NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT
Cyber Security – BES Cyber System Logical Isolation

Technical Rationale and Justification for Reliability Standard CIP-005-7

RELIABILITY | ACCOUNTABILITY

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

Table of Contents

Introduction

This document is the technical rationale and justification for the proposed Reliability Standard CIP-005-7. The Standard Drafting Team's (SDT) intent of this document is to provide stakeholders and the ERO Enterprise with an understanding of the proposed revisions and the technical concepts of the Reliability Standard. This Technical Rationale and Justification for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Executive Summary

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. The Standard Drafting Team (SDT) is proposing changes to CIP-005-6 as it updates the standards based on technology innovation and changes such as the increasing use of virtualization. Project 2016-02 SDT was assigned the task to address the technological innovation in virtualization within the CIP standards. The SDT's purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards. The SDT's intent is to better position the CIP standards to be applicable to additional future technological innovation.

The Project 2016-02 CIP SDT proposes the following modified terms within the NERC Glossary:

- BES Cyber Asset (BCA);
- External Routable Connectivity (ERC);
- Interactive Remote Access (IRA);
- Intermediate System (IS);
- Physical Access Control System (PACS);
- Physical Security Perimeter (PSP);
- Protected Cyber Asset (PCA);
- Removable Media (RM); and
- Transient Cyber Asset (TCA).

The Project 2016-02 CIP SDT proposes the following new terms to the NERC Glossary:

- Electronic Access Control Systems (EACS);
- Electronic Access Monitoring System (EAMS);
- Electronic Security Zone (ESZ);
- Physical Access Monitoring System (PAMS);
- Shared Cyber Infrastructure (SCI); and
- Virtual Cyber Asset (VCA).

The Project 2016-02 CIP SDT proposes to retire the following terms:

- Electronic Access Control and Monitoring System (EACMS); and
- Electronic Access Point (EAP).

These modified terms, new terms, and retired terms are further explained herein.

The title and purpose of CIP-005-7 changed from Electronic Security Perimeters to Logical Isolation. ESP's and EAPs remain a valid option and are one method for implementing logical isolation. However, virtualized technologies present other equally effective methods than ESPs that deal only with layer 3 routable protocol addressing. To adapt virtualization's characteristics, CIP-005-7 focuses on logical isolation such that high and medium impact BES Cyber Systems 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-005-7 is shared infrastructure. For virtualized environments where shared infrastructure (hardware) is used, a risk of side channel attacks exists. CIP-005-7 proposes to require the placing of virtualized systems of differing trust levels into differing ESZ's, and then affinity controls must be applied to these zones. These affinity groups must be configured such that a hypervisor does not allow workloads in these differing zones to simultaneously exist or execute on the same hardware underlay compute resources.

Additionally, the SDT is proposing a new requirement (CIP-005-7 R1.6) to separate the management plane of the SCI from the data plane. This is needed to ensure the reliability and security of the management plane.

CIP-005-7 also introduces exemptions and requirements for extending ESPs or ESZs across geographic locations also known as "Super ESPs". This allows, for example, entities to extend a network to replicate data at high speed between two virtualization infrastructures (SCI) or two databases in two different geographic locations to improve the resilience and reliability of BES Cyber Systems. Requirement 1 Part 1.3 within CIP-005-7 requires that data traversing "Super ESPs" be protected to preserve its integrity and confidentiality.

Proposed Modified Terms:

BES Cyber Asset (BCA)

A Cyber Asset or Virtual Cyber Asset; excluding Shared Cyber Infrastructure, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Rationale

The BCA definition is changing to allow for BES Cyber Assets to be either Cyber Assets (hardware included) or Virtual Cyber Assets (without the underlying hardware). The definition of BCA excludes the underlying hardware for virtualized environments, now defined as Shared Cyber Infrastructure (SCI). The SDT recognizes that SCI indeed has the same impact as a virtual BES Cyber Asset and even more so if hosting numerous BES Cyber Assets. For the first formal posting of all affected standards, the requirements for SCI will be equal to BCA and in fact be subjected to additional requirements due to its impact (e.g. CIP-005 R1 Part 1.6). See the SCI definition below.

External Routable Connectivity (ERC)

The ability to access a BES Cyber System from a Cyber Asset or Virtual Cyber Asset that is outside of its associated Electronic Security Perimeter or Electronic Security Zone via a bi-directional routable protocol connection.

Rationale

The ERC definition is used throughout the CIP Standards, within the Applicable Systems column, as a scoping mechanism based on the inherent risk associated with external routable connectivity. In order to maintain the correct ERC scoping the SDT made conforming changes to the ERC definition to include both Virtual Cyber Assets and ESZs, but maintained the caveat of "via a routable protocol connection." This effectively updates the ERC term to include the applicable new concepts presented within the updated CIP Standards.

Interactive Remote Access (IRA)

User-initiated access by a person employing a remote access client.

Rationale

The IRA definition is changing to remove several requirements and scoping mechanisms that were embedded within it so that it becomes a simple glossary definition. The requirements and scoping mechanisms have been moved into CIP-005 R2. The references to ownership of the remote client have been removed as immaterial to the definition or the CIP-005 requirements. The reliance on "using a routable protocol" has been removed to incorporate IP to serial conversion scenarios to serial only Cyber Assets. See discussion under the General Considerations section below.

Intermediate Systems (IS)

A type of EACS that is used to restrict Interactive Remote Access.

Rationale

The IS definition is changing to remove requirements-like language (e.g. where an IS must reside) that was embedded within the definition. Such language has been moved to CIP-005 R2.

Physical Access Control Systems (PACS)

Cyber Assets or Virtual Cyber Assets that control access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Rationale

The PACS definition is changing to 1) allow Virtual Cyber Assets as a form that PACS can take, and 2) separate out the non-access control functions (see PAMS below). This will allow differentiation in requirements based on the different risk profiles of a system that controls physical access versus systems that only log or alert (i.e. a SIEM or internal or outsourced monitoring service). The intent is that a system that both controls and monitors physical access remains a PACS. If the system controls physical access, it is a PACS regardless of its monitoring capabilities.

Physical Security Perimeter (PSP)

The physical border at which access is controlled.

Rationale

The PSP definition is changing to remove references to EACMS and other applicable systems. The applicability of the CIP-006 PSP requirements was included within the definition, so as the applicability of the requirements change over time (such as adding SCI), the definition would need to change. The SDT is proposing to remove not only the proposed retired term EACMS but all applicability from the definition to avoid current and future issues.

Protected Cyber Asset (PCA)

Cyber Assets or Virtual Cyber Assets that:

- Are connected using a routable protocol within or on an Electronic Security Perimeter that are not part of the highest impact BES Cyber System within the same Electronic Security Perimeter; or
- Are within the same Electronic Security Zone that are not part of the highest impact BES Cyber System within the same Electronic Security Zone; or
- Share compute resources (CPU or memory) with a BES Cyber System.

Rationale

The PCA definition is being updated to include the ESZ option so that Cyber Assets within an ESZ that are not part of the highest impact BES Cyber System within the zone become an associated PCA of the highest impact BES Cyber System.

The definition is also being updated to include “share compute resources (CPU or memory) with a BES Cyber System” to mitigate the risks of hardware-based vulnerabilities (Spectre, Meltdown, Rowhammer, etc.) on Shared Cyber Infrastructure. Since virtualization can allow systems of differing trust levels to simultaneously execute on the same hypervisor servers in the hardware underlay and thus share the same CPU and memory, this addition to the PCA definition requires that those VCAs that do share CPU and memory become associated PCA’s of any BES Cyber Systems sharing the same hypervisor compute resources. This provides the high water marking of VCAs sharing a single hypervisor’s CPU or memory.

See the “Shared Infrastructure and ‘Mixed Trust’ Risks” section below for a more in-depth discussion.

Removable Media

Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP or ESZ, a Protected Cyber Asset, or SCI.

Rationale

The Removable Media definition has conforming changes to allow the targets to which the media may be connected include SCI and a network within an ESZ.

Transient Cyber Asset (TCA)

A Cyber Asset or Virtual Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
    - BES Cyber Asset,
    - Shared Cyber Infrastructure (SCI),
    - network within an Electronic Security Perimeter (ESP) or Electronic Security Zone (ESZ) containing high or medium impact BES Cyber Systems, or
    - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Rationale

The TCA definition is changing to incorporate the virtualization definitions in three ways. First, VCA is being added as a form a TCA can take. The intent is to handle VCAs that are created for typical TCA uses but are normally dormant (e.g. a Virtual Machine (VM) with Wireshark for troubleshooting network issues within a virtualized infrastructure). Secondly, SCI was added as a target to which TCA's can be directly connected. Thirdly, conforming changes were made to add connection to a network within an ESZ as an option.

Proposed New Terms:

Electronic Access Control Systems (EACS)

Cyber Assets or Virtual Cyber Assets that provide electronic access control to an ESP, ESZ, or BES Cyber Systems.

Rationale

The EACMS definition is splitting into two terms. The EACS definition is proposed to 1) allow Virtual Cyber Assets as a form that EACS can take, and 2) separate out the non-access control functions. This will allow differentiation in requirements based on the different risk profiles of a system that controls access (i.e. a firewall) versus systems that only log or alert (i.e. a SIEM or internal or outsourced monitoring service). The intent is that a system that both controls and monitors electronic access remains an EACS. If the system controls electronic access, it is an EACS regardless of its monitoring capabilities.

Electronic Access Monitoring System (EAMS)

Cyber Assets or Virtual Cyber Assets that provide electronic access monitoring of an ESP, ESZ, or BES Cyber Systems.

Rationale

The EACMS definition is splitting into two terms. The EAMS definition is proposed to 1) allow Virtual Cyber Assets as a form that EAMS can take, 2) incorporate ESZs, and 3) separate out the non-access control functions. This will allow differentiation in requirements based on the different risk profiles of a system that controls access (i.e. a firewall) versus systems that only log or alert (i.e. a SIEM or internal or outsourced monitoring service).

Electronic Security Zone (ESZ)

A segmented section of a network that contains systems and components to create logical isolation.

Rationale

In previous versions of the CIP standards, CIP-005 required declarations of Electronic Security Perimeters (ESP) based on OSI layer 3 routable protocols. All BES Cyber Assets (BCA) that were connected to a network with routable protocols had to reside inside a declared ESP. Any External Routable Connectivity (ERC) to the BES Cyber Systems inside the ESP had to enter and exit via an Electronic Access Point (EAP) that limited the traffic entering or leaving the ESP to only necessary traffic. It denied all other traffic by default.

This “castle and moat with drawbridge” protection, where the castle is the BES Cyber Systems (BCS), the moat is the ESP, and the drawbridge is the EAP, has been in place for many years. For many situations, the ESP/EAP model remains a valid network architecture however it is no longer the only model. Prescribing the ESP/EAP as the sole model hinders the adoption of other models that are equally or even more effective. Network access control is expanding beyond perimeter-based security at routable protocol address levels into other models where access controls are enforced within the network fabric itself. The entire network is becoming “the firewall” rather than a centralized point at a network boundary. Within virtualized environments, entities can describe network access at a policy level within a *zone* and zones may not follow the typical IP subnet defined network space. Zones allow for network access permissions to be applied to workloads based on their function and/or trust level rather than purely by network location which for resiliency purposes can be very dynamic. If a virtual machine is a member of a zone, it gets that zone’s access permissions applied to it regardless of its network location. IP addresses and port numbers, which are simply protocol data, become less common methods of identifying and filtering communications, especially in virtual environments where workloads dynamically move and may change network location but stay within the same zone. The zone’s policies follow the workload, not a network address range. This is driving solutions more towards policy-based user access controls for workloads that the infrastructure then dynamically applies within the environment.

In essence, as network access controls become embedded into the infrastructure, these environments may no longer have an “Electronic Access *POINT*”; no single interface on a perimeter where network access rules are enforced but are instead highly distributed within the network. This is the reason the CIP standards are adding the ”Electronic Security Zone” (ESZ) concept as an option that can be chosen for systems in addition to or in place of the ESP/EAP model.

Physical Access Monitoring System (PAMS)

Cyber Assets or Virtual Cyber Assets that alert or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Rationale

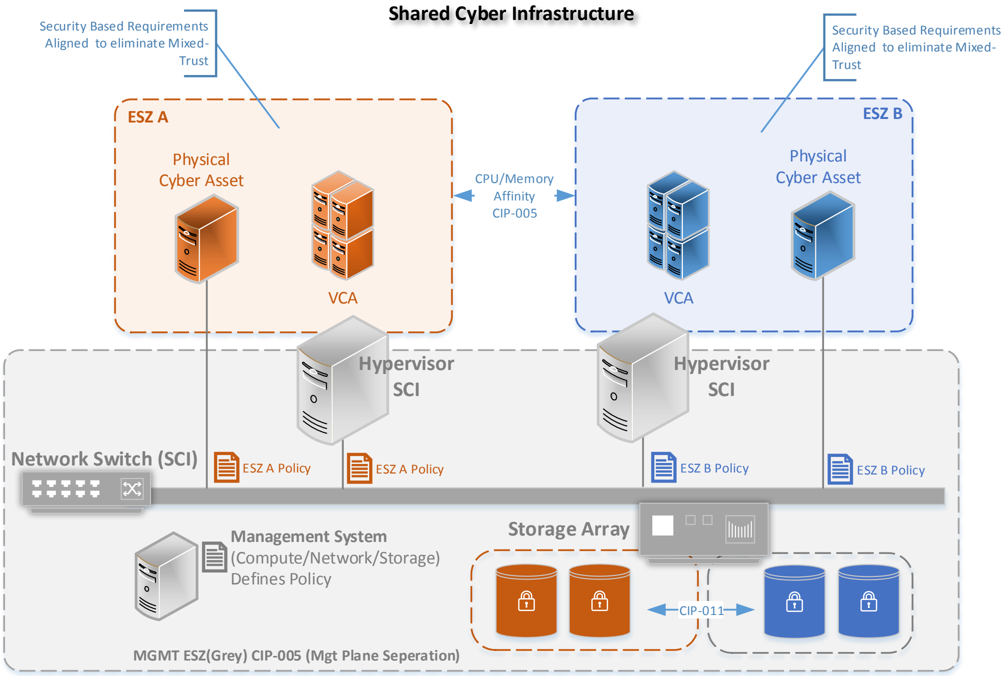
The PACS definition is splitting into two terms. The PAMS definition is proposed to 1) allow Virtual Cyber Assets as a form that PAMS can take, and 2) separate out the non-access control functions. This will allow differentiation in requirements based on the different risk profiles of a system that controls access (i.e. a badging system) versus systems that only log or alert (i.e. a SIEM or internal or outsourced monitoring service that only receives data).

Shared Cyber Infrastructure (SCI)

Programmable electronic devices whose compute, storage (including network transport), or network resources are shared with one or more Virtual Cyber Assets or that perform logical isolation for an ESZ or ESP. This includes its management systems.

Rationale

The SCI definition is being created to separate the underlying hardware from the VCAs that it hosts. This allows security requirements to be targeted to SCI to address the unique risks of virtualization and shared hardware. There are many requirements that now include the newly defined term SCI in the "Applicable Systems" column to maintain security level parity with traditional Cyber Assets. This change is justified because the hardware underlay would not have required protections at the same level as an applicable virtual system without this inclusion.


Shared Cyber Infrastructure
Security Based Requirements Aligned to eliminate Mixed-Trust
Security Based Requirements Aligned to eliminate Mixed-Trust
ESZ A
Physical Cyber Asset
VCA
CPU/Memory Affinity CIP-005
ESZ B
Physical Cyber Asset
VCA
Hypervisor SCI
Hypervisor SCI
Network Switch (SCI)
ESZ A Policy
ESZ A Policy
ESZ B Policy
ESZ B Policy
Management System (Compute/Network/Storage) Defines Policy
Storage Array
CIP-011
MGMT ESZ(Grey) CIP-005 (Mgt Plane Seperation)

Beyond security level parity with protecting a typical hardware based Cyber Asset, the SCI can have a more significant impact in a virtualized environment since it can host, and therefore impact, multiple virtualized systems. Because of this capability, some additional controls only apply to SCI, such as the management plane isolation required by the proposed CIP-005-6 R1.6.

The statement "or performs logical isolation for an ESZ or ESP" is found within the Shared Cyber Infrastructure definition. This inclusion is intended to ensure that devices that provide logical isolation for an ESZ or ESP, and therefore have an associated risk, have protection for the associated management systems (management plane) as required by Part 1.6. This inclusion is meant to ensure protection of firewalls or network switches if used to provide logical isolation to an ESP, ESZ, or within Shared Cyber Infrastructure (see discussion and examples under the R1.6 section below). This can be viewed as a replacement for the Electronic Access Point (EAP) found in the previous version of the standard.

In the diagram above, an orange ESZ and a blue ESZ are depicted. Each ESZ contains VCAs and a physical Cyber Asset along with storage configured within a storage array. The individual ESZs are defined via policies created in the management system that are implemented by the SCI to create the logical isolation of that zone within the SCI's compute, network, and storage resources. The SCI for this scenario is depicted in grey and includes the hypervisor servers, the network switch, the storage array hardware, and the management system(s) for each.

Virtual Cyber Asset (VCA)

A logical instance of an operating system, firmware, or self-contained application hosted on SCI.

Rationale

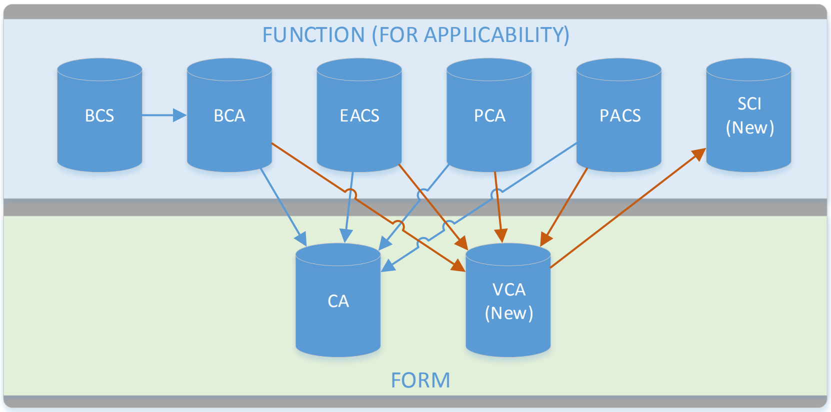
The NERC Glossary definition of Cyber Asset has a direct tie to the hardware on which it relied. This affected the definitions of the “Applicable Systems” terms such as BES Cyber Systems (BCS), EACS, PACS, and Protected Cyber Assets (PCAs). Because the Reliability Standard is applicable to the aforementioned systems, the control for the Cyber Assets also applies to the hardware. This tie to hardware implies a singular one BCA, EACS, PACS or PCA per individual hardware system. This one-to-one relationship between a Virtual Cyber Asset and its underlying hardware is what virtualization intentionally breaks to increase reliability and resiliency by allowing Virtual Cyber Assets to be abstracted from a particular hardware cyber asset and therefore able move to any available hardware out of a pool of resources.

The proposed NERC Glossary definition of Virtual Cyber Asset (VCA) allows the tie between a specific piece of hardware and the related applicable systems to no longer be singularly defined. The definition of VCA is not inclusive of hardware, and the EACS, PACS and PCA definitions have been updated to allow for VCA versions. With the addition of SCI and revisions to the “Applicable Systems”, there can be one or more virtualized instances of a BCA, EACS, PACS or PCA that reside on SCI.

Examples of Virtual Cyber Assets may include, but are not limited to, logical instances of the following:

- Operating Systems (Virtual Machines (VM));
- Containers, which are executable software package images that are standalone and self-contained;
- Networking devices such as switches, routers, and load balancers;
- Security appliances such as firewalls and VPN concentrators; and
- Helper appliances with logical connectivity (such as malware detection, plugins, etc.).

This diagram depicts the relationship between many of the glossary definitions in that some are the “form” of an object and some are the “function” it provides. The top row shows definitions of “functions” or services that are performed or provided. The bottom row is the “form”. Previously the only form that existed was the Cyber Asset definition which included the hardware and historically had a 1:1 relationship (e.g. a digital relay, a desktop computer operator workstation, a database server in a rack, etc.). The addition of the Virtual Cyber Asset definition clarifies a new form that the functions can take which is abstracted from the underlying hardware. The new SCI definition provides the functions of compute, network, and storage resources and logical isolation for VCAs. The blue arrows are the existing definitional relationships and the red arrows are the new definitional relationships that are being added.



Proposed Retired Terms:

EACMS

Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.

Rationale

The EACMS definition is splitting into two terms (EACS and EAMS) to allow differentiation in requirements based on the different risk profiles of a system that controls access (i.e. a firewall) versus systems that only log or alert (i.e. a SIEM or internal or outsourced monitoring service). The combined term is proposed to be retired.

EAP

A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Rationale

With the move to an objective based requirement in CIP-005 and the need to not prescribe a cyber asset interface, an electronic access POINT, on a network boundary as the only model for addressing network access control, the term EAP is no longer used within the standard and is proposed to be retired. Entities are free to continue to use the term in their internal documentation to maintain backwards compatibility. See also the discussion for the SCI and ESZ definitions.

Logical Isolation

The title and purpose of CIP-005-7 changed from Electronic Security Perimeters to Logical Isolation. ESP's and EAPs remain a valid option and are one method for implementing logical isolation. However, virtualization technologies present other equally effective methods than ESPs that deal only with layer 3 routable protocol addressing. Virtualization and its accompanying shared infrastructure have other characteristics such as shared computing hosts, shared storage, shared virtual networks and switches, all of which pose different security concerns but also have different security controls. To adapt to these changes, CIP-005-7 focuses on an objective-based requirement (in Requirement Part 1.2) for logical isolation.

The SDT chose the term "logical isolation" to distinguish the type of isolation required from complete isolation or physical isolation alone. Logical isolation refers to the isolation of communications between systems. Two BES Cyber Systems can be physically isolated into two different access-controlled areas, but still have uncontrolled communication between them. Also, two virtual cyber systems within two different ESZs or ESPs of differing trust or impact levels may be running on two hypervisors within the same physical area, but still be logically isolated from each other. *Logical isolation means that only known, controlled communications can occur between a system and anything outside of its ESZ or ESP and that all other communication is blocked.* Serial communications such as RS-232 or RS-485 are logically isolated communications methods as well. These types of communications move data from the TX pin on one end of a cable to the RX pin on the other end of the cable. There is no addressing scheme or routing/firewall capability, so it meets the intent of logical isolation.

If a BCS is executing on a virtual host along with another related virtual machine that may not have a 15-minute impact, (e.g. a control system and its data historian), the entity must either consider all these workloads as part of a single system or declare the system with the 15-minute impact as a BCS and the historian as a separate system. If the latter is chosen, the entity will need to prove that the two systems are logically isolated and that every communication between the two is limited to only what is necessary.

Logical isolation is also relevant to other layers of a computing stack. Imagine in a virtualized data center where you are looking at a BES Cyber System architecture "from the side". You can see the different layers of the system, from the storage on a Storage Area Network (SAN) through the virtual networks, switches, and firewalls at the virtual network layer, up to the virtual hosts that are executing the application workloads. If you rotate the view until you are looking down at the system from above, you should be able to see the touch points of all these layers to other systems. Logical isolation refers to this top-down view. An entity needs to be able to show that only necessary data flows are allowed through any of these layers that have an interface to another system. For example, at a storage layer, BCS systems should have their storage logically isolated from other systems that are not part of the BCS. At a networking layer, there should be no communications channels that allow the BCS to talk to any other system that is not controlled. At a virtual machine level, there should be logical isolation between VMs. As you "look down" through the computing stack, you should only see interface points that are controlled and locked down to a least-privilege position. To allow for implementation of this isolation, the ESZ concept has been introduced so that systems of the same trust level can be placed into their own ESZ and the controls placed on the zone.

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 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 such as DRAM. 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 Shared Cyber Infrastructure.

As this class of vulnerability is specifically about processes executing side by side on the same CPU or memory chips in a SCI environment, the risk of these vulnerabilities is being mitigated in CIP-005-7 by either:

- Declaring the VCAs that share compute resources (CPU, memory) or are within the same ESZ or ESP with a BES Cyber System as associated PCAs which will require they meet the same security requirements (high water marking); or
- Configuring the virtualization infrastructure to place VCA's of differing impact or trust levels into differing ESZ's 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.

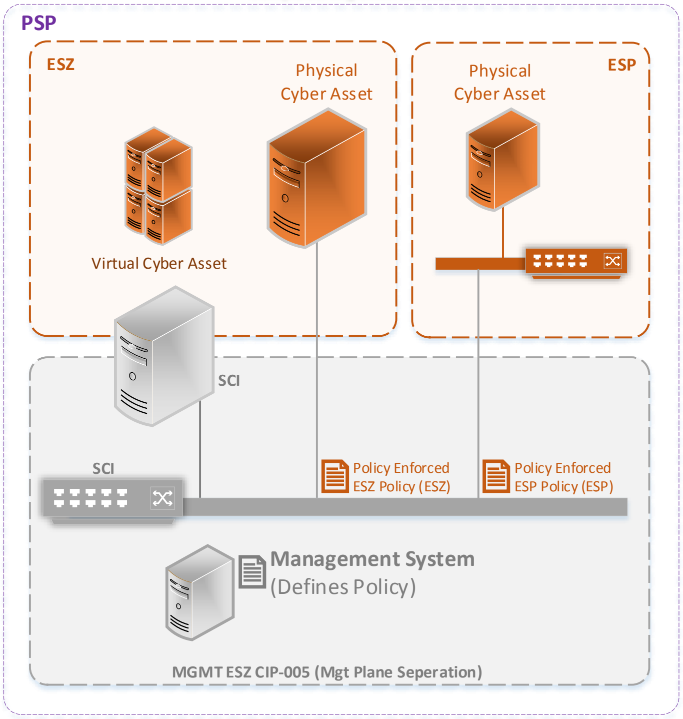
Hybrid Virtual/Physical Scenarios with ESP/ESZ's

Typically, virtualized environments will use the ESZ structure and physical asset environments will use the ESP structure for meeting CIP-005 requirements. However, numerous scenarios will include a hybrid of both virtual and physical Cyber Assets. An entity could configure their SCI so that both virtual and physical Cyber Assets are in the same ESZ to reduce the number of zones required to implement the new concepts. The following series of diagrams illustrates some hybrid scenarios.

Hybrid ESP/ESZ Inside of a Single PSP

In this scenario, a virtual Cyber Asset and physical Cyber Asset are shown with logical isolation (ESZ) provided by SCI using a policy enforced ESZ. Another physical Cyber Asset is show using an ESP for logical isolation. In this case, the same SCI is used to provide both the equivalent EAP functionality and logical isolation (ESP) via a policy enforced ESZ. Note that the management plane of the SCI resides within its own ESZ.

ESP/ESZ Hybrid Model


PSP
ESZ
Physical Cyber Asset
Physical Cyber Asset
ESP
Virtual Cyber Asset
SCI
SCI
Policy Enforced ESZ Policy (ESZ)
Policy Enforced ESP Policy (ESP)
Management System (Defines Policy)
MGMT ESZ CIP-005 (Mgt Plane Seperation)

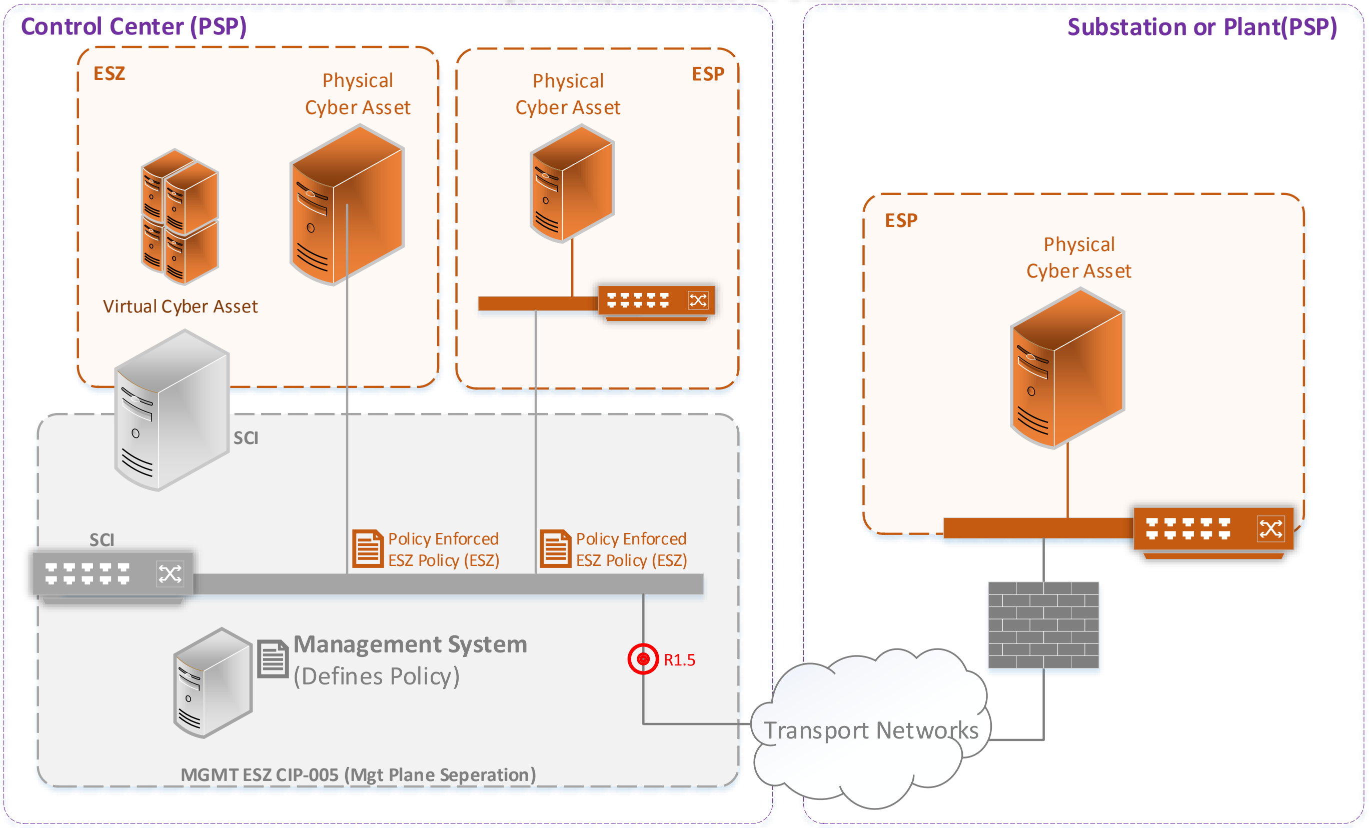
Hybrid ESP/ESZ across PSP's

In the left portion of this scenario (the Control Center), a virtual Cyber Asset and physical Cyber Asset are shown with logical isolation provided by SCI using a policy enforced ESZ. Another physical Cyber Asset is shown using an ESP for logical isolation. In this case, the same SCI is used to provide both the equivalent EAP functionality and logical isolation (ESP) via a policy enforced ESZ. Note that the malicious communications detection required for the Control Center (R1.5) is being provided by the SCI.

In the right portion of the drawing (Substation or Plant), another physical Cyber Asset is shown where its logical isolation is provided by an ESP. A physical firewall (EACS/SCI) is used to provide the logical isolation.

Note that the management plane of the SCI resides within its own ESZ.

Hybrid ESZ/ESP Across PSP's Model



Combined ESZ for Cyber Assets and Virtual Cyber Assets

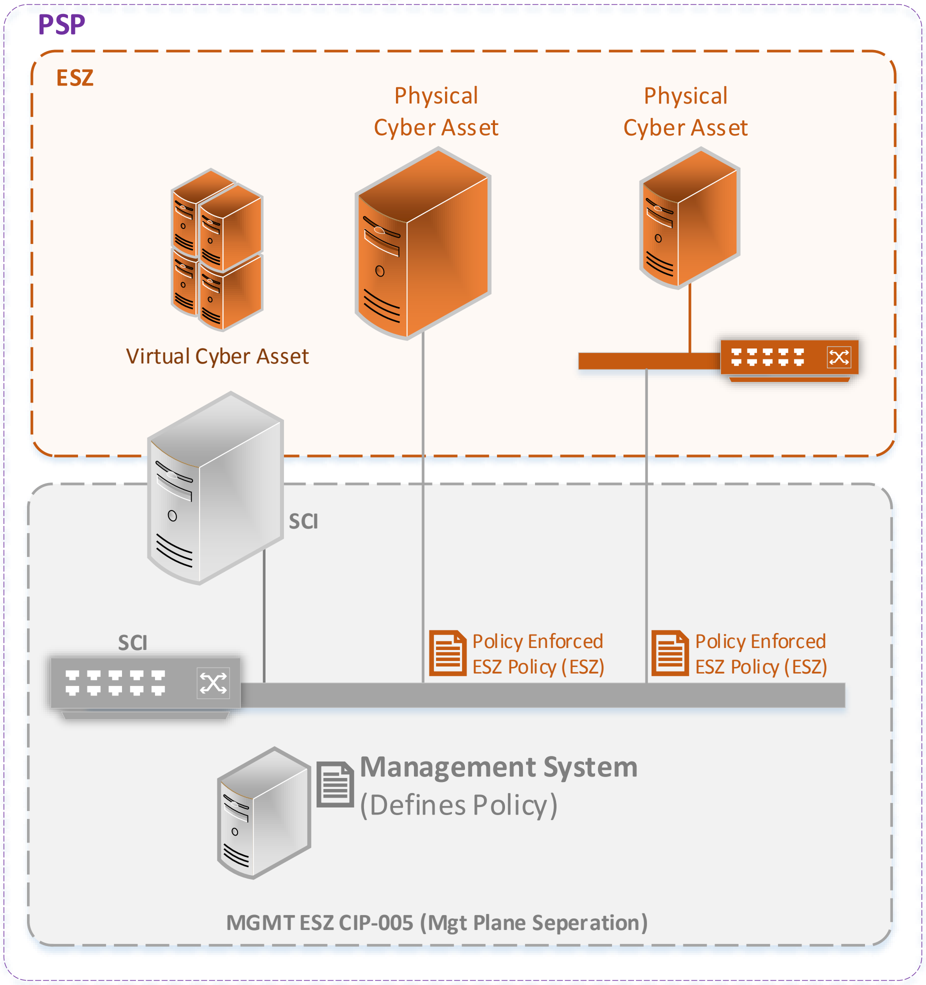
In this drawing, virtual and physical Cyber Assets are located within a single ESZ where the logical isolation is provided by the SCI. Previously, this would have required a physical firewall to both provide an EAP and logical isolation. In the left portion of the drawing, a VCA and supporting SCI are being utilized where logical isolation (ESZ) is being provided by the SCI using a policy enforced ESZ. The SCI is also enforcing logical isolation for the physical Cyber Assets by configuring the appropriate policy enforced ESZ. This effectively converts what would have been an ESP for the physical Cyber Assets into a similar policy enforced ESZ used by the virtual Cyber Asset where traditional EAP functionality is now provided by the SCI. This has the following advantages:

a) Access control for this environment is centrally managed and a single policy for the ESZ is enforced for virtual and physical Cyber Assets.

b) For applicable Control Centers, it alleviates the need for a multiple ESPs or ESZs and methods to detect malicious communication for network traffic between them within the Control Center.

Note that the management plane of the SCI resides within its own ESZ.

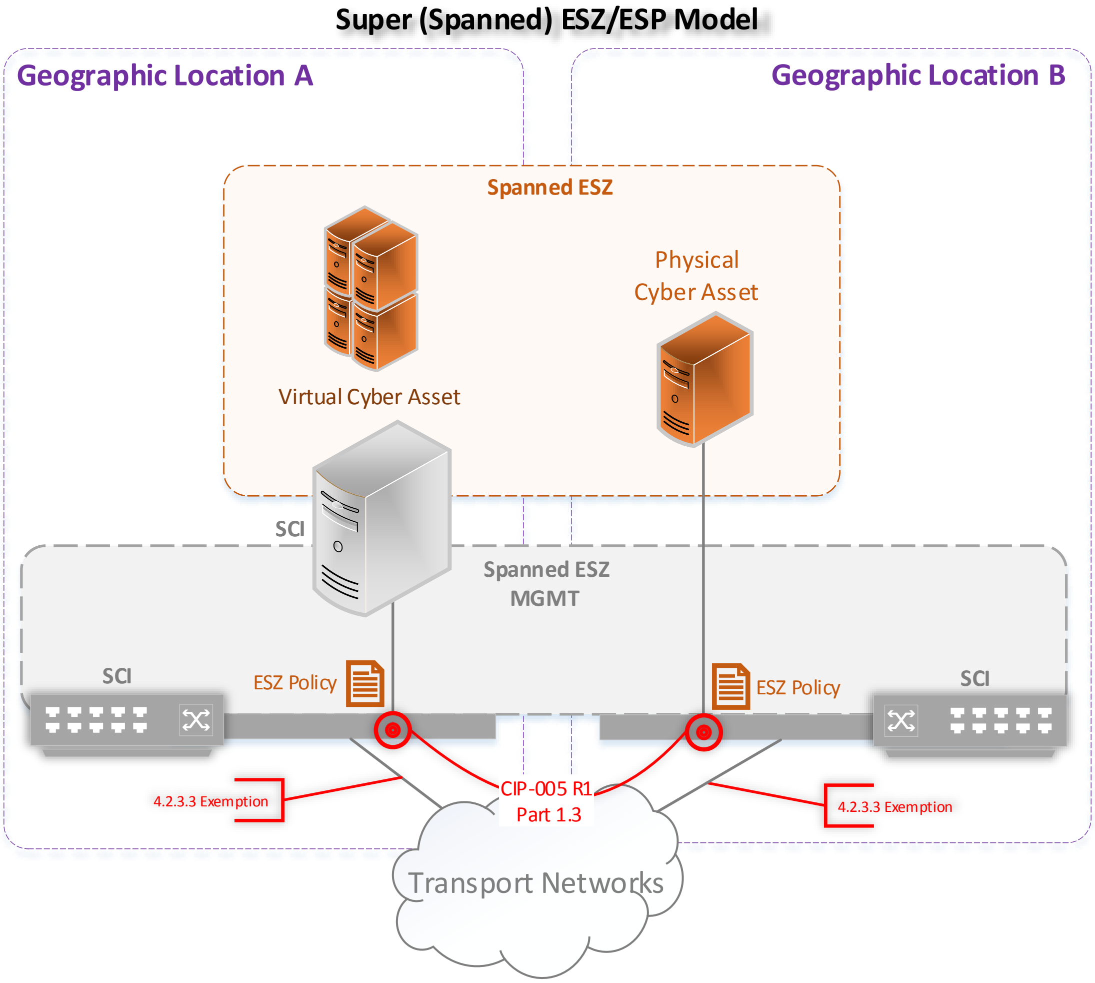
ESZ Replaces ESP Model



Spanned ESZ Model

In this model, two different geographic locations are connected by a transport network. The transport network is utilized to span the SCI and the same logical isolation (a single ESZ) between these two locations. In one location, a virtual Cyber Asset running on SCI is within the policy enforced ESZ. In the other location, a physical Cyber Asset is within the same ESZ that is spanned between the two locations. This allows the exact same ESZ policy to be enforced across the locations as well. Note that malicious communication detection is not required for network traffic within the same ESZ, even if it flows between the locations. However, the network data traversing the transport network must still be protected under CIP-005-7 Requirement R1.3 or CIP-012-1 where applicable.

Note that as the same management plane of the SCI is spanned between locations, the ESZ protecting the SCI management plane is also spanned as well.



EACMS/PACS Glossary Terms

As technologies and attacks have advanced and become more complex, entities are becoming more interested in partnering with outside and government security services. These includes services like NERC's Cyber Security Risk Information Sharing Program (CRISP), Cybersecurity for the Operational Technology (OT) Environment (CYOTE), and those of other external security services and internal monitoring centers. Going forward, these types of service and providers will become more cloud based. Security service providers have visibility into emerging threats and trends that come through their extensive collections of information. Analysis of this information can then be shared more broadly, improving the overall cybersecurity posture and reliability of the BES through early detection of compromise and the ability to monitor for threats and indicators of compromise (IOCs) at machine speeds.

Under the current body of CIP Standards, using the types of services that include electronic access monitoring data (not involved in the actual control of electronic access) may bring all Cyber Assets involved into scope as an EACMS. This may discourage or even preclude entities from using these services based on the Cyber Asset level requirements of an EACMS. These limitations affect personnel, physical security, patching, baselines, and other requirements that focus on a Cyber Asset. Entities may also be discouraged from providing and correlating security events across enterprise and control networks, even though most cyber-attacks against control systems today enter through business networks. There is great value in correlating security events seen across enterprise and OT networks that may be discouraged or precluded through the "M" in EACMS growing to include much an enterprise's other monitoring only Cyber Assets.

The cyber systems that do perform electronic access control will remain as they are today in the standards. Those cyber systems, such as firewalls and routers with ACLs and other systems that do perform access control and actively protect the networks to which BES Cyber Systems are connected should not change. However, the monitoring and logging aspect of EACMS presents a different risk of information protection. The creation of two different defined terms recognizes this. EACS represents those systems that do control electronic access and will essentially be a drop-in replacement for today's EACMS.

The parallel also exists for PACS where a differentiation between systems that control physical access can be made with systems that only monitor or log access information.

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

External Routable Connectivity (ERC) is used in the CIP standards for different purposes, including:

1. Establishing when EAPs are required
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 (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 a geographically distributed BES. Many requirement parts should be scoped based on whether the system has ERC for the following reasons:

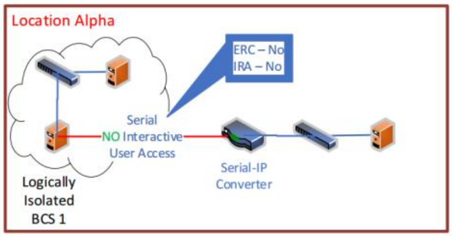
- The risk is increased for systems with ERC. The requirement should apply to those systems with an increased attack surface and risk due to their connectivity/accessibility.
- Locations that have legacy connectivity such as non-routable serial leased circuits should not have to increase their level 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.

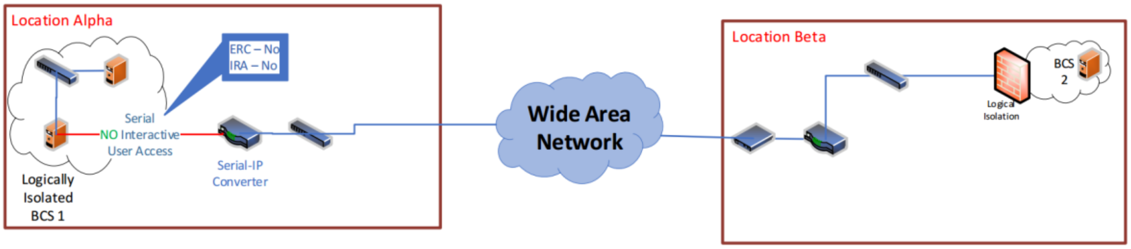
One issue with the ERC definition from the V5TAG transfer document has been that of BES Cyber Assets (BCA) that only speak non-routable protocols over a serial port. These BCAs are not in an ESP and therefore can be considered to not have ERC because it is defined in terms of an "associated ESP." These BCAs, however, can have Interactive Remote Access through an upstream serial-to-IP conversion. 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 R2. Appropriate controls (CIP-005 R2) are now required for these Interactive Remote Access sessions without regard to ERC.

The following diagrams show different scenarios and whether ERC and/or IRA exist in the situation.

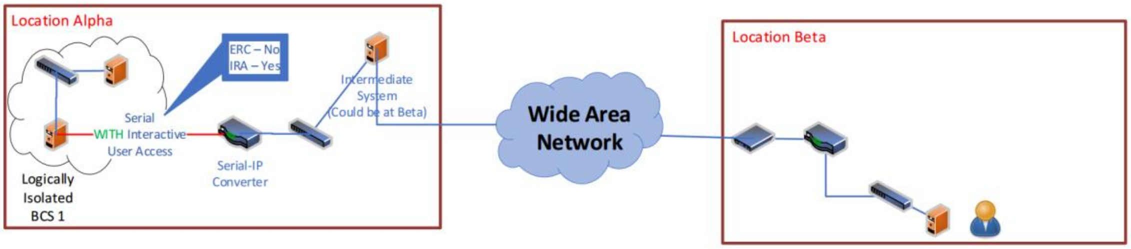
Local Serial Data



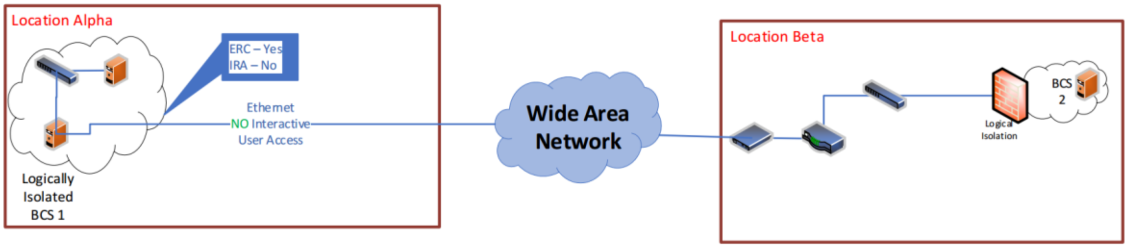
Remote Serial Data w/IP Conv



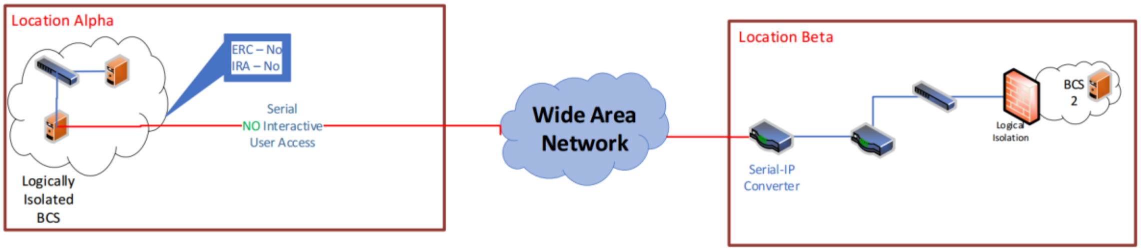
Remote Serial Access



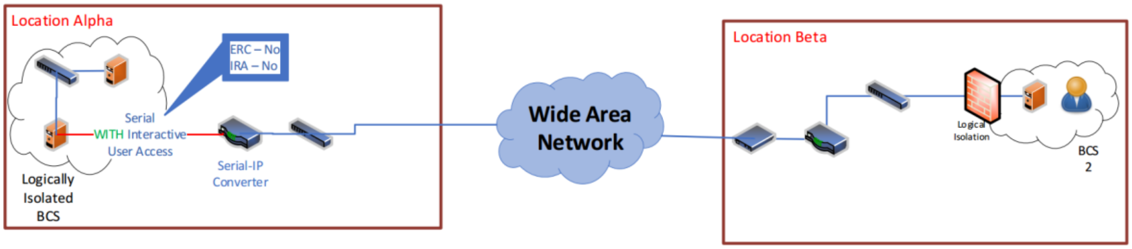
Remote Routable Data



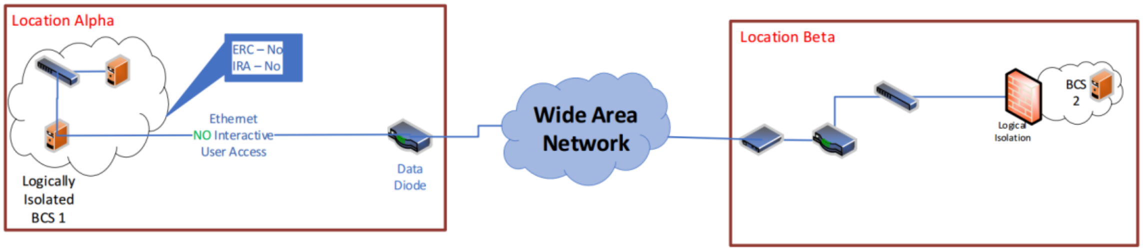
Remote Serial Data



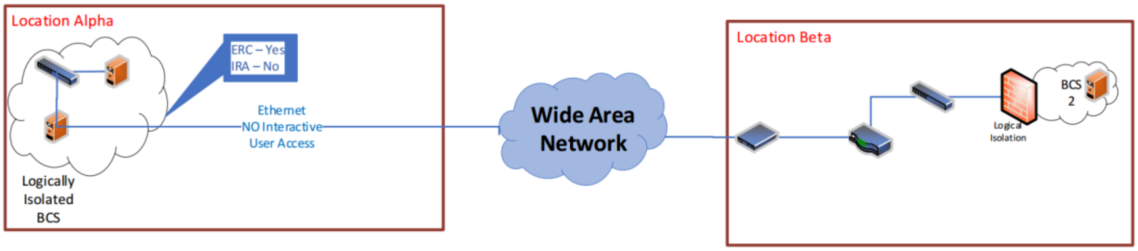
Remote Serial Access From Another BCS



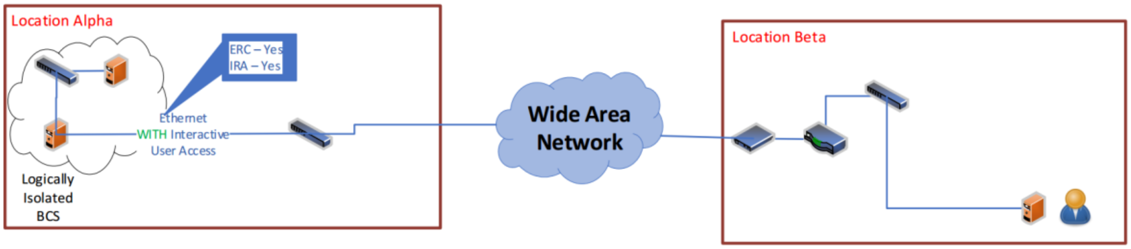
Diode



Remote Routable Data



Remote Routable Access



Assets with Multiple Classifications (PCA, EACS, IS, SCI, etc.)

The definitions created in support of the CIP Standards have historically included overlap. In this current version of CIP-005-7, the definition of PCA is updated with conforming changes that include Virtual Cyber Assets, as well as those that share computer resources with BES Cyber Systems. Additional definitions such as Shared Cyber Infrastructure and Virtual Cyber Asset will add to the possibility of additional instances of assets or systems meeting multiple definitions, such as EACS that are also PCAs, or SCI that is also an EACS.

These definitions are used in both the Applicable Systems column as well as within the language of the Requirement. 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 EACS definition, requirements that apply to either definition would be applicable.

Requirement R1

General Considerations for Requirement R1

> **Requirement R1:** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Logical Isolation. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

Rationale

Requirement 1 is designed to implement various forms of logical isolation between systems in different ESPs or ESZs and have the access controlled between them. The ESP model continues unchanged as the 1.2 requirement part moves to an objective-based requirement that the EAP model can meet. However, requirement R1 allows for other models (such as zones and zero-trust models) that can also meet the objective in 1.2. For the ESZ concept, the requirement has new requirement parts to cover what systems can reside in what zones to mitigate the risks of “mixed trust” environments that are possible on shared infrastructure.

Requirement R1 Part 1.1

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems connected to a network via routable protocol and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	All applicable systems shall reside within one or more defined ESPs or ESZs.	An example of evidence may include, but is not limited to, a list of all ESPs or ESZs with all uniquely identifiable applicable systems.

Rationale

This requirement part gives the entity the option to use either the ESP model or the ESZ model for implementing the logical isolation of the applicable systems. For a discussion of the ESZ option, see the rationale for the ESZ and SCI definitions above, the General Considerations section above, as well as the diagram depicting various ESZ configurations in Attachment 1.

Requirement R1 Part 1.2

Part	Applicable Systems	Requirements	Measures
1.2	Electronic Security Perimeters and Electronic Security Zones created in Part 1.1.	Require inbound and outbound logical access permissions, including the reason for granting access, and deny all other logical access by default. Excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	An example of evidence may include, but is not limited to, architectural diagrams that detail how network communication is limited and a list of rules (firewall, access control lists, software defined policies, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.

Rationale

Removal of Electronic Access Point (EAP):

The SDT is proposing the removal of EAP as a definition, therefore, the applicability of CIP-005-7 R1.2 also needs to change. The SDT chose ESP(s) and ESZ(s) created in Part 1.1 as the Applicable Systems where Registered Entities are required to apply the inbound and outbound access controls to replace the term EAP. By doing so, current Access Control Lists in-place for established EAPs continue to serve the same purpose and should remain compatible with this requirement part. Also see the discussion of the ESZ and EAP terms above.

Requirement Parity within ESZ to establish security level and address “mixed trust”:

The SDT chose to establish the ESZ at a single trust level by assigning the same set of requirements throughout the CIP standards to systems that reside within an ESZ. The goal of this is to minimize the ability of an attacker to pivot from one system to another within an ESZ. An example of this is the threat of an attacker escaping a virtual machine to access the host hypervisor and other Virtual Machines (VMs). If there were systems within the ESZ that were not held to the same trust level, compromising those systems could be potentially easier, which would allow an attacker to pivot and compromise systems to the higher impact targets within the same ESZ.

For example, if a Protected Cyber Asset (PCA) within an ESZ is not subject to the same CIP-004 requirements for personnel accessing the PCA as it is for the BES Cyber Systems within the same ESZ, it could be used as a “pivot” for allowing unauthorized access to the BES Cyber Systems within the ESZ.

In future formal postings of the CIP standards with conforming changes applied, the affected requirements will have “hosted on SCI” phrasing within the “Applicable Systems” column. These requirements establish a single security or trust level for the applicable systems within an ESZ. Each of these requirements serves a specific security need, and if missing, would reduce the security level of the hosted virtualized systems potentially reducing the security level of the associated BCS.

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 the 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. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions.

Requirement R1 Part 1.3

Part	Applicable Systems	Requirements	Measures
1.3	Electronic Security Zone or Electronic Security Perimeter that spans more than one geographic location containing: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems	Protect the confidentiality and integrity of the data traversing communication networks and data communication links used to extend an applicable ESP or ESZ, excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	Evidence may include, but is not limited to, architecture documents detailing the methods used to mitigate the risk of unauthorized disclosure. Examples include physical protection and the points where encryption initiates and terminates.

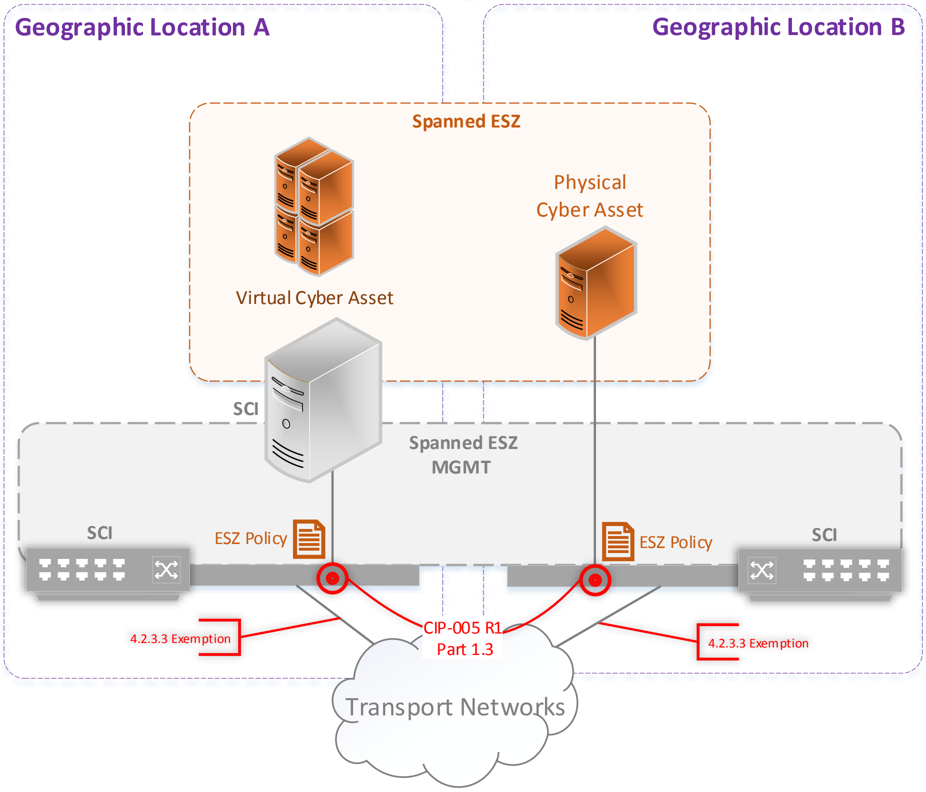
Rationale

Part 1.3 is a new requirement intended to protect the confidentiality and integrity of data flowing between an entity's facilities when that data is contained within a single ESP or ESZ that spans more than one geographic location, commonly referred to as a 'Super ESP.'

One of the issues with the ESP construct carried forward into the logical isolation model is the situation where entities have BES Cyber Systems that include components at separate locations. For example, if an entity has a need to replicate data at high speed between two databases in two different geographic locations to improve the resilience and reliability of BES Cyber Systems, the entity may have issues with the 4.2.3.2 exclusion in the standards that exempts the network and communications gear that is "between discrete ESPs." If the protocol is not routable then no ESP can be created. The entity needs to be able to have a "Super-ESP" that can span more than one location.

The ESP model, along with the 4.2.3.2 exclusion within the CIP standards applicability does not lend itself to this construct. As technology evolves, there will be many more instances where a BES Cyber System may need to span locations. Traditionally this situation could be addressed by installing an EAP at each site as an ESP boundary that would then allow the communications equipment between the sites to be subject to the exemption if routable protocols are used.

Super (Spanned) ESZ/ESP Model



The 'Super ESP' construct has been addressed with a new exclusion and a new requirement (CIP-005 R1.3). The new exclusion in 4.2.3.3 allows Cyber Assets associated with communication networks and data communication links used to extend an ESP or ESZ to more than one geographic location to be exempt from the standard since many of these Cyber Assets may be owned by carriers. However, the new R1.3 in CIP-005 requires that data over this exempted communication be protected to preserve its integrity and confidentiality, with the exception of time sensitive protection functions.

The exemption within this requirement part for "Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012" does not exempt it from protection under the CIP standards as it is covered by CIP-012. The intent of this exemption is to keep any issues with CIP-012 compliance from becoming a CIP-005 issue as well if the two control centers in question also have the "Super-ESP" implemented.

Requirement R1 Part 1.4

Part	Applicable Systems	Requirements	Measures
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI •	Perform authentication when establishing Dial-up Connectivity with applicable systems, per system capability.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

Rationale

CIP-005-7, Part 1.4 reinforces that dial-up connectivity should perform authentication whenever possible so that the BES Cyber System is not directly accessible with only a phone number. It has been changed to apply to virtualized environments as well and update the TFE requirements to the “per system capability” language.

Requirement R1 Part 1.5

Part	Applicable Systems	Requirements	Measures
1.5	High Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	Have one or more methods for detecting known or suspected malicious routable Internet Protocol (IP) communications to or from ESPs or ESZs.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

Rationale

CIP-005-7 requirement 1.5 reflects the retirement of the term EAP in favor of utilizing the terms ESP and ESZ. The intent of requirement 1.5 is to detect known or suspected malicious communications at the ESP or ESZ boundaries.

The use of "to or from" in the requirement is to solidify where the detection should take place, which is at the boundary of the ESP or ESZ and not communications within the ESP or ESZ. The use of the phrase “routable Internet Protocol (IP) communications” is intended to eliminate internal storage transport protocols including, but not limited to Fibre Channel, iSCSI, and InfiniBand from the scope of this requirement as well as serial communications.

The change in the applicable systems is to provide both forward and backward compatibility within the same requirement.

Requirement R1 Part 1.6

Part	Applicable Systems	Requirements	Measures
1.6	Shared Cyber Infrastructure that hosts High Impact BES Cyber Systems Shared Cyber Infrastructure that hosts Medium Impact BES Cyber Systems	Management systems may only share CPU, memory, and ESZ or ESP with other management systems and the management plane.	Examples of evidence may include, but is not limited to, documentation that includes the configuration of systems that enforce authentication and isolation such as: • Logically isolated out-of-band network infrastructure configuration (ACL, VLAN, VXLAN, MPLS) • Physical isolated out-of-band network for dedicated management interfaces, embedded management interfaces • Compute configuration showing the isolation of the management plane resources (e.g., hypervisor, containers)

Rationale

The SDT is proposing a new Requirement, CIP-005-7 Requirement R1, Part 1.6. The purpose of this new Requirement is to separate the management plane of SCI from the data plane.

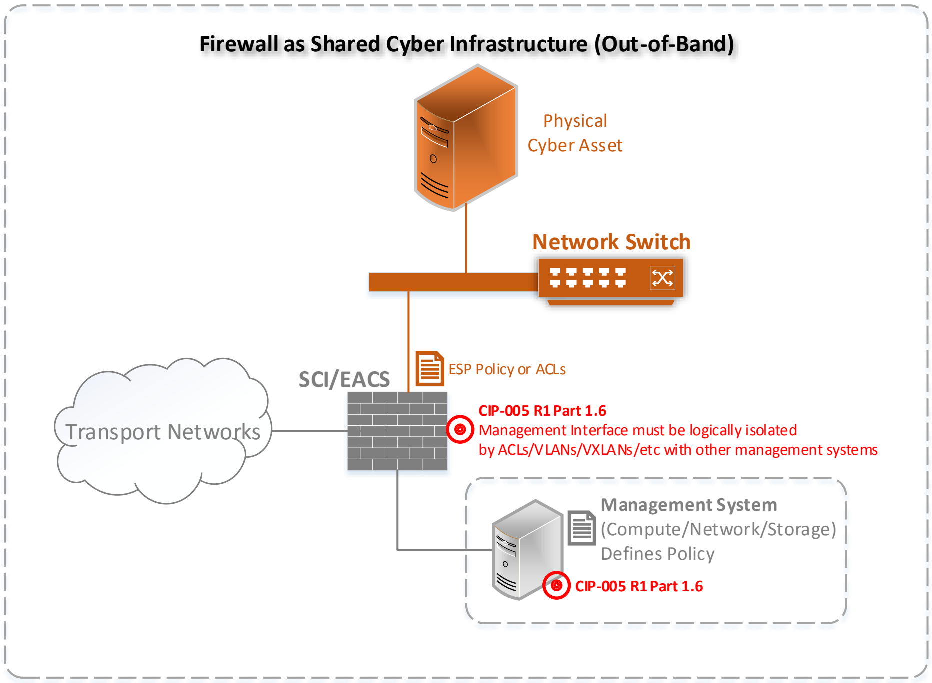
As virtualized servers, networks, switches, firewalls, and storage are logical constructs, controlling access and communications to the management plane of these systems becomes imperative. Access to the management plane (interface, console, etc.) allows users to create, modify, or delete objects or entire infrastructures, or move objects from one zone or network to another. Therefore, administrative level or “management plane” access to the SCI is critical to the security and reliability of the hosted systems. By isolating the management interface of these devices from the larger audience of users that can access the data plane, the threat base is reduced to the group of users with access to the administrative functions.

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. CIP-005 R1.6 will mitigate that issue by bringing the isolation of the management plane into the scope of the CIP standards. This is accomplished by requiring that entities allow management systems to share CPU and memory (e.g. hypervisors) only with other management systems. It also requires that management systems share an ESZ only with other management systems.

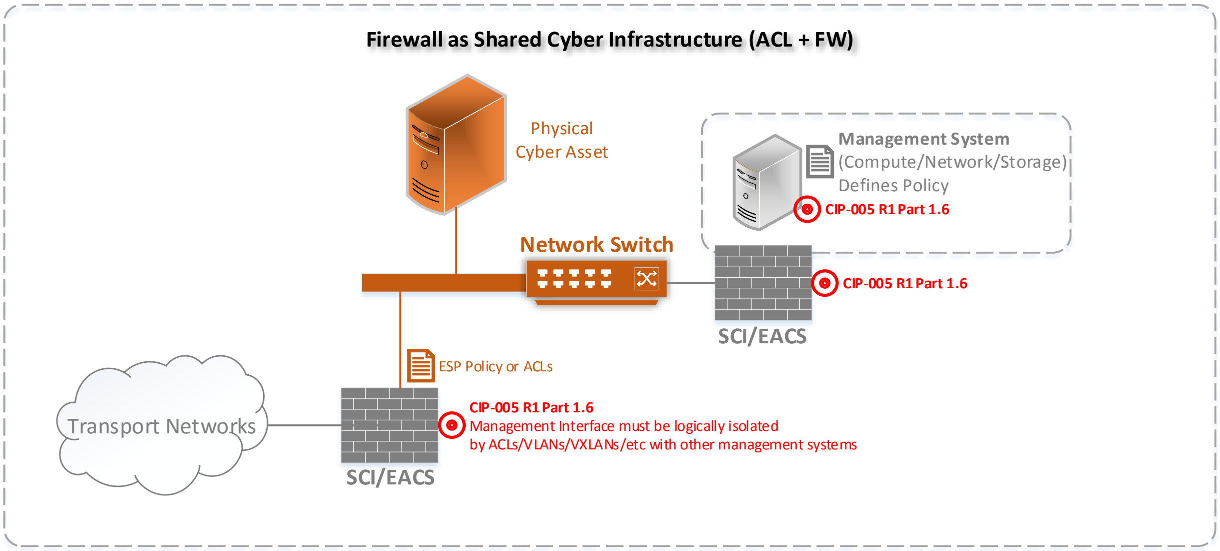
Because hypervisors give us the ability to use affinity rules to determine what VMs use what resources, affinity and anti-affinity rules are a critical part of the isolation solution for management systems hosted on SCI. An affinity rule will ensure a group of virtual machines are only allowed to reside on a group of hypervisors. The use of an anti-affinity rule will ensure another group of VMs cannot reside on the group of hypervisors reserved in the previous affinity rule. While different hypervisors have different methods for achieving this, the idea is the same across all mass market hypervisors.

The statement "or performs logical isolation for an ESZ or ESP" is found within the Shared Cyber Infrastructure definition. This inclusion is intended to ensure that devices that provide logical isolation for an ESZ or ESP have protection for the associated management systems (management plane). This inclusion means the management plane of firewalls or network switches that provide logical isolation to an ESP, ESZ, or within Shared Cyber Infrastructure now fall within scope of R1.6. It is not intended for network switches that are part of a system and are not providing logical isolation between ESPs or ESZs. The following diagrams outline numerous options that help to further clarify the intent of R1.6 as it applies to firewalls and network switches that implement ESP or ESZ logical isolation.

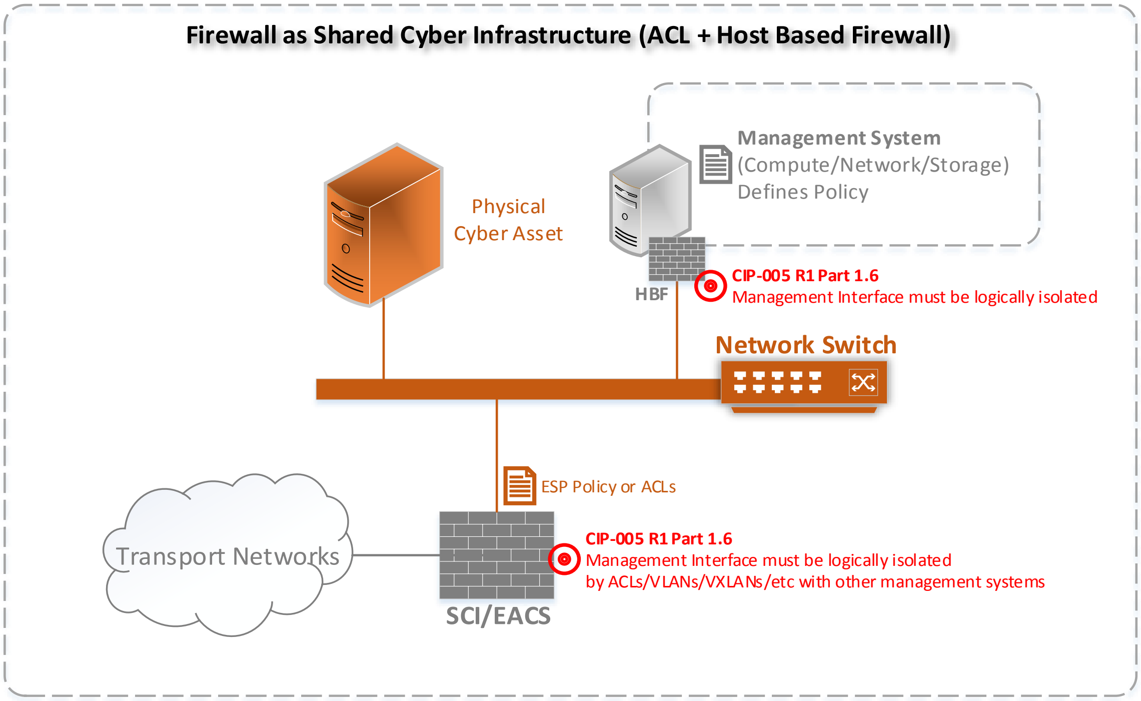
The option below shows the typical out-of-band management of the SCI by putting the management system on a separate interface. This keeps the management system in an ESP or ESZ not shared with other non-management systems. The network switch is not used to perform logical isolation.


Firewall as Shared Cyber Infrastructure (Out-of-Band)
Physical Cyber Asset
Network Switch
ESP Policy or ACLs
SCI/EACS
Transport Networks
CIP-005 R1 Part 1.6
Management Interface must be logically isolated by ACLs/VLANs/VXLANs/etc with other management systems
Management System (Compute/Network/Storage) Defines Policy
CIP-005 R1 Part 1.6

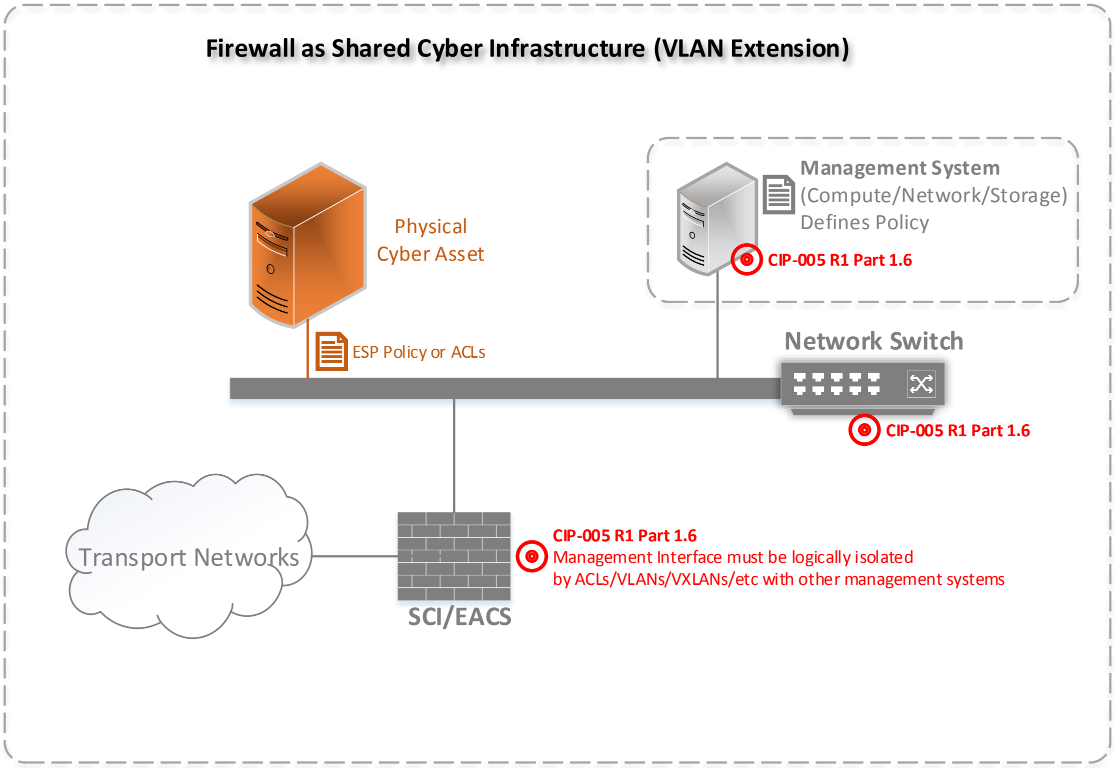
The option below depicts a management system that is located at a site with one network switch. Some sort of logical isolation is required so that the management system is not visible to those with access to the Cyber Asset on the same switch. Another firewall is implemented here to put the management system in an ESP or ESZ separate from the other Cyber Assets. The network switch is not used for logical isolation.


Firewall as Shared Cyber Infrastructure (ACL + FW)
Physical
Cyber Asset
Management System
(Compute/Network/Storage)
Defines Policy
CIP-005 R1 Part 1.6
Network Switch
CIP-005 R1 Part 1.6
SCI/EACS
ESP Policy or ACLs
Transport Networks
CIP-005 R1 Part 1.6
Management Interface must be logically isolated
by ACLs/VLANs/VXLANs/etc with other management systems
SCI/EACS

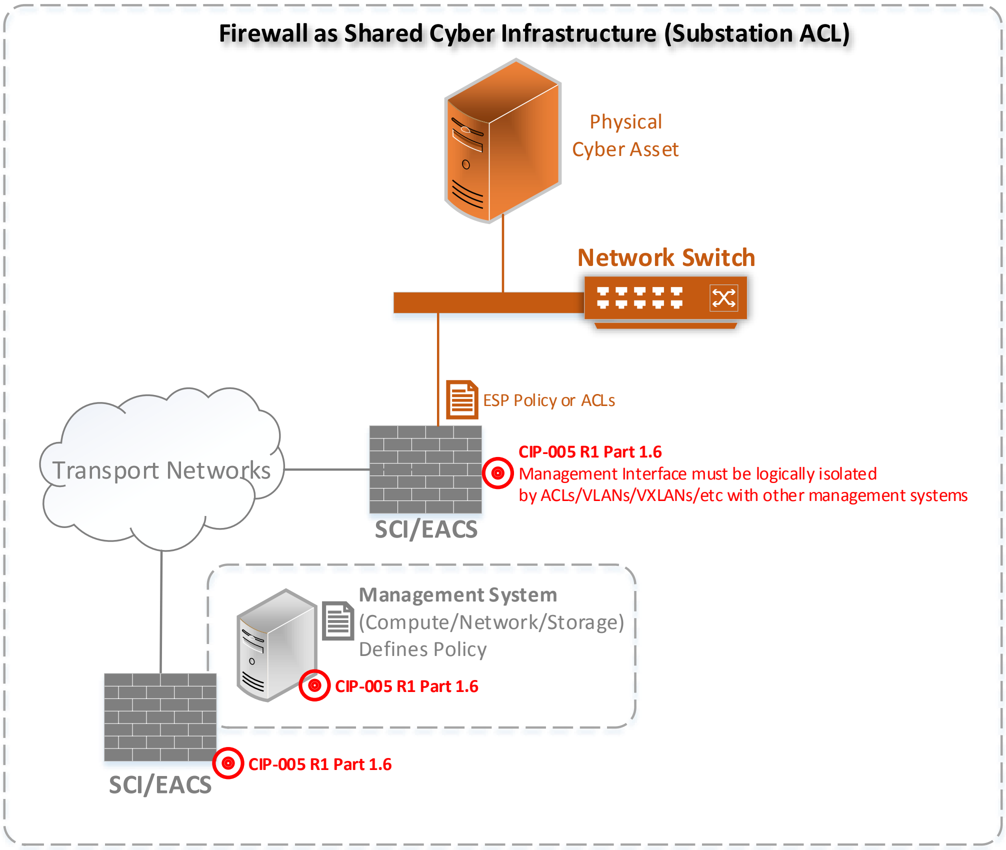
In the option below, the same situation exists, but instead of a separate physical firewall a host based firewall is used on the management system to logically isolate it.


Firewall as Shared Cyber Infrastructure (ACL + Host Based Firewall)
Management System
(Compute/Network/Storage)
Defines Policy
Physical
Cyber Asset
HBF
CIP-005 R1 Part 1.6
Management Interface must be logically isolated
Network Switch
ESP Policy or ACLs
Transport Networks
CIP-005 R1 Part 1.6
Management Interface must be logically isolated
by ACLs/VLANs/VXLANs/etc with other management systems
SCI/EACS

In the option below, the management system is connected to the network switch and the switch is used for the logical isolation. Virtual LANs (VLANs) are configured in the switch along with ACL's in the firewall in order to implement the two different ESZs to isolate the management system. The network switch itself now also becomes SCI and it's management plane now must be in the management ESZ as well.


Firewall as Shared Cyber Infrastructure (VLAN Extension)
Physical Cyber Asset
ESP Policy or ACLs
Management System (Compute/Network/Storage) Defines Policy
CIP-005 R1 Part 1.6
Network Switch
CIP-005 R1 Part 1.6
Transport Networks
SCI/EACS
CIP-005 R1 Part 1.6
Management Interface must be logically isolated by ACLs/VLANs/VXLANs/etc with other management systems

In the option below, a centralized management system is depicted at another location. ACLs are implemented in the intervening firewalls (SCI) such that the access to the management plane of those firewalls is only allowed to the centralized management system.


Firewall as Shared Cyber Infrastructure (Substation ACL)
Physical Cyber Asset
Network Switch
ESP Policy or ACLs
CIP-005 R1 Part 1.6
Management Interface must be logically isolated by ACLs/VLANs/VXLANs/etc with other management systems
Transport Networks
SCI/EACS
Management System (Compute/Network/Storage) Defines Policy
CIP-005 R1 Part 1.6
SCI/EACS
CIP-005 R1 Part 1.6

Requirement R2

R2. Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-7 Table R2 –Remote Access Management* for all remote access that originates from outside of any of the entities' ESP's or ESZ's containing high or medium impact BES Cyber Systems or associated SCI. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*

General Considerations for Requirement R2.

Rationale

This requirement added wording for ESZs containing either high or medium impact BES Cyber Systems or associated SCI to provide the equivalent logical protections for remote access that existed before. The wording for existing ESPs was retained for backward compatibility purposes to CIP-005-6.

Previously, the applicability of the remote access was included within the definition of IRA, which included access that did not originate from within another of the entity's ESPs. That applicability has been removed from the definition (see discussion of IRA above) and placed within the requirement so that the definition does not need to change when the applicability of a requirement that uses it changes.

Requirement R2 Part 2.1

Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: • PCA • SCI Medium Impact BES Cyber Systems with IRA and their associated: • PCA • SCI	Ensure that Interactive Remote Access is through an Intermediate System that is not inside an applicable ESP or ESZ.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.

Rationale

The Applicable Systems section of this requirement was updated to include SCI associated with high and medium impact BES Cyber Systems. This was done to ensure that same safeguards for remote access methods and technologies exist for the applicable SCI as the high and medium impact BES Cyber Systems and associated PCA's being hosted on that SCI. Backwards compatibility with CIP-005-6 is maintained for entities that do not currently use SCI.

For Medium Impact BES Cyber Systems, the Applicable Systems wording was updated from "with External Routable Connectivity" to "with IRA". This was done to cover serial connectivity associated IRA for those applicable systems without External Routable Connectivity (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. Please refer to the section of this document entitled "External Routable Connectivity (ERC) and Interactive Remote Access (IRA)."

The inclusion of the wording for "associated SCI" is intended to target the management plane of the associated SCI. This is to ensure that the management plane of the SCI being used to support BES Cyber Systems is also protected in an equivalent manner.

Backwards compatibility with CIP-005-6 is maintained except in the above situations.
The requirement language itself was simplified. Note that the definitions of IRA and IS have been updated. Please note that the definition of IRA was changed to include serial communications connections. This change maintains backwards compatibility with CIP-005-6 except where serial connectivity is being used for IRA.
The required location of an Intermediate System was within the definition previously. The definition of IS has been simplified and its required location (not inside an applicable ESP or ESZ) is now within the requirement rather than the definition.

Requirement R2 Part 2.2

Part	Applicable Systems	Requirements	Measures
2.2	Intermediate Systems associated with High Impact BES Cyber Systems. Intermediate Systems associated with Medium Impact BES Cyber Systems.	Protect the confidentiality and integrity of Interactive Remote Access between the client and the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

Rationale

The Applicable *Systems* was changed to IS from high or medium BES Cyber Systems and associated PCA's. This change better reflects that this requirement is associated with the IS itself.

The requirement was changed from a specific technical based requirement for encryption to an objective based requirement to protect the IRA session. The proposed language of this requirement takes into account the possibility that other equally effective methods could be developed and deployed. This also prevents outdated encryption methods from being utilized.

The changed requirement is backwards compatible with the CIP-005-6 except where outdated encryption methods have been used.

Requirement R2 Part 2.3

Part	Applicable Systems	Requirements	Measures
2.3	Intermediate Systems associated with High Impact BES Cyber Systems. Intermediate Systems associated with Medium Impact BES Cyber Systems.	Require multi-factor authentication to IS.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

Rationale

The Applicable Systems was changed to IS from high or medium BES Cyber Systems and associated PCA's. This change better reflects that this requirement is associated with the IS itself. Note that serial connection-based IRA is now included due to the IRA definition change. The requirement itself was not changed.

The changed requirement is backwards compatible with the CIP-005-6 except where serial connection-based IRA is being utilized.

Requirement R2 Parts 2.4 – 2.5

Part	Applicable Systems	Requirements	Measures
2.4	High Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI •	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.
2.5	High Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI •	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

Rationale

The Applicable Systems section was changed to include associated SCI, PACS hosted on SCI, EACS hosted on SCI, EAMS hosted on SCI. This change is needed due to the possibility of “differing trust levels” when these types of assets utilize the same SCI. Please refer to the section in this document entitled ‘Shared infrastructure and “Mixed Trust” Risks‘. In summary, this change is intended to mitigate the risk associated with “side channel” based attack vectors where it could be possible to compromise one virtual cyber asset and then subsequently access the any other virtual cyber asset running on the same SCI. Also note that serial connection-based IRA is now included due to the change in the definition of IRA.

The inclusion of the wording for "associated SCI" is intended to target the management plane of the associated SCI. This is to ensure that the management plane of the SCI being used to support BES Cyber Systems 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.

Note that the changes to applicable systems only applies to those virtual cyber assets hosted on the same SCI. These changes don't apply where SCI is not utilized. These changed requirements are backwards compatible with the CIP-005-6 except where SCI is currently being utilized and where serial connection-based IRA is being utilized.

Requirement R2 Part 2.6

Part	Applicable Systems	Requirements	Measures
2.6	Intermediate Systems that are hosted on SCI and are associated with High Impact BES Cyber Systems. Intermediate Systems that are hosted on SCI and are associated with Medium Impact BES Cyber Systems.	IS may only share CPU, memory, and ESZ or ESP with other IS.	An example of evidence may include, but is not limited to, documentation that includes the following: configuration showing that the CPU and memory can only be shared with other IS.

Rationale

This is a new requirement that only applies to IS hosted on SCI. This new requirement is proposed due to the possibility of:

- IS being used by external parties outside of the entities such as vendors; and,
- IS being accessible to external connections outside of the entity such as entity support staff utilizing IRA across an internet connection to support a remote site.

Please refer to the section in this document entitled "Shared infrastructure and "Mixed Trust" Risks" and the subsequent discussion on "affinity". The new requirement is for "affinity" and a separate ESZ.

In summary, this new requirement is intended to mitigate the risk associated with "side channel" based attack vectors where it could be possible to compromise the IS from an external source and then subsequently access the any other virtual Cyber Asset running on the same SCI.

As this is a new requirement only applies to IS hosted on SCI, it is backwards compatible with the CIP-005-6 except where SCI is currently used.

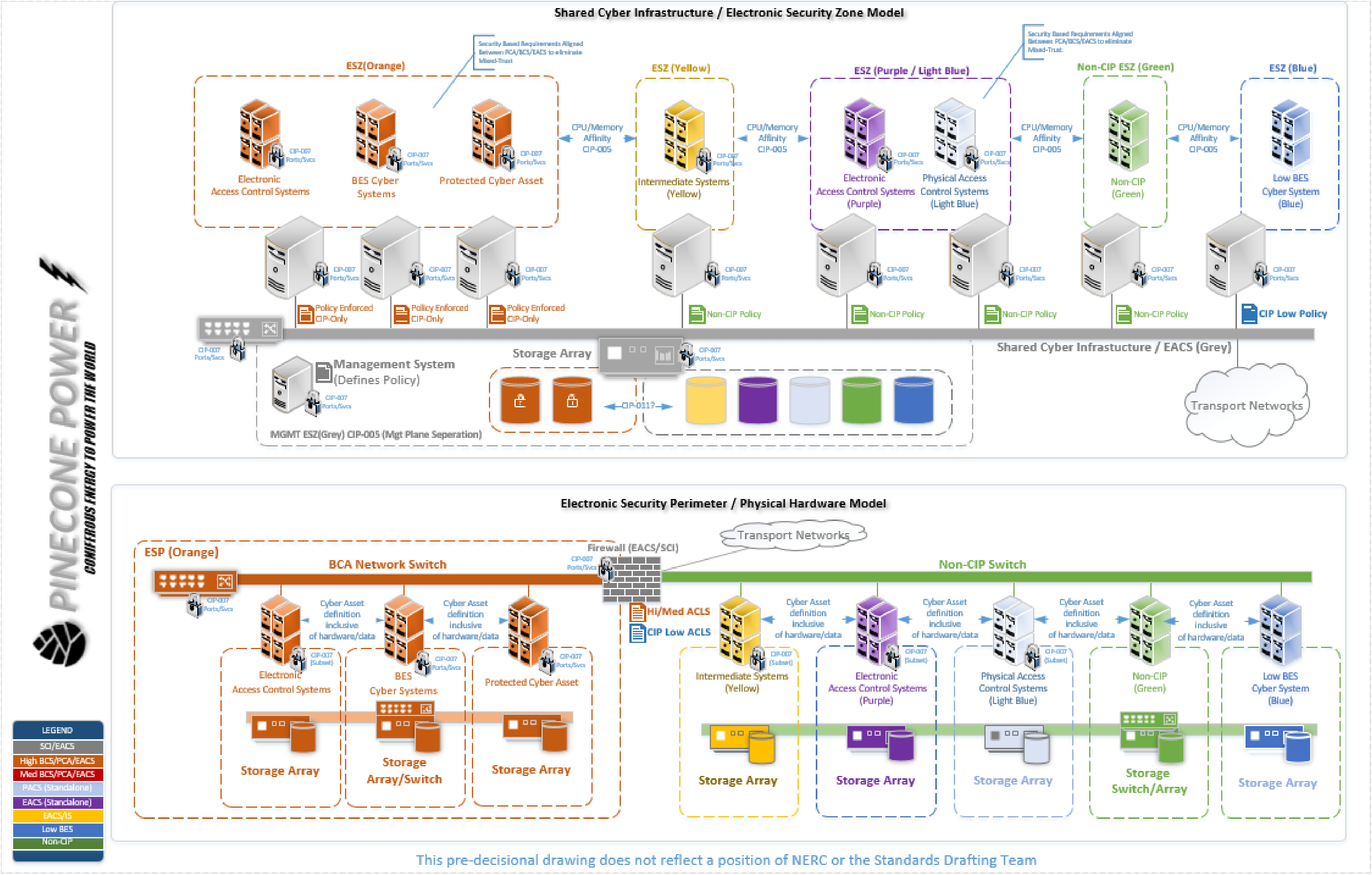
Appendix 1 – ESZ's

This section contains a diagrams for a fictional utility company ("Pinecone Power").

Figure 1 is used to show a virtualized scenario at the top of diagram and contrasts it with a typical physical hardware model on the lower half. The virtualized scenario fully utilizes the ESZ concept and has practically every kind of system hosted within the environment. The color coding (see legend at lower left) depicts the categorization of various components. The diagram shows the different ESZs that would be required and the affinity rules that would be needed between them such that systems of different security levels would not share the same hypervisor with systems in other zones.

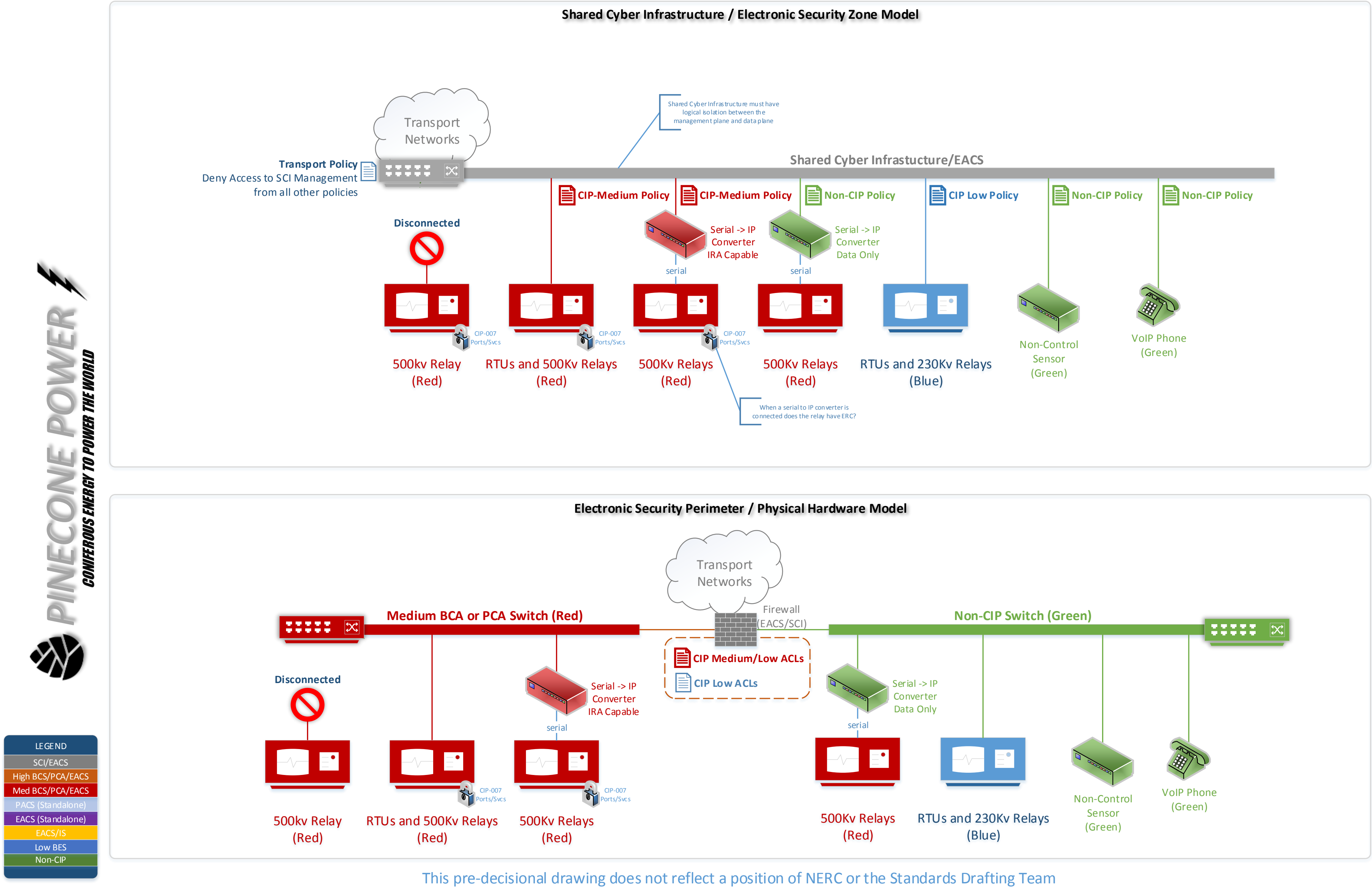
Figure 2 is used to describe substation and plant hybrid virtualization scenarios. It also uses the ESZ concept to secure devices connected to the switch.

Figure 1


Shared Cyber Infrastructure / Electronic Security Zone Model
Security Based Requirements Aligned Between PCA/BCS/EACS to eliminate Mixed-Trust
ESZ(Orange)
Electronic Access Control Systems
BES Cyber Systems
Protected Cyber Asset
CIP-007 Ports/Svcs
CPU/Memory Affinity CIP-005
ESZ (Yellow)
Intermediate Systems (Yellow)
ESZ (Purple / Light Blue)
Electronic Access Control Systems (Purple)
Physical Access Control Systems (Light Blue)
Non-CIP ESZ (Green)
Non-CIP (Green)
ESZ (Blue)
Low BES Cyber System (Blue)
Policy Enforced CIP-Only
Non-CIP Policy
CIP Low Policy
Shared Cyber Infrastructure / EACS (Grey)
Management System (Defines Policy)
Storage Array
CIP-011?
MGMT ESZ(Grey) CIP-005 (Mgt Plane Seperation)
Transport Networks
Electronic Security Perimeter / Physical Hardware Model
ESP (Orange)
BCA Network Switch
Firewall (EACS/SCI)
Hi/Med ACLS
CIP Low ACLS
Non-CIP Switch
Cyber Asset definition inclusive of hardware/data
CIP-007 (Subset)
Electronic Access Control Systems
BES Cyber Systems
Protected Cyber Asset
Storage Array
Storage Array/Switch
Intermediate Systems (Yellow)
Electronic Access Control Systems (Purple)
Physical Access Control Systems (Light Blue)
Non-CIP (Green)
Low BES Cyber System (Blue)
Storage Switch/Array
PINECONE POWER
CONIFEROUS ENERGY TO POWER THE WORLD
LEGEND
SCI/EACS
High BCS/PCA/EACS
Med BCS/PCA/EACS
PACS (Standalone)
EACS (Standalone)
EACS/IS
Low BES
Non-CIP

This pre-decisional drawing does not reflect a position of NERC or the Standards Drafting Team

Figure 2


Shared Cyber Infrastructure / Electronic Security Zone Model
Transport Networks
Shared Cyber Infrastructure must have logical isolation between the management plane and data plane
Transport Policy
Deny Access to SCI Management from all other policies
Shared Cyber Infrastucture/EACS
CIP-Medium Policy
CIP-Medium Policy
Non-CIP Policy
CIP Low Policy
Non-CIP Policy
Non-CIP Policy
Disconnected
Serial -> IP Converter IRA Capable
Serial -> IP Converter Data Only
serial
serial
CIP-007 Ports/Svcs
CIP-007 Ports/Svcs
CIP-007 Ports/Svcs
500kv Relay (Red)
RTUs and 500Kv Relays (Red)
500Kv Relays (Red)
500Kv Relays (Red)
RTUs and 230Kv Relays (Blue)
Non-Control Sensor (Green)
VoIP Phone (Green)
When a serial to IP converter is connected does the relay have ERC?
Electronic Security Perimeter / Physical Hardware Model
Transport Networks
Medium BCA or PCA Switch (Red)
Firewall (EACS/SCI)
Non-CIP Switch (Green)
CIP Medium/Low ACLs
CIP Low ACLs
Disconnected
Serial -> IP Converter IRA Capable
serial
Serial -> IP Converter Data Only
serial
CIP-007 Ports/Svcs
CIP-007 Ports/Svcs
500kv Relay (Red)
RTUs and 500Kv Relays (Red)
500Kv Relays (Red)
500Kv Relays (Red)
RTUs and 230Kv Relays (Blue)
Non-Control Sensor (Green)
VoIP Phone (Green)
LEGEND
SCI/EACS
High BCS/PCA/EACS
Med BCS/PCA/EACS
PACS (Standalone)
EACS (Standalone)
EACS/IS
Low BES
Non-CIP

This pre-decisional drawing does not reflect a position of NERC or the Standards Drafting Team

Appendix 2 - 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.

Requirement R2:
See Secure Remote Access Reference Document (see remote access alert).

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)

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.

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.