changes made to the CIP Senior Manager were dated and documented within 30 calendar days of the change.
	Verify the CIP Senior Manager is a single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-015.

Auditor Notes:

R4 Supporting Evidence and Documentation

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-003-11, R4

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented a process to delegate authority, unless no delegations are used.
	Verify that all delegates have been identified by name or title.
	Verify that the delegation of authority includes the specific action delegated.
	Verify specific actions delegated by the CIP Senior Manager are allowed by the CIP Standards.
	Verify that the dates for all delegations have been recorded.
	Verify that the CIP Senior Manager approved all delegations.

	Verify that any changes made to delegations were dated and documented within 30 days of the change.
Note to Auditor: Delegations of the CIP Senior Manager's authority are permitted for the required approvals in CIP-002-7, Requirement R2, CIP-007-7, Requirement R2, Part 2.4, and CIP-013-3 R3.	

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-003-11 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Standards”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 822

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS including any supporting SCI to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need, as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or Virtual Cyber Asset (VCA), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, where electronic access is:

i. Between:

- a low impact BCS; or
- an SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:

- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems;

the Responsible Entity shall implement one or more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for both inbound and outbound electronic access;

3.1.3 Authenticate each user prior to permitting access to a network(s) containing

low impact BCS or SCI that supports a low impact BCS, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted;

3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System(s) outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BCS or SCI that supports a low impact BCS;

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, the Responsible Entity shall implement one or more control(s) that authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. For Section 3.1.1, documentation showing the permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, such as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BCS or SCI that supports a low impact BCS and a Cyber System outside the asset containing low impact BCS.
   - Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways); or
   - Original equipment manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.
2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Anti-malware technologies;
   - Intrusion detection system (IDS)/intrusion prevention system (IPS);
   - Monitor or alert for changes to communication baselines;
   - Logging and alerting configuration for security incident and event management (SIEM) systems or other event correlation systems;

- Automated or manual log reviews;
- Alerting; or
- Other operational, procedural, or technical controls.

3. For Section 3.1.3, documentation showing the ability to authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted, such as:
   - Authentication mechanism(s) including but not limited to:
     - Utilization of public key infrastructure (PKI), lightweight directory access protocol (LDAP), remote authentication dial-in user service (RADIUS), and/or similar implemented solutions; or
     - Enforcement of multi-factor authentication (MFA).
   - Virtual private network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
   - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BCS; or
   - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System outside the asset containing low impact BCS or SCI that supports a low impact BCS and
   - The authentication system used to meet Section 3.1.3, or
   - The asset containing low impact BCS or SCI that supports a low impact BCS,

   such as protection mechanism(s) including, but not limited to:
   - Implementation of an encrypted protocol or service (hypertext transfer protocol secure (HTTPS), secure shell (SSH), etc.);
   - Implementation of an IPsec or secure sockets layer (SSL) VPN; or
   - Other operational, procedural, or technical controls.
5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;

- Security information management logging alerts;
- Time-of-need session initiation;
- Session recording;
- System logs; or
- Other operational, procedural, or technical controls.

6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Disabling vendor electronic access user or system accounts;
   - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, remote desktop, remote control, or other hardware or software used for providing vendor electronic access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic access; or
   - Other operational, procedural, or technical controls.
7. For Section 3.2, documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and

5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

   Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.
3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFT1v0	10/31/2024		Initial Draft

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-04 Modifications to CIP-003

Final Documents Posted

Now Available

The drafting team is posting the final documents of **CIP-003-11 – Cyber Security – Security Management Controls,** but not conducting a final ballot, per the Standard Processes Manual (SPM) section 4.13, which allows the drafting team to conclude the standards action without conducting a final ballot if:

- the previous ballot achieved at least 85% weighted segment approval;
- the drafting team made a good faith effort at resolving applicable objections;
- the drafting team responded in writing to comments as required by section 4.12; and
- the drafting team is proposing no further changes to the balloted documents.

Consistent with these requirements, the last ballot received 93.89% approval. The drafting team has made a good faith effort to resolve objections and responded to comments in writing, including making minor corrections to two of the non-mandatory and enforceable sections of the standard.

Per SPM section 2.5: "The only mandatory and enforceable components of a Reliability Standard are the: (1) applicability, (2) Requirements, and the (3) effective dates. The additional components are included in the Reliability Standard for informational purposes and to provide guidance to Functional Entities concerning how compliance will be assessed by the Compliance Enforcement Authority."

The Ballot Results page provides the detailed voting results from the previous ballot. CIP-003-11 will be presented to the NERC Board at the December Board of Trustees meeting.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Manager, Standards Development, Alison Oswald (via email) or at 404-275-9410.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit G

Standard Drafting Team Roster,
Project 2023-04 Modifications to CIP-003

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Drafting Team Roster

Project 2023-04 Modifications to CIP-003

	Name	Entity
Chair	Tony Hall	LG&E and KU Energy
Vice Chair	Jay Cribb	Southern Company Services
Members	Monica Jain	Southern California Edison
	Clayton Whitacre	Great River Energy
	Barry Jones	Western Area Power Administration
	Robert Montgomery	Duke Energy
	Peggy McDannald	Associated Electric Cooperative, Inc.
	Josef Chesney	Powder River Energy Corp
	Sean Randles	Leeward Renewable Energy, LLC
	Lemon Williams	Pine Gate Renewables
	Jeff Sykes	Utility Services
PMOS Liaison	Kirk Rosener	CPS Energy
NERC Staff	Alison Oswald – Manager of Standards Development	North American Electric Reliability Corporation
	Lauren Perotti – Legal	North American Electric Reliability Corporation
	Sarah Crawford – Legal	North American Electric Reliability Corporation