NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security – Electronic Security Perimeter(s)

Technical Rationale and Justification for Reliability Standard CIP-005-8

April 2024

RELIABILITY | RESILIENCE | SECURITY

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

Table of Contents

Technical Rationale for Reliability Standard CIP-005-8

Introduction

This document is the technical rationale and justification for Reliability Standard CIP-005. It includes the rationale for changes in the current proposed version (CIP-005-8) as well as previous versions of the standard. The intent of this document is to provide stakeholders and the ERO Enterprise with an understanding of the revisions and the technical concepts of the Reliability Standard as well as the rationale for such revisions, both the currently proposed and historical revisions from previous versions and SDTs.

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-8. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-8 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition Advisory Group (V5TAG), which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005-8 and the definitions of Cyber Asset and Electronic Access Point (EAP) that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

Summary

The Project 2016-02 Standard Drafting Team (SDT) proposal accommodates for increasing use of virtualization and other technology innovation. The SDT's purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards, but also to better position the CIP standards to be applicable to additional future technological innovation while, to the extent possible, maintaining backwards compatibility.

CIP-005-8 remains a standard concerned with controlling communications to and from BES Cyber Systems (BCS) by establishing an Electronic Security Perimeter (ESP) with increased security controls for Interactive Remote Access (IRA) and vendor remote access. However, virtualization is enabling models for network security, such as "Zero Trust", that are not network perimeter based. Therefore, in CIP-005-8 the ESP focuses on being a security model rather than a network topology-based perimeter as the only option. Securing the communications to and from BCS is the security objective, but the standard no longer prescribes "where", as in where on a network, the controls must be implemented. Innovations such as Zero Trust models are moving access control from network borders to a session level orientation and eliminating the implicit trust within a local network. Network perimeter-based ESP and EAP implementations remain a valid option and are one method for allowing only necessary communications to the Cyber Systems within the ESP.

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in “CIP Definitions and Exemptions Technical Rationale” document for reference when reading the technical rationale that follows.

Requirement R1 General Considerations

ESP Redefined

For backwards compatibility purposes, network border-based ESPs and EAPs remain a valid option for controlling the communications to and from BCS. However, virtualization technologies and models such as Zero Trust present equally effective methods that are not network border-based solutions. A Zero Trust model can implement more granular controls throughout a network on a per-access or per-session level.

Shared infrastructure and “Mixed Trust” Risks

For virtualized environments where SCI is used, a risk of side channel attacks exists. Virtualization allows disparate workloads of what could be differing impact to execute on the same CPUs and share the same memory (i.e., RAM). In this case the lower impact systems would become high water marked with the higher impact system through the PCA definition. This would in turn affect what requires protection by any associated ESPs. The risks associated with this scenario is mitigated in CIP-005-8 by either:

- Declaring the VCAs that share CPU or memory or are within the same ESP with a BCS as associated PCAs which will require they meet the security requirements (high water marking) that include ‘associated PCAs’; or
- Configuring the virtualization infrastructure to place VCAs of differing impact or trust levels into differing CPU and memory pools and configuring affinity controls to these pools such that hypervisors do not allow workloads in these differing pools to simultaneously exist or execute on the same hypervisor.

Assets with Multiple Classifications (PCA, EACMS, Intermediate System, SCI, etc.)

The definitions created to categorize Cyber Assets have historically included overlap. The definition of PCA was revised to include VCAs that share CPU or memory with a BCS. Additional definitions such as SCI and VCA will add to the possibility of additional instances of assets or systems meeting multiple definitions, such as SCI that are also EACMS.

These definitions are used in both the Applicable Systems column as well as within the requirement language. The fact that one asset or system may meet multiple definitions and therefor have multiple classifications does not pose a significant challenge as long as the Responsible Entity ensures that all requirements that pertain to ANY of the classifications are applied. In other words, if an asset or system meets both the SCI and the EACMS definition, requirements that apply to either categorization are applicable.

Firewall/Router on a Stick

A “firewall on a stick” or “router on a stick” is a reference to a networking design scenario by which a firewall or router has one single physical connection to a switch, but has access to multiple networks and broadcast domains by utilizing logical interfaces in combination with VLANs (Virtual Local Area Networks).

Devices on different VLANs are not able to communicate by default, so the primary purpose of this design is to allow for inter-VLAN routing enabling communication between devices which reside on different VLANs by way of the firewall or router.

As all traffic between these VLANs passes through the firewall or router it is uniquely positioned to restrict access and log traffic flows between devices on different VLANs facilitating compliance and the enforcement of security requirements.

This design allows an entity additional flexibility with respect to the creation of multiple Electronic Security Perimeters while minimizing the cost and number of physical networking devices required to provide proper levels of protection and isolation to each of the created Electronic Security Perimeters.

An entity may select this design to enable further isolation of distinct applications and systems from each other based on the assessed risk that they pose to the BES or to enhance their ability to control access to these systems.

Careful attention should be given to the isolation and access control of management interfaces that support this design as they have the potential to impact multiple Electronic Security Perimeters.

SDWAN

Software-Defined Wide Area Networks (SDWANs) are comprised of an underlay network and an overlay network.

The underlay network is what we traditionally refer to as our Wide Area Networks and is constructed with various telecommunications provider circuits and technologies, including Serial, MPLS, LTE, Cable Modem, DSL, etc.

The overlay network is a virtual network layer created upon the underlay network, generally via encrypted tunnels or other similar mechanisms. An overlay network may utilize one or more underlay networks via load balancing or network policies. The policies governing the overlay network may dictate parameters such as what traffic is permitted, what underlay to utilize based on the application type, what should be utilized as the primary path, and various other parameters.

SDWAN enables the construction of secured and isolated network paths with enhanced management and monitoring capabilities in addition to enabling additional services to and from the SDWAN such as VPN connectivity, firewall services, traffic inspection, and shared gateways.

This technology provides an increased level of control over Wide Area Networks while enhancing visibility, security, and redundancy, all while offering the potential to reduce the costs associated with providing connectivity between an entity's locations and assets.

Figure 1 depicts a typical SD-WAN where encrypted tunnels protect traffic between sites A to C as well as sites B to C.

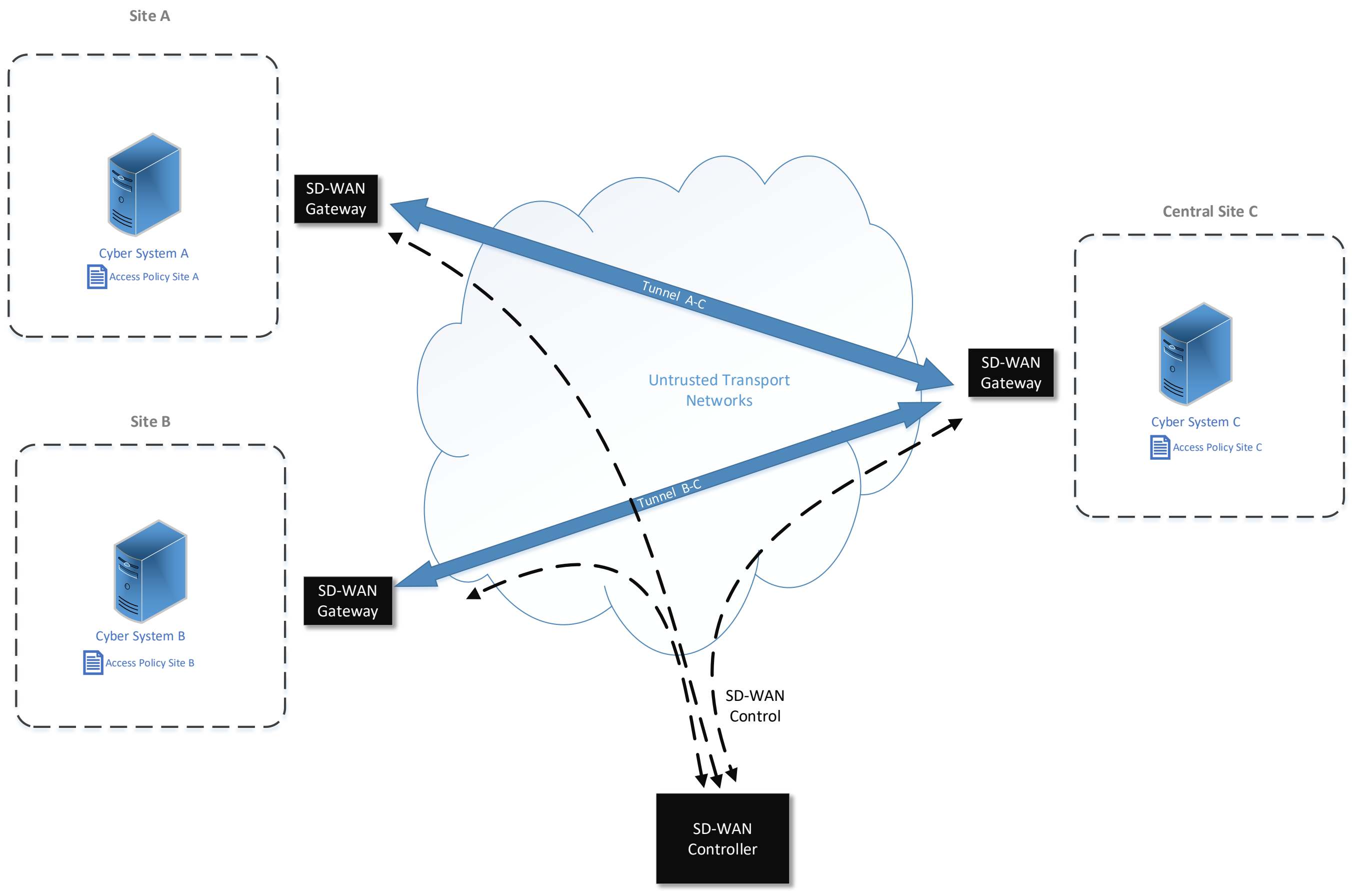

Figure 2 Typical SD-WAN

VXLAN

VXLAN is similar in concept to SDWAN in that it is a form of a Software Defined Network, but in the case of VXLAN the focus is on networks within the Datacenter as opposed to SDWAN which focuses on networks between Datacenters and other facilities.

VXLAN also utilizes the underlay and overlay terminology that we are familiar with given our review of SDWAN. The primary distinction is that VXLAN itself is the name of the overlay protocol utilized in this design and is the most common protocol used for overlay networks within a Datacenter.

The goal of VXLAN is to enhance the ability to segment network resources while also easing the burden of managing, automating, and orchestrating this segmentation by creating a virtual network that is agnostic of the physical network components supporting it.

The VXLAN protocol encapsulates Layer 2 Ethernet frames within Layer 3 UDP packets between devices comprising the design and allows for upwards of 16 million network segments to be created versus the traditional limit of 4094 VLANs. These network segments are identified with a VNI (VXLAN Network Identifier) which is synonymous with VLAN ID.

The components of the design that are capable of encapsulating and de-encapsulating the VXLAN protocol are referred to as VTEPs (VXLAN Tunnel Endpoints) and are commonly network switches or virtual machine hypervisors.

Physical devices and servers rely on switches to act as their VTEP whereas a virtual machine, hosted on VMWare ESX in this example, relies on the hypervisor as its' VTEP.

Figure 3 depicts a typical VXLAN where access control policies are implemented in the IP fabric.

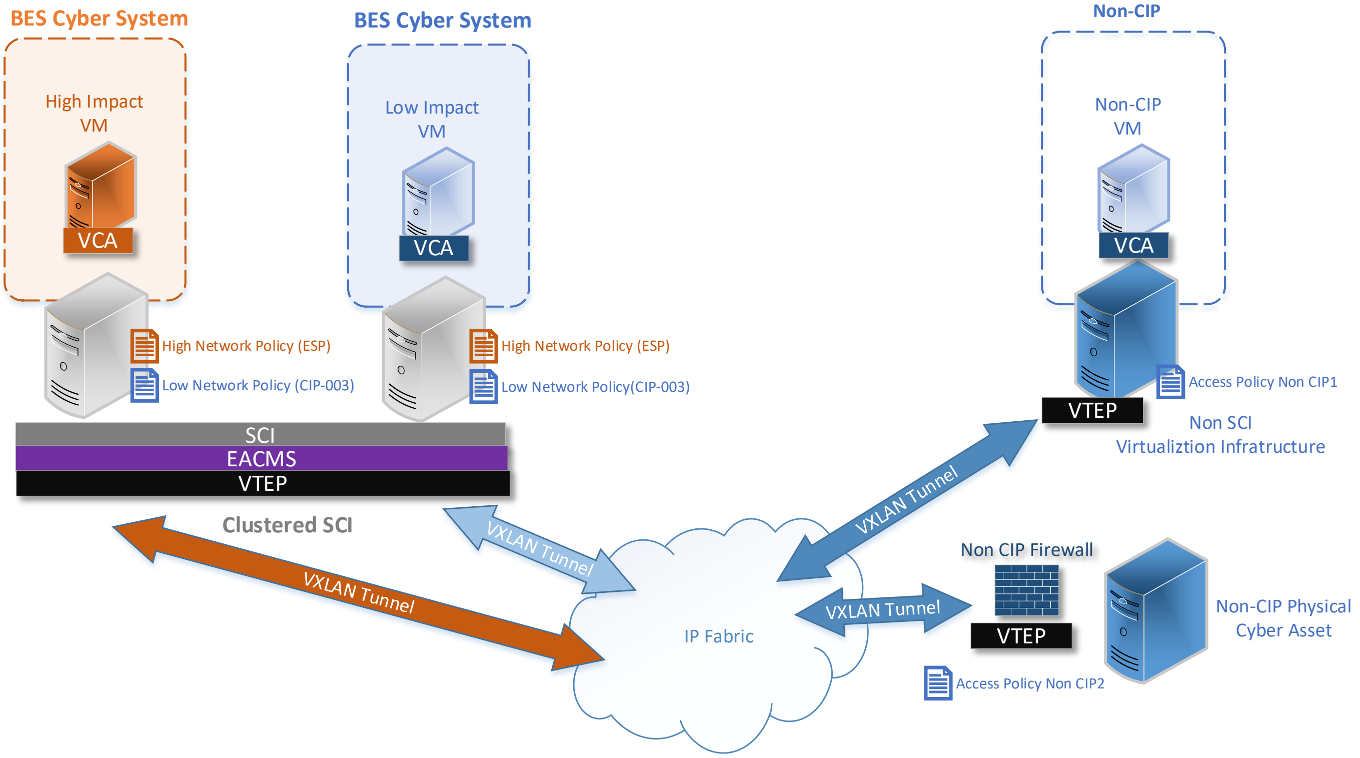

Figure 4 Typical VXLAN

VXLAN facilitates increasing the level of network segmentation within and between an entities Datacenters, while also enhancing their ability to automate and orchestrate the deployment of network resources. With this increased network segmentation an entity is granted more granular control over the flow of traffic and is given more opportunities to inspect that traffic to ensure appropriate levels of access control and protection.

Requirement R1

Rationale

Requirement R1 requires implementation of an ESP for BCS permitting only necessary communication through the ESP. However, there are other network security models available (such as zero trust) that can accomplish this security objective by controlling communications end-to-end at a more granular level than a network perimeter-based model. The definitions (ESP and EAP) and the changes to R1 allow entities the flexibility to implement different models that meet the security objective, or retain their current perimeter-based implementation.

Requirement R1 Part 1.1:

Rationale

This Requirement Part requires all high and medium impact BCS and their associated PCAs to be protected by an ESP. In recognition of non-perimeter based models, the language changed from “shall reside within” to “must be protected by”. Note, a PCA can now be defined by two different attributes of what they share with a BCS – not only network location, but also the sharing of CPU and memory from the underlying hypervisor(s) for VCAs. In the instance that a VCA becomes an ‘associated PCA’ from its sharing of CPU or memory with a high or medium impact BCS, that associated PCA must also be protected by an ESP.

Note that this Requirement Part applies to all high and medium impact BCS without regard to external connectivity from the local network to other networks. This allows for the identification of PCAs and the scope of TCA connectivity even on isolated networks.

Requirement R1 Part 1.2:

Rationale

This Requirement Part changed to a security objective, rather than prescribing ERC must be controlled at an EAP. Virtualization technologies introduce additional methods to isolate systems. This requirement part no longer prescribes one method of controlling communications to Applicable Systems, and opens it up for alternative solutions.

This allows for other models such as zero trust architectures. Such models are not based on controlling communications at a Cyber Asset interface located on a network boundary. Communications can be authorized by software defined policy enforcement points throughout the infrastructure. In this model, network security is less topology-based and more policy-based (configurations and settings) and can be used to granularly protect communication at an individual system or even process or resource level.

While pure zero-trust architectures are an emerging model, the objective-based requirement also allows for hybrid models of various combinations of network border-based and zero trust architectures. As technology changes, this requirement and broadened ESP definition are flexible in how the objective is met.

The intent of “through the ESP” is to better incorporate future Zero Trust implementations where there is no “logical border surrounding a network” but instead Policy Enforcement Points at the accessed resource itself or as close to it as possible. In these instances that are designed to be perimeter-less, the concepts of “inside” and “outside” begin to fail and the SDT is removing those now to be better prepared for future technologies. The SDT asserts that even in traditional Layer 3 firewalls that define an ESP, the communications between systems that are encapsulated in packets go “through” the perimeter (ESP) in order to reach their destination.

The core security objective, of permitting only needed communications and denying all others by no longer prescribing this must be implemented at a Cyber Asset interface on a network border (an EAP), is retained. The intent of this Requirement Part is to control the ‘reachability’ of the Applicable Systems; filtering network communications *before* they reach the Applicable Systems and their OS, not as part of it. This is not to discourage the use of integrated host-based firewalls to further filter network traffic to a host.

Note that the requirement now explicitly includes “the reason for granting access”. Previously, this had been an implied part of the requirement based on the Measures.

The SDT had considered adding “physical isolation” to the Measure, but did not do so as the applicability explicitly includes ERC. Additionally, within the Measures, the SDT uses examples of VLAN and VXLAN configurations as evidence. These configurations could be used as methods to “Permit only needed routable protocol communications”, despite not being OSI layer routable protocols in and of themselves.

Time-sensitive communications between Protection Systems (i.e., digital relays) that use routable communication protocols are excluded. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by inserting an ESP and its controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles (sub-second response times) to protect BES assets. The SDT intent is a Responsible Entity using this technology is not expected to implement the electronic access controls in a situation where it would prohibit the proper function in the proper timeframe.

Requirement R1 Part 1.3:

Rationale

It is important to note that Requirement Part 1.2 is scoped to the Applicable Systems protected by (inside) the ESP while Requirement Part 1.3 is scoped to protect the Management Interface of the Cyber Assets creating and controlling the ESP and thus not protected by the ESP itself. These different scopes show the need for separate Requirements Parts. In addition, the separation into different Requirement Parts prevents a recursive requirement. Otherwise, each EACMS would require an EACMS creating an impossibility to implement.

The objective of this new Requirement Part is to protect ESP configurations and SCI configurations. The intent is preventing unauthorized changes to these important configurations by controlling what can connect to administrative interfaces for SCI and certain EACMS.

This can be done by permitting only needed communications to the Management Interfaces, denying all other communications, of the systems that are providing protection of BCS; namely SCI that is supporting an Applicable System from Part 1.1 (SCI isolates systems of different impact levels from each other) and certain EACMS that are controlling an ESP. This Requirement Part only applies to SCI and EACMS controlling an ESP, and not to the BCS itself).

These are vital controls performing the isolation/segmentation between systems of differing impact levels, and warrant protection of the Management Interface that could be used to compromise them.

Certain EACMS that can control access to an ESP are subject to this requirement. This includes those EACMS such as a firewall that is controlling an ESP, a centralized station administering firewalls controlling ESPs as well as a network switch configured with VLANs to isolate and segment traffic. These certain EACMS will need to have their Management Interfaces protected. The SDT intended to exclude EACMS not associated with control and ESP such as domain controllers that provide only authentication services. The SDT is aware of possible implementations where an authentication server is used to provide real-time control of ESP access on a per user basis. In these situations, the authentication server does fall within scope of an EACMS that controls access to an ESP.

The ‘per system capability’ is included in this Part in recognition that some Management Interfaces, such as “ILO” interfaces, may do inbound but not outbound traffic controls.

Requirement R1 Part 1.4:

Rationale

The SDT included “SCI supporting an Applicable System in this Part” to the scope of the requirement part to ensure that controls regarding Dial-up Connectivity are also applicable to VCAs and SCI; and ‘technical feasibility’ has been replaced with the ‘per system capability’.

Additionally, in order to maintain a decipherable Applicable Systems column, the SDT replaced the scoping phrase “with Dial-Up Connectivity” from the Applicable Systems column, with a reference to “if any” in the Requirement Language.

Requirement R1 Part 1.5:

Rationale

Known or suspected malicious communication detection is specific to routable protocol based traffic that enters or leaves the required ESP. Products available to implement this malicious communication detection are usually based on IP traffic (as defined in RFC 791 and upon which TCP and UDP reside). The SDT intended to exclude other data center communications protocols currently in use such as Fibre Channel, where it would not be possible to meet this requirement.

The requirement applicability was changed to the ESP instead of EAPs; lifting it to an objective level and keeping it from being a prescriptive ‘where’ that forces certain architecture. These protections at the ESP level do not preclude entities from accomplishing the security objective by implementing controls at the EAP level, but offer entities the flexibility to implement other methods at the ESP level.

The SDT considered adding SCI to the Applicable Systems; however, chose not to do so as this functionally may be provided by SCI, thus resulting in a recursive requirement issue. Note that the Management Interfaces of SCI are protected by Requirement R1.3. Entities may wish to implement malicious communications detection on these Management Interfaces of SCI.

Requirement R1 Part 1.6:

Rationale

Requirement R1 Part 1.6 was written to address the issue of “Super ESPs” with high or medium impact BCS at Control Centers that extend a single ESP beyond one PSP. This often applies to virtualized Control Center environments that implement network adjacency to allow workloads to automatically move from one physical location to another to increase BCS resiliency between primary and backup Control Centers.

The security objective is to protect the confidentiality and integrity of the data traversing communication links used to span a single ESP between multiple PSPs. This is especially important when portions of the transport are not within the Registered Entity’s control. Many encryption methods (such as IPSec and TLS) can fulfil this objective; however, some encryption methods fall short of providing both confidentiality and integrity controls.

This Requirement Part works in conjunction with the new 4.2.3.3 exemption in the CIP standards that exempts the Cyber Systems associated with such communication links since the data is required to be protected per this requirement. Also, the former CIP-006-6, Requirement R1, Part 1.10 has been removed and incorporated into this new 1.6 requirement part; consolidating the protections of an ESP and its components that extend outside of a PSP within one standard.

Communications equipment associated with communications links (e.g., equipment belonging to carriers) is exempted from the CIP standards with the 4.2.3.2 exemption. However that only applies to equipment between discrete ESPs. In this extended ESP situation where a single ESP spans multiple sites or PSPs, that exemption does not apply and the potential exists for data to traverse a connection that uses third-party communications equipment that is unprotected inside an ESP; hence the need to enforce confidentiality and integrity controls (such as encryption) on the data that traverses PSPs while within the same ESP to isolate any protected data from access through the communications equipment.

This consolidation also incorporates cabling and non-programmable communication components that are not PSP-protected, intending to protect data moving across the state as well as data traversing cabling that crosses the hall outside of the PSP. Note: the language specifically exempts the data that falls under CIP-012 Requirements in order to avoid the potential for double jeopardy as well as the time-sensitive protection or control functions as described in CIP-005-8 Requirement R1 Part 1.1 above.

The SDT had considered adding SCI to the Applicable Systems; however, chose not to do so as this functionality may be provided by SCI, thus resulting in a “hall of mirrors” issue.

Requirement R2:

General Considerations for Requirement R2.

External Routable Connectivity (ERC) and Interactive Remote Access (IRA)

The ERC and IRA definitions have been updated in order to:

1. Incorporate new models such as Zero Trust where a security perimeter is not necessarily a network perimeter and ESPs become very granular based on policies that can be established at "people to resource" levels rather than IP address levels.
2. Recognize those Cyber Systems that are of an increased risk due to their "reachability" via ERC and that have IRA available to them even if they are serial-only, non-routable devices.
3. Continue to limit scope of Requirement Parts to BCS with ERC and not those that have connectivity such as non-routable serial leased circuits.

The V5TAG transfer document in the SDT's scope includes the issue of a BES Cyber Asset (BCA) that only uses non-routable protocols over a serial port. These BCAs are not connected to a network with a routable protocol themselves and therefore can be considered to not be within an ESP and thus not have ERC. However, these BCAs can have interactive user access using those serial connections. The SDT's intent is to clarify that IRA can occur to a device with only a serial, non-routable connection through IP-to-serial conversions and be subject to CIP-005-8 Requirement R2. For example, the intent is to clearly cover situations where a serial-only, non-routable BCA, such as a digital relay in a substation, has its serial communication from a 'console port' converted to IP or other routable protocols thus

allowing IRA from users outside the substation to use a routable protocol to interact with the serial device and to require the CIP-005-8 Requirement R2 protection for that IRA.

Due to the inclusion of serial based connections into the revised definition of IRA, other CIP requirements (i.e., CIP-004) have been revised to conform. Entities should review serial/IP converters that are currently being used for remote access.

The SDT removed the requirement-style language "The Intermediate System must not be located inside the Electronic Security Perimeter" from the Intermediate System definition in favor of a clarified objective in CIP-005-8 Requirement R2 that all IRA must be *through* an Intermediate System. Requirement R2 Part 2.6 was added to objectively address the location of the Intermediate System.

See the "*CIP Definitions and Exemptions Technical Rationale*" document for further explanation of the changes to the R2 related definitions.

Requirement R2 Part 2.1:

Rationale

Applicable Systems was updated to include SCI to ensure the same safeguards for remote access methods exist for SCI supporting an Applicable System within the Part as they do for the high and medium impact BCS and associated PCA hosted on that SCI. Backwards compatibility is retained for entities that do not use SCI. Please note that there may be situations where an Intermediate System is implemented as a VCA on SCI. The SDT intends that applicability for SCI is to ensure that the objectives of Requirement R1.3 are met such that the Management Interfaces of SCI are appropriately protected. VCAs are not considered part of SCI and therefore could be used to access a Management Interface of SCI.

The requirement language was simplified, and definitions for IRA and Intermediate System have been updated. Please note that the definition of IRA was changed to include serial communications that are converted to/from routable protocols by the Responsible Entity. This change maintains backwards compatibility except where serial connectivity and routable protocol conversion is being used for IRA.

Requirement R2 Part 2.2:

Rationale

The “Applicable Systems” scope was changed to “Intermediate Systems used to access Applicable Systems in Part 2.1”. This clarifies this requirement is associated with the IRA communications between an Intermediate System and the remote clients, as opposed to between the Intermediate System and the BCS. This is important so that it does not require encryption through the ESP to the BCS which would hinder monitoring and inspection.

The requirement was changed from a specific technical-based requirement for encryption to an objective-based requirement to protect confidentiality and integrity of the IRA session between the Intermediate System and the remote client (with encryption as a primary example). The proposed language accounts for the possibility that other equally effective methods could be developed and deployed. This objective also keeps methods from being used that are merely obfuscation methods (XOR, ROT13, etc.) or deprecated encryption methods (DES with 56-bit keys) that no longer meet the objective to protect the confidentiality and integrity of the IRA session.

The changed requirement is backwards compatible except where deprecated encryption methods are in use.

Requirement R2 Part 2.3:

Rationale

Applicable Systems was changed to “Intermediate Systems used to access Applicable Systems of Part 2.1”. This clarifies this requirement is associated with the Intermediate System itself, and where the requirement for multifactor authentication should be applied (multi-factor authentication to the Intermediate System).

Note that the wording of the requirement was updated to specially apply to IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System. This was previously implied.

Requirement R2 Part 2.4 – 2.5:

Rationale

The applicability and requirements have not changed.

Requirement R2 Part 2.6:

Rationale

This is a new requirement that applies to Intermediate Systems. The intent of this new requirement is to further protect the BCS from the Intermediate System by reducing the attack surface between the two. It is important to note that a virtualized Intermediate System (VCA) hosted in such a way that it can share CPU and share memory with a BCS will also meet the definition of PCA and become an ‘associated PCA’ of the BCS. CIP-005 R1.1 requires that PCA to be within an ESP, in conflict with this requirement. This is by design, and thus a VCA performing the function of an Intermediate System must not share CPU or memory with the BCS it is controlling access for. This is due to the access granted to the less trusted side of the Intermediate System and the risk for side-channel attacks to other VCAs sharing the same CPU and memory. Entities must therefore use affinity rules or some other means to keep Intermediate System VCAs from sharing the same CPU and memory as a BCS or its associated PCAs.

Figure 5 depicts an Intermediate System VCA where an affinity ruleset prevents the sharing of CPU or the sharing of memory with a BES System by ensuring these systems run on different on the hypervisor.

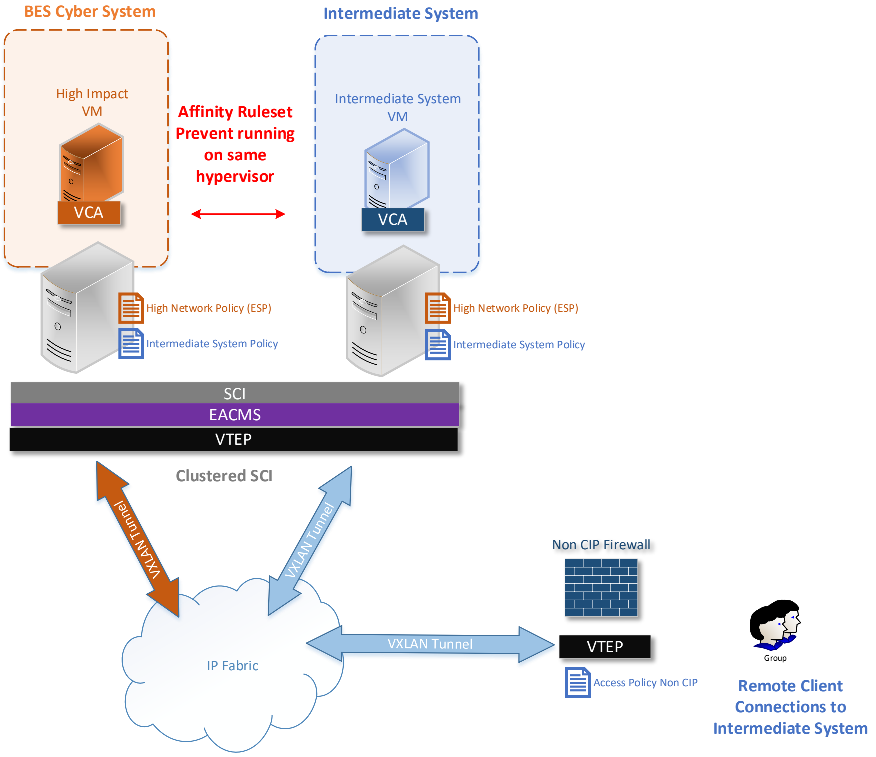

Figure 6 Affinity Rules - Intermediate System does not share CPU or share memory with BES Cyber Systems

Requirement R2 Part 2.7:

Rationale

This is a new requirement that applies to Intermediate Systems. The intent of this new requirement is to further protect the BCS from the Intermediate System by reducing the attack surface between the two. Intermediate Systems have an externally accessible interface that may be used by external parties such as vendors or entity support staff using IRA across an Internet connection to support a remote site. Since Intermediate Systems by nature provide IRA from a less-trusted network and are accessible from yet-to-be authenticated users (in order to authenticate them), a degree of separation from the higher-trust systems they are protecting is necessary in case the Intermediate System is compromised. Previously, this risk was addressed within the glossary definition of Intermediate System ("…must not be located inside the ESP") instead of within an actual requirement. The SDT removed this from the definition and included a security objective in CIP-005-8 Requirement R2 Part 2.7 to require that routable protocol communications between Intermediate Systems and Applicable Systems of Part 2.1 must be through an ESP.

It is important to note that the SDT does not intend to prescribe architecture to the point of what Cyber Asset or Virtual Cyber Asset a function may reside. For example, some "security appliances" that have firewall/EAP capability also have separate functionality within them that can perform part of the Intermediate System function. Historically this definition has stated "must not be located inside" which allowed for "outside or ON" the ESP. The SDT does not want to preclude architectures where at least some portion of the Intermediate System functionality may execute on the EAP.

Figure 7 depicts an Intermediate System running on non SCI infrastructure. Network connections from the Intermediate System to the BES Cyber Systems must pass through the ESP protecting those systems. In this case, access control policies, implemented on SCI are used to control network connections.

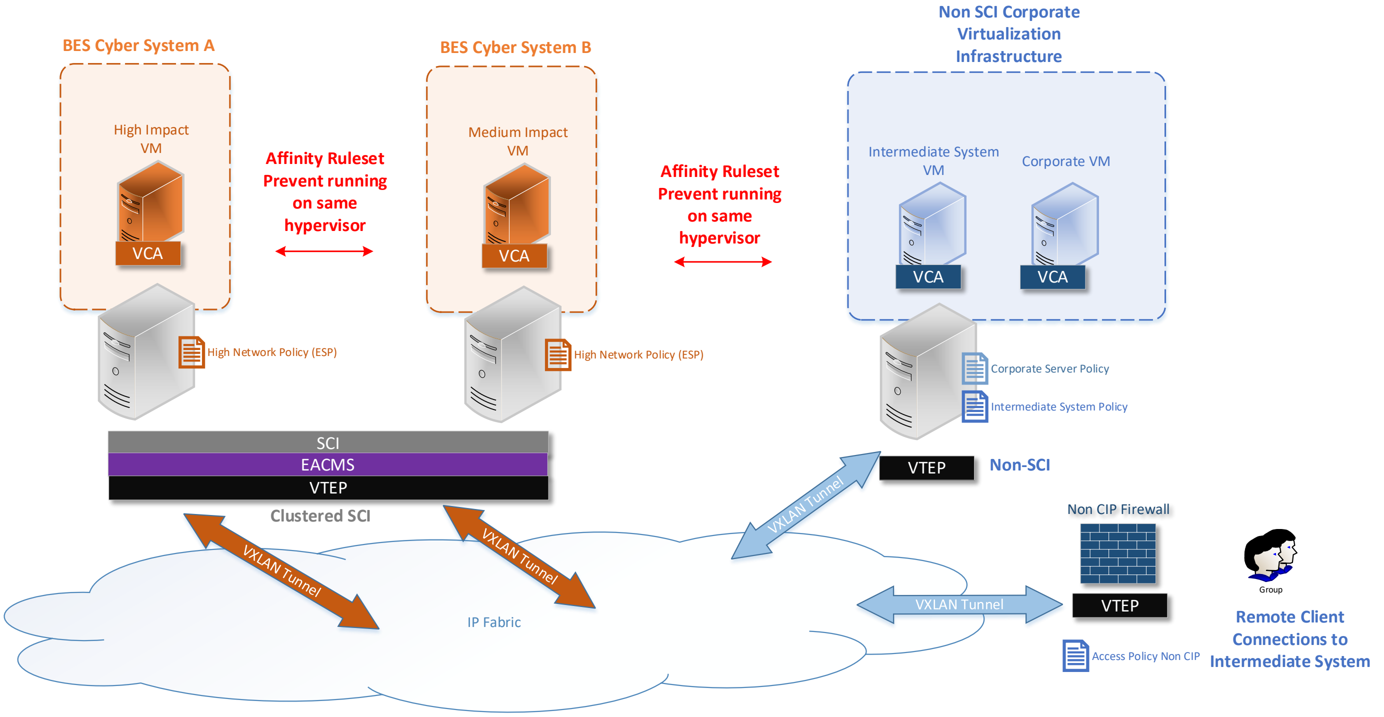

Figure 8 Intermediate System must connect through the Electronic Security Perimeter protecting the BES Cyber Systems

Requirement R3

Rationale

The Applicable Systems section of CIP-005-8 Requirement R3 was updated to include SCI to ensure the same safeguards for vendor-initiated remote connections exist for the applicable SCI. Backwards compatibility is retained for entities that do not currently use SCI.

Background Section from Reliability Standard CIP-005-7

The section 6. Background has been retired. removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BCS and require a minimum level of organizational, operational and procedural controls to mitigate risk to BCS.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BCS. For example, a single training program could meet the requirements for training personnel across multiple BCS.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

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

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.

- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.

- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.

- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

Technical Rationale for Reliability Standard CIP-005-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

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

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

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of Bulk Electric System (BES) Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Updates to this document now include the Project 2019-03 – Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting changes to the requirements.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those system that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require Responsible Entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

Additionally, the Project 2019-03 SDT removed Interchange Coordinator or Interchange Authority as that registration has been retired.

New and Modified Terms Used in NERC Reliability Standards

CIP-005-7 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The ESP serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network-based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R1

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, then each Cyber Asset of the low impact BES Cyber System are "Associated Protected Cyber Assets" of the high impact BES Cyber System and must meet all the requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero-day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communication to that known range. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rouge connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2

General Considerations for Requirement R2

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources should only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.

But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Requirement R3

Requirement Part 3.1 and Part 3.2 Vendor Remote Access Management for EACMS and PACS

The 2019-03 SDT added Requirement R3 to contain the requirements for all types of vendor remote access management for EACMS and PACS (i.e., system to system, user to system). EACMS were added based on FERC order 850 paragraph 5 where FERC ordered NERC to create a drafting team to add these devices. EACMS were added based on the risks FERC noted in paragraph 4, where a Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (DHS ICS-CERT) said firewalls (normally defined as an EACMS) is the “first line of defense within an Industry Control System (ICS) network environment”. The compromise of those devices that control access management could provide an outsider the “keys to the front door” of the ESP where BES Cyber Systems reside. An intruder holding the “keys to the front door” could use those “keys” to enter the ESP or modify the access controls to allow others to bypass authorization.

In Requirement R3 Part 3.1 and Part 3.2, the word "connection" is the mechanism for a user or a system to interact with an EAMCS or PACS for the purpose of authenticating.

In Requirement R3 Part 3.1 and Part 3.2, the word "authenticate" is the mechanism for the EACMS or PACS to identify the user or device. This permits the EACMS or PACS to first perform its function to authenticate the user or device that is connecting, which in turn permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections. This new proposed language is not prescriptive as to how authentication must occur to permit administrative and technical methods.

In Requirement R3 Part 3.2, the word "control" provides the entity flexibility to allow the vendor to reconnect under a specific set of conditions, established by the entity, where the reconnection is necessary to support critical operations of the entity. If the entity determines that they do not want to allow or does not need to allow a reconnection they can employ means to stop any reconnection.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability

Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Since remotely compromised PACS still require physical presence to exploit BES Cyber Systems, the SDT conducted extensive dialogue and considerations for the addition of PACS. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warranted their inclusion as an applicable Cyber Asset. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[1].

NERC's final report on "*Cyber Security Supply Chain Risks"*, states on page 4, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." PACS are intended to manage physical threats to BES Cyber Systems, thus protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical accesses or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access.

While other Reliability Standards mitigate certain security risks relating to PACS none address supply chain risk. Based on this analysis the SDT included PACS within the applicable section of both Requirement Parts 3.1 and 3.2.

An additional aspect of the NERC Supply Chain Report, the SDT considered was the risk associated with the access control vs. access monitoring functions of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the access control function beyond the access monitoring function. The SDT considered limiting the scope of the requirements to only those access control functions, however chose to stay with the currently approved definition of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally, an attempt to change the EACMS and PACS definition was outside the 2019-03 SAR.

Entities may or may not allow remote access into any of its systems, (BES Cyber Systems, EACMS or PACS), however if remote access is allowed, options to determine remote access connection(s) and capability to disable remote access connection(s) is required.

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Technical Rational for Reliability Standard CIP-005-6

This section contains an as-is "cut and paste" of the former Guidelines and Technical Basis (GTB) from Reliability Standard CIP-005-6 Technical Rationale to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

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

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

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

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an “Associated Protected Cyber Asset” of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually ‘command and control’ hosts on the Internet, or compromised ‘jump hosts’ within the Responsible Entity’s other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT’s intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity’s address space. The SDT’s intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and ‘deny by default’ type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear ‘perimeter type’ security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions (“TFEs”) rather than increased security.

As for dial-up connectivity, the Standard Drafting Team’s intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
E*xplicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.

But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)

This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Change Rationale: (Part 2.4 and 2.5)
Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).