NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – BES Cyber System Logical Isolation

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

January 2021

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 consists 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.

The title and purpose of CIP-005-8 changed from Electronic Security Perimeters (ESP) to Logical Isolation. Virtualization is enabling models for network security (such as "zero trust") that are not perimeter based. These innovations are the reason behind the move to a more flexible logical isolation basis for the standard since an ESP is now becoming one option among others. ESP and EAP implementations remain a popular and valid option well into the future and are one method for allowing only necessary and controlled communications while logically isolating all other communications. CIP-005-8 now focuses on this logical isolation such that high and medium impact BES Cyber Systems (BCS) must be "logically isolated" from all other systems (regardless of protocol) to replace the routable protocol-based ESP requirement as the solitary method that may be used.

Another concept introduced within CIP-005-8 is shared infrastructure. With the introduction of hardware (servers, storage, networks) as a generic infrastructure fabric on top of which virtual cyber systems, networks, and storage locations are built, the need to logically isolate cyber systems from others of different trust levels must move beyond a 'routable protocol only' separation. In these virtualized environments where shared infrastructure (hardware) is used, a risk of side channel attacks exists where, for example, a low impact BCS that shares CPU or memory with a high impact BCS and could be used to attack the high impact BCS through hardware-based vulnerabilities. CIP-005-8 mitigates this risk by either:

- Using affinity controls within the virtualization environment to configure the hypervisor(s) to disallow Virtual Cyber Assets (VCA) in these differing trust levels to simultaneously exist or execute on the same hardware underlay CPU and memory, or
- Treating all VCA that can simultaneously share the same CPU or memory as Protected Cyber Assets (PCA) of the highest impact system (high watermarking).

Additionally, the SDT is proposing a new requirement (CIP-005-8 Requirement R1 Part 1.5) to separate the management plane of the Shared Cyber Infrastructure (SCI) from the data plane. This is needed to ensure the reliability and security of the management plane as this is where the logical isolation is configured, as well as where the VCAs themselves are created or deleted.

CIP-005-8 also introduces exemptions and requirements for extending logical isolation or ESPs across different Physical Security Perimeters (PSP) (formerly known as "Super ESPs"). This can allow entities to extend a network to replicate data at high speed between two virtualization infrastructures (defined as SCI) or two databases in two different locations to improve the resilience and reliability of BCS. Requirement 1 Part 1.3 within CIP-005-8 requires that data traversing these "Super ESPs" be protected to preserve its integrity and confidentiality.

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 rational that follows.

Requirement R1 General Considerations

Logical Isolation

The title and purpose of CIP-005-8 changed from ESPs to Logical Isolation. Isolation methods such as ESPs and EAPs remain a valid option and are one method for implementing logical isolation. However, virtualization technologies present other equally effective methods than a perimeter-based solution that deals only with layer 3 routable protocols at a network boundary. Virtualization and its accompanying SCI have other characteristics such as shared hypervisors, shared storage, shared virtual networks and switches, all of which pose different security concerns but also have their own security controls. To adapt to these changes, CIP-005-8 focuses on an objective-based requirement (in Requirement R1 Part 1.1) for logical isolation.

CIP-005-8 Requirement R1 does not require logical isolation such that BCS must be completely isolated from each other if communication between them is needed. While allowing only necessary network communication between two systems, it requires "logical isolation" of all other unnecessary communication.

Shared infrastructure and "Mixed Trust" Risks

For virtualized environments where shared infrastructure (hardware) is used, a risk of side channel attacks exists. Virtualization allows disparate workloads of what could be differing impact or trust levels to execute on the same CPUs and share the same memory (i.e. RAM) within the infrastructure. There are vulnerabilities that are directly related to sharing hardware such as Spectre, Meltdown, and Rowhammer. Rowhammer, for example concerns processes sharing certain forms of hardware memory. Repeated writing of bits in one process could flip bits in a process in adjacent physical memory. This type of vulnerability is one of the unique risks of SCI.

As this class of vulnerability is specifically about processes executing side by side on the same CPU or memory chips of SCI, the risk of these vulnerabilities is being mitigated in CIP-005-8 by either:

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

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

The definitions created in support of the CIP Standards have historically included overlap. In this current version of CIP-005-8, the definition of PCA is updated with conforming changes that include VCA, as well as those that share CPU or memory with 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 EACMS that are also PCA, or SCI.

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 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 definition are applicable.

Requirement R1

Rationale

Requirement R1 is designed to implement various forms of logical isolation between systems such that only necessary communication is allowed between them. There are other network security models available now (such as zero trust) that can accomplish this security objective that are not perimeter based and control these communications only at various discrete points on a VCA or hosting SCI through either software-based policy or interface configuration.. However, the ESP model continues unchanged as CIP-005-8 Requirement R1 moves to an objective-based requirement that the ESP/EAP model can meet as well.

Requirement R1 Part 1.1:

Rationale

This requirement part is a combination of the first three requirement parts in the former CIP-005-7 version of the standard. Virtualization technologies introduce multiple additional methods to isolate systems and communications, beyond the ESP/EAP perimeter-based model. This requirement part is now objective-based and does not prescribe one method of controlling communications to applicable systems and logically isolating all other communications.

By moving to an objective-based requirement, ESP-based models may still meet the objective. The “or as a group” phrase within the requirement part allows for the protection of a group of applicable systems with an ESP/EAP model in order to permit only needed communications to and from those systems while logically isolating (deny by default) all other communications. While the definitions of ESP and EAP will move to inactive status in the retired section of the NERC Glossary of Terms upon the effective date of CIP-005-8, these former terms may still be used by registered entities for perimeter-based architectures to allow entities to continue to use these terms without having to update documentation.

The objective-based requirement allows for other models as well, such as zero trust architectures. Such models are not based on perimeter security that controls communications at a network boundary. Communications are authorized by policy enforcement points throughout the infrastructure. In this model, network security is less topology based and more policy based and is used to protect communication at a very granular level (an individual system or even process level).

While zero-trust architectures are an emerging model, the objective-based requirement also allows for hybrid models that are various combinations of perimeter-based and zero trust architectures. As technology changes, this requirement is flexible as to how the objective is met.

The obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by any required electronic access 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. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein in this situation.

Requirement R1 Part 1.2:

Rationale

The SDT is proposing a new Requirement, CIP-005-8 Requirement R1, Part 1.2. The purpose of this new Requirement is to require the separation of the Management Systems of SCI from systems that are not Management Systems. In essence to deny tenant systems hosted on the SCI the ability to communicate with Management Systems.

As virtualized servers, networks, switches, firewalls, and storage are logical constructs, controlling communications to the management of these systems becomes imperative. Communication with the Management Systems and Management Interfaces can allow users to create, modify, or delete objects or entire infrastructures, or move objects from one network to another. Therefore, administrative level or "management access" to the SCI is critical to the security and reliability of the hosted systems. By isolating the Management Systems and Management Interfaces of these devices from the larger audience of users that can communicate with the hosted tenant systems, the attack surface of the SCI is reduced to the group of users with the administrative functions.

As the same technologies used in on-premise virtualization are used by cloud vendors hosting systems from many different customers, the methods used to separate the management plane from the data plane developed quickly as systems moving to the cloud increased. For a cloud-based hosting facility to be successful, the tenants must share hardware resources (SCI as defined here) but have no ability to access or modify other tenants or their configuration. Cloud technology was forced to enhance existing methods and develop new methods to accomplish this separation. SCI presents the same issue for in-house (on-premise) virtualization environments to prevent users of various systems hosted on the SCI from affecting each other or the SCI's configuration. CIP-005-8 Requirement R1 Part 1.2 will mitigate that issue by bringing the isolation of the Management Systems and Management Interfaces into the scope of the CIP standards.

Requirement R1 Part 1.3:

Rationale

Requirement R1 Part 1.3 was written to address the issue of "Super ESPs" which extend a single ESP beyond one PSP. This Requirement may also apply to virtualized environments that implement network adjacency to allow workloads to automatically move from one physical location to another to increase BCS resiliency.

A security gap was identified that dealt with the potential for data to traverse a connection that uses third-party communications equipment, which is excluded from the CIP Standards. In order to close this security gap, the SDT chose to create Requirement R1 Part 1.3 to enforce confidentiality and integrity controls (such as encryption) on the data that traverses PSPs that are within the same logical isolation. In this case where communication equipment is used to extend a single ESP to more than one PSP, the confidentiality and integrity controls required in CIP-005-8 Requirement R1 Part 1.3 isolate any protected data from access through the communications equipment used to extend the logical isolation, therefore mitigating the threat from third-party communications equipment in use.

This Requirement Part applies to the data that traverses between PSPs. The SDT also combined CIP-006-6 Requirement R1 Part 1.10) into this Requirement Part because cabling and non-programmable communication components that are not protected within a PSP are considered within the CIP-005-8 Requirement R1 Part 1.1 logical isolation. The intent is to protect data moving across the state as well as data traversing cabling that crosses the hall outside of the PSP.

The requirement 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 chose to include "SCI hosting…" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in BCS, EACMS, Physical Access Control Systems (PACS) or PCA. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset's supporting hardware's impact on the individual Cyber Asset itself.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCA, and are therefore applicable.

Requirement R1 Part 1.4:

Rationale

The SDT chose to include "SCI hosting…" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets used in BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the Shared Cyber Infrastructure, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset's supporting hardware's impact on the individual Cyber Asset itself.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and are therefore applicable.

Requirement R1 Part 1.5:

Rationale

The SDT made conforming changes to specify that the malicious communication detection is for Internet Protocol (IP) based traffic that enters or leaves the required logical isolation in order to not prescribe a perimeter-based model.

The SDT chose to include "SCI hosting…" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets used in BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset's supporting hardware's impact on the individual Cyber Asset itself.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and are therefore applicable.

Requirement R2:

General Considerations for Requirement R2.

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

ERC has been used in the CIP standards for different purposes, including:

1. Establishing when EAPs are required (CIP-005-7)
2. Limiting scope of ~38 requirement parts to those locations that have a high enough level of remote connectivity to support the requirement

The move to the more objective-based requirements shifts the obligation away from implementing access controls at a defined cyber asset interface point (or by former definition, EAP). The objective can now be accomplished without dictating any architecture or access control method, thus eliminating ERC's role in determining EAPs. However, ERC

is still needed as a scoping mechanism for the vast scale of systems and their components within the geographically distributed BES locations. Many requirement parts should be scoped based on whether the system has ERC for the following reasons:

- The risk is increased for systems with ERC. The requirement should apply to those BCS with an increased attack surface and risk due to their connectivity/accessibility.
- Locations that have connectivity such as non-routable serial leased circuits should not have to increase their level of remote connectivity and attack surface to meet security requirements. For example, it would not be advisable to put in an IP network into a site to get SNMP traps out for alerts if a serial circuit with reduced attack surface is all that is needed for operations.

One issue with the ERC definition from the V5TAG transfer document is that of a BCA that only speaks non-routable protocols over a serial port. These BCAs do not use a routable protocol themselves and therefore can be considered to not have ERC because it is defined in terms of "routable protocol." These BCAs, however, can have interactive user access using those serial connections. The SDT has kept ERC as-is with only conforming changes in order to not disrupt its scoping function as noted above. However, the IRA definition has been modified so that a device with only a serial, non-routable connection can now have IRA and be subject to CIP-005-8 Requirement R2; and, appropriate controls are now required for these IRA sessions without regard to ERC. The intention is to cover situations where a serial-only, non-routable BCA, such as a digital relay in a substation, has that serial communication converted to IP or other routable protocols thus providing IRA from users outside the substation to interact with the serial device. Such situations require the CIP-005-8 Requirement R2 protection.

In modifying both the IRA and Intermediate Systems definitions, the SDT moved related requirement language from the previous definition into CIP-005-8 Requirement R2. The SDT added the "…that originates from outside…" text to the high level Requirement R2, removing it from the IRA definition. In this case the language works in collaboration with the IRA definition to allow access to a system that originates and terminates inside the logical isolation from CIP-005-8 Requirement R1 Part 1.1 without requiring an Intermediate System. However, for remote access that originates from outside of the logical isolation that accesses a device inside of the Requirement R1 Part 1.1 isolation would require CIP-005-8 Requirement R2 protections.

Requirement language includes wording for required logical isolation containing either high or medium impact BCS or associated SCI to provide the equivalent logical protections for remote access that existed before. Existing ESPs under CIP-005-7 can be used to provide the "required logical isolation" and thus remain backward compatible.

Similarly, the applicability was updated for virtualized environments so that it applies for remote access to Management Modules, Management Systems and Management Interfaces that did not originate from within another of the entity's instance of required logical isolation.

Requirement R2 Part 2.1:

Rationale

The Applicable Systems section of this requirement was updated to include SCI associated with high and medium impact BCS. This was done to ensure that same safeguards for remote access methods and technologies exist for the applicable SCI as for the high and medium impact BCS and associated PACS, EACMS, or PCA being hosted on that SCI. Backwards compatibility with CIP-005-7 is maintained for entities that do not currently use SCI.

The Applicable Systems section of this requirement was also updated to include Management Modules of SCI associated with high and medium impact BCS. This was done to ensure that same safeguards for remote access methods and technologies exist for the applicable SCI as for the high and medium impact BCS and associated PACS, EACMS, or PCA being hosted on that SCI. Backwards compatibility with CIP-005-7 is maintained for entities that do not currently use SCI.

The inclusion of the SCI is intended to target the Management Modules and Management Systems (included in SCI definition) of the associated SCI. This is to ensure that the management of the SCI being used to support BCS is also protected in an equivalent manner.

For Medium Impact BCS, the Applicable Systems wording was updated from "with ERC to "with IRA". This was done to cover serial connectivity associated IRA for those Applicable Systems without ERC. This aspect of IRA was missing from earlier versions of CIP-005. This change is intended to mitigate risks associated with a possible external (to the entity) attack vector in situations where serial connectivity is converted to network connectivity using a terminal server type device. This is one of the issues noted by the V5TAG and is not associated with changes required for virtualization. Please refer to the section of this document entitled "**External Routable Connectivity (ERC) and Interactive Remote Access (IRA)**."

The requirement language itself was simplified. Note the definitions of IRA and Intermediate System have been updated. Please note that the definition of IRA was changed to include serial communications connections. This change maintains backwards compatibility with CIP-005-7 except where serial connectivity is being used for IRA.

The required location of an Intermediate System was within the definition previously. The definition of Intermediate System has been simplified and the requirement to be logically isolated from its Applicable Systems is now within the requirement itself (Part 2.6.2) rather than within the definition.

Requirement R2 Part 2.2:

Rationale

The Applicable Systems was changed to Intermediate Systems from high or medium BCS and associated PCA. This change better reflects that this requirement is associated with the Intermediate System itself.

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. The proposed language of this requirement accounts for the possibility that other equally effective methods could be developed and deployed. This also prevents outdated encryption methods from being used that no longer meet the objective.

The changed requirement is backwards compatible with the CIP-005-7 except where outdated encryption methods have been used.

Requirement R2 Part 2.3:

Rationale

The Applicable Systems was changed to Intermediate Systems from high or medium BCS and associated PCAs. This change better reflects that this requirement is associated with the Intermediate System itself. Note that serial connection-based IRA is now included due to the IRA definition change. This change also clarifies where the requirement for multifactor authentication should be applied.

The changed requirement is backwards compatible with the CIP-005-7 except where serial connection-based IRA is being utilized.

Requirement R2 Part 2.4 – 2.5:

Rationale

The Applicable Systems section was changed to include SCI hosting High or Medium impact BCS or their associated PCA, including its Management Modules, in instances where vendor remote access is allowed to the SCI or Management Modules. The applicable systems were also modified such that only those with vendor remote access

are in scope and thus need to have one or more methods for CIP-005-8 Requirement R2 Parts 2.4 and 2.5.

The inclusion of SCI is intended to target the Management Modules and Management Systems (included in SCI definition) of the associated SCI. This is to ensure that the management of the SCI being used to support BCS is also protected in an equivalent manner.

The requirements themselves have not been changed. Note that the requirement includes both vendor based IRA and system-to-system access.

Requirement R2 Part 2.6:

Rationale

This is a new requirement that applies to Intermediate Systems that are required by CIP-005-8 Requirement R2 Part 2.1. This is due to instances where 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, a degree of separation from the higher-trust systems they are protecting is necessary in case the Intermediate System is compromised. Previously, this separation "requirement" was not an actual requirement but was contained within the glossary definition of Intermediate System ("…must not be located inside the ESP"). The SDT has removed this from the definition and included an objective in CIP-005-8 Requirement R2 Part 2.6.2 to permit only needed and controlled communications between the Intermediate System and the applicable systems it is providing IRA to.

In order to further mitigate the risk of a compromised virtualized Intermediate System hosted on SCI, Requirement CIP-005-8 Requirement R2 Part 2.6.1 restricts CPU and memory sharing on SCI to only its associated SCI itself and other Intermediate Systems.
In summary, CIP-005-8 Requirement R2 Part 2.6 is intended to mitigate the risk associated with "side channel" based attack vectors where it could be possible to compromise the Intermediate System from an external source and then subsequently access another VCA running on the same hypervisor within the SCI.

Requirement R3

Rationale

The Applicable Systems section of CIP-005-8 Requirement R3 was updated to include SCI hosting EACMS or PACS associated with high or medium impact BCS to ensure the same safeguards for vendor-initiated remote connections exist for the applicable SCI. Backwards compatibility with CIP-005-7 is maintained for entities that do not currently use SCI.

The Applicable Systems section of this requirement was also updated to include Management Modules of SCI hosting EACMS or PACS associated with high or medium impact BCS to ensure the same safeguards for vendor-initiated remote connections exist for the applicable Management Modules. Backwards compatibility with CIP-005-7 is maintained for entities that do not currently use SCI.

The inclusion of the SCI is intended to target the Management Modules and Management Systems (included in SCI definition) of the associated SCI to ensure the management of the SCI is also protected in an equivalent manner.

Former Background Section from Reliability Standard CIP-005-7

The section **6. Background** has been retired and 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 a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard 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).