NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2016-02

Modifications to CIP Standards

Virtualization and other Technology Innovations

RELIABILITY | ACCOUNTABILITY




Presenters

- Jay Cribb, Southern Company
- Steve Brain, Dominion Energy
- Forrest Krigbaum, Bonneville Power Administration
- David Revill, GSOC
- Scott Klauminzer, Tacoma Power
- Heather Morgan, EDP Renewables North America LLC

Agenda

- NERC Antitrust Guidelines
- How we got here today
- Overview
- Definitions
- Exemptions
- CIP Exceptional Circumstances
- CIP-004, CIP-005, CIP-006, CIP-007, and CIP-010
- Next Steps
- Q&A

NERC Antitrust Compliance Guidelines

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers, or any other activity that unreasonably restrains competition.

Public Announcement

Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities.

Standards Authorization Request

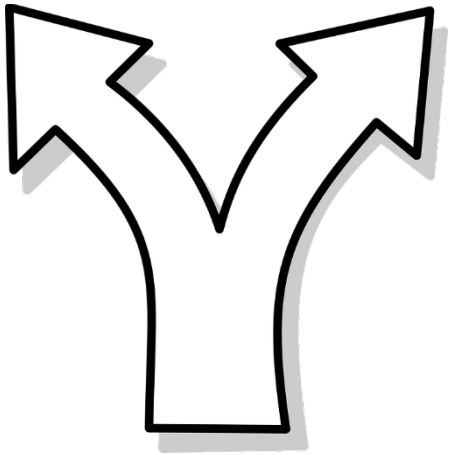
- Consider the Version 5 Transition Advisory Group (V5TAG) issues identified.
  - Virtualization – The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider virtualization for the CIP V5 standards, the associated definitions regarding permitted architecture and the security risks of virtualization technologies.
  - CIP V5TAG Issues for Consideration (Link to Report)

Modified Standards

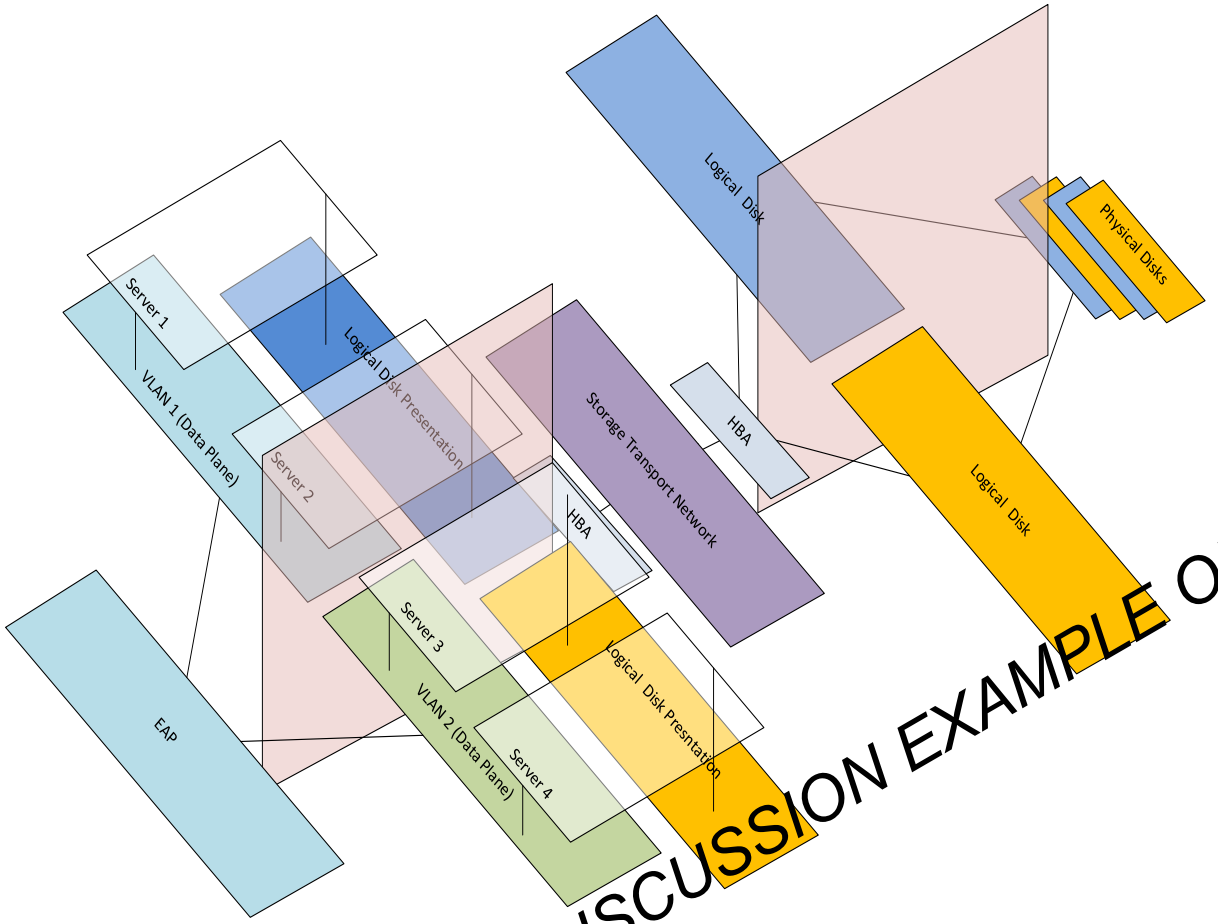
- Updated Definitions
- Standards being modified:
  - CIP-005, CIP-007, CIP-010
  - With conforming changes to the remainder

The Left Path

- *Modify existing or create new definitions for devices and networking to include virtualization concepts*
- *Create additional technical requirements for securing today's version of virtualization technology.*

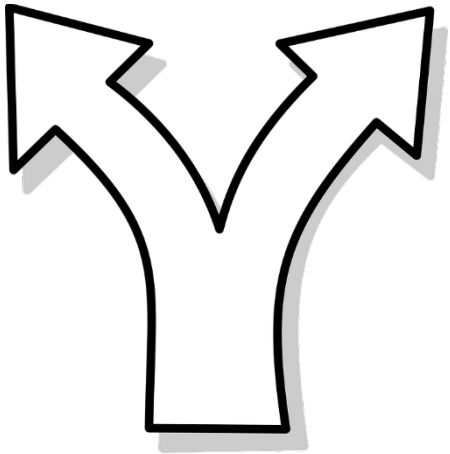


The Left Path



A Fork In The Road

- *Modify existing or create new definitions for devices and networking to include virtualization concepts*
- *Create additional technical requirements for securing today's version of virtualization technology.*



- *More fully embrace the Cyber System concept introduced in Version 5.*
- *Change existing prescriptive technical requirements to be more security objective-based and future-proof.*

Definitions

Group 1 Assets: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Cyber Asset (CA)	Programmable electronic devices, including the hardware, software, and data in those devices.	A programmable electronic device, including the physical or virtual hardware, software, and data in the device.

Definitions

Group 1 Assets: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
BES Cyber System (BCS)	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.	Any combination of hardware (including virtual hardware), software (including application virtualization), and data, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.

Definitions

Group 1 Assets: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
BES Cyber Asset (BCA)	A Cyber Asset 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	Retired

Definitions

Group 1 Assets: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Transient Cyber Asset (TCA)	A 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, • network within an Electronic Security Perimeter (ESP) 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.	A 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 System (PCS) 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 System (BCS), • A BES Cyber System Logical Isolation Zone containing high or medium impact BES Cyber Systems, or • PCS 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.

Definitions

Group 1 Assets: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
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 a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.	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 System, or a Protected Cyber System.

Definitions

Group 1 Assets: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.	Retired

Definitions

Group 1 Assets: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Protected Cyber System (PCS)	N/A	Cyber systems that are able to communicate with a BES Cyber System from within the BES Cyber System's Logical Isolation Zone. The impact rating of Protected Cyber Systems is equal to the highest rated BES Cyber System within the Logical Isolation Zone.

Definitions

Group 1 Assets: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Secure Configuration	N/A	The implemented set of controls supporting the security objectives found within the CIP Reliability Standards where the following text exists within the requirement language: “NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.”

Definitions

Group 2 Systems: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.	The physical border surrounding locations in which BES Cyber Systems or Electronic Access Control Systems reside and for which access is controlled.

Definitions

Group 2 Systems: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Physical Access Control Systems (PACS)	Cyber Assets that control, 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.	Cyber systems 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.

Definitions

Group 2 Systems: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Physical Access Monitoring Systems (PAMS)	N/A	Cyber systems 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.

Definitions

Group 2 Systems: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Electronic Access Control or Monitoring Systems (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.	RETIRED – Proposed Develop EAMS and EACS

Definitions

Group 2 Systems: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Electronic Access Control System (EACS)	N/A	Cyber systems that provide electronic access control to BES Cyber Systems.
Electronic Access Monitoring Systems (EAMS)	N/A	Cyber systems that provide electronic access monitoring of BES Cyber Systems.

Definitions

Group 3 Security Controls: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	Retired

Definitions

Group 3 Security Controls: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Electronic Access Point (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.	Retired

Definitions

Group 3 Security Controls: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Logical Isolation Zone (LIZ)	N/A	A logical security zone created by applying controls to communications to or from BES Cyber Systems and Protected Cyber Systems.

Definitions

Group 3 Security Controls: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
External Routable Connectivity (ERC)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Logical Isolation Zone via a bi-directional routable protocol connection.

Definitions

Group 3 Security Controls: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Intermediate Systems (IS)	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	A system acting as part of the protection applied to a logically isolated BCS that limits external user-initiated access to authorized users.

Definitions

Group 3 Security Controls: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	User-initiated access by a person employing a remote access client to a BES Cyber System or Protected Cyber System from outside of a Logical Isolation Zone. Interactive Remote Access does not include system-to-system process communications or access initiated from an Intermediate System.

CIP Exceptional Circumstances

- CIP Exceptional Circumstances (CEC) language added to:
  - CIP-004

- **CIP-004 R3, Part 3.5** Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed except during CIP Exceptional Circumstances, according to Parts 3.1 to 3.4 within the past seven years.

  - CIP-006

    - **CIP-006 R1, Part 1.8**: Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.
    - **CIP-006 R1, Part 1.9**: Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.

CIP Exceptional Circumstances

- CIP-006
  - Requirement R2:

- **CIP-006 R2:** Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*
- **CIP-006 R2 Part 2.1:** Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter~~, except during CIP Exceptional Circumstances~~.
- **CIP-006 R2 Part 2.2:** Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor~~, except during CIP Exceptional Circumstances~~.

CIP Exceptional Circumstances

- CIP Exceptional Circumstances (CEC) language added to:
  - CIP-007

R4. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to monitor security events to mitigate the risk posed by detectable security incidents that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring*.

CIP Exceptional Circumstances

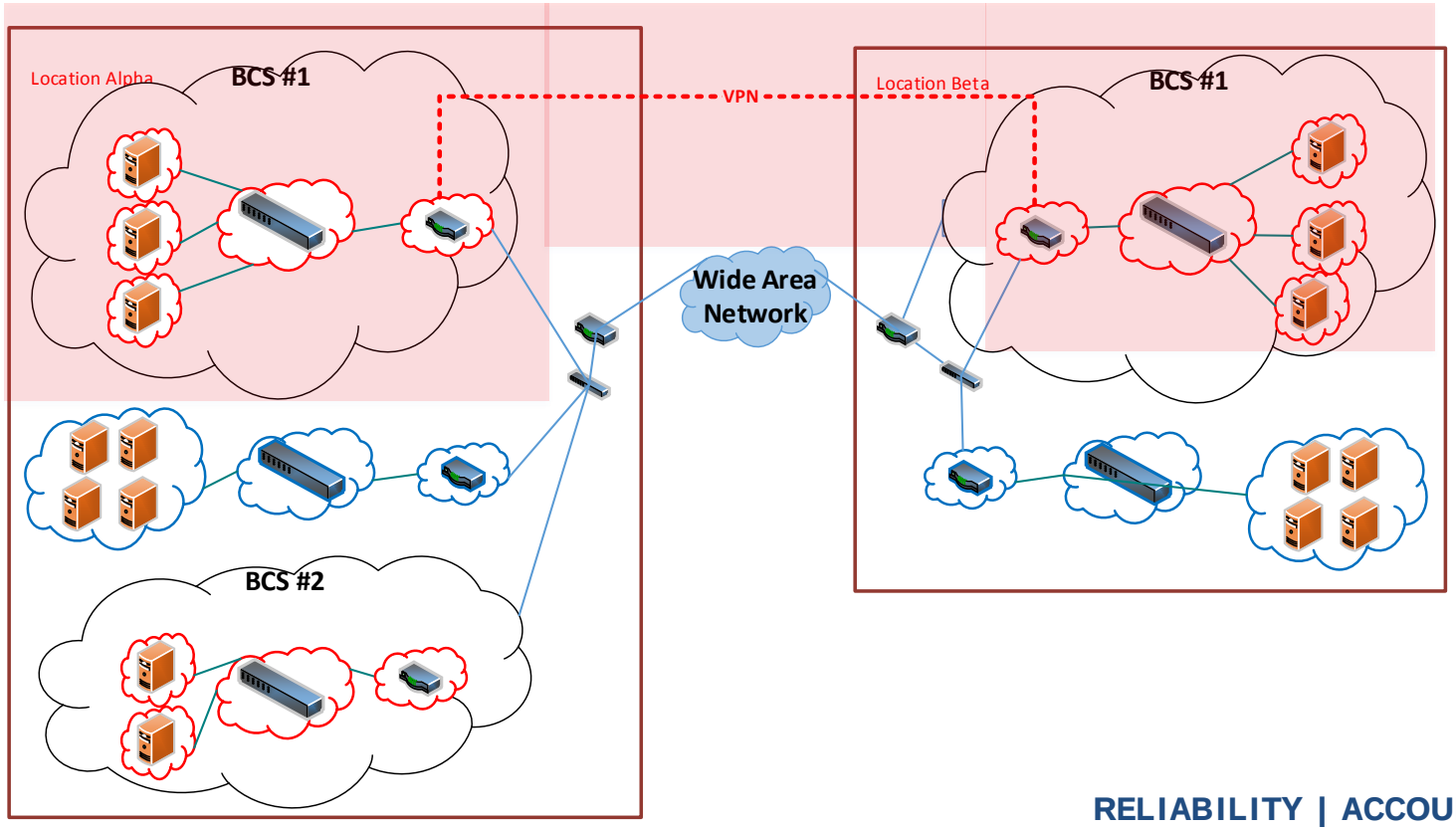
- CIP Exceptional Circumstances (CEC) language added to:
  - CIP-010

1.~~2~~5	High Impact BES Cyber Systems	~~Where technically feasible, f~~For each change that deviates from the ~~existing baseline~~ implemented Secure C~~c~~onfiguration, perform the following, per system capability, except during CIP Exceptional Circumstances: 1.2.1. Prior to implementing any change in the production environment, test the changes in a test environment; or ~~-~~test the changes ~~test the changes~~ in a production environment where the test is performed in a manner that minimizes adverse effects, that models the ~~baseline~~ Secure C~~c~~onfiguration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.2.~~2~~2.3 Document the results of the testing and,~~: and, i~~if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation

Exemption Language

4.2.3.2. Cyber Assets associated with communication networks and data communication links between BES Cyber Systems' Logical Isolation Zones ~~discrete Electronic Security Perimeters~~.

~~4.2.3.2.~~4.2.3.3. Cyber Assets associated with communication networks and data communication links used to extend a Logical Isolation Zone to more than one geographic location.



CIP-004/CIP-006

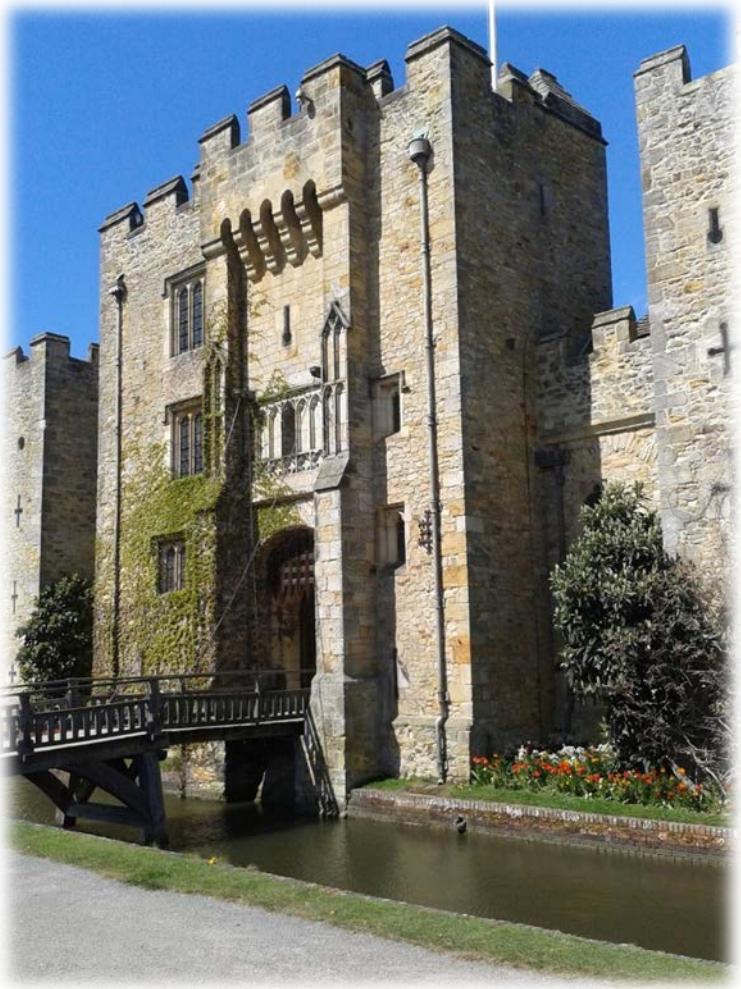
- CIP-004 and CIP-006 were included in this posting as examples to demonstrate what conforming changes to the standards may look like
  - CIP-004 and CIP-006 were also included to demonstrate the SDT's commitment that it is not making substantial changes across all of the standards.
- In CIP-004, SDT added EAMS and PAMS to the applicability. This is currently the only standard where the EAMS and PAMS definitions appear.
- The SDT also added PCS to the applicability in CIP-004. With the new LIZ approach especially with virtualization, the SDT determined that it was necessary to also require access management for those systems that are within the Logical Isolation Zone even if they are not BES Cyber Systems

- **ESP transition to Logical Isolation Zone** – To accommodate advances in network security that go beyond routable protocol address filtering at perimeters, the SDT is proposing a transition to the zone concept while retaining backward compatibility with ESPs.
- **Management plane isolation** – Virtualization allows BES cyber systems with a 15 minute impact to share infrastructure with systems that do not share that time constraint (e.g., a control system and its historian). The SDT has added a new requirement (R3) to bring the management plane and its isolation controls into scope of the CIP standards.

CIP-005 R1, Part 1.1

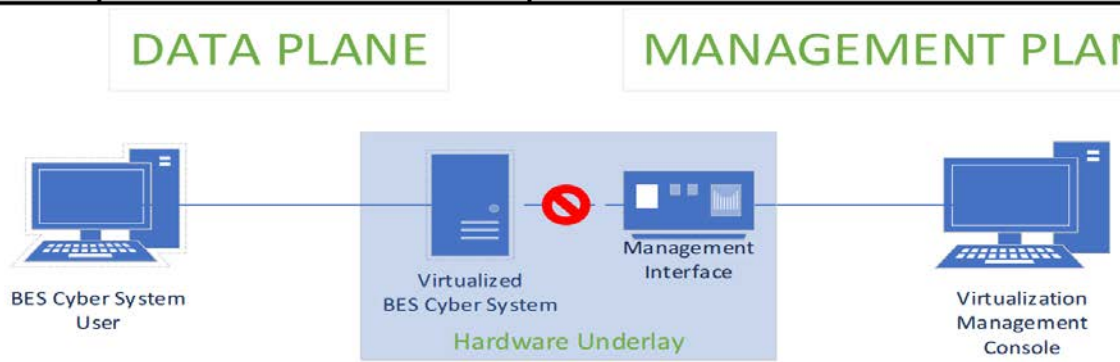
CIP-005-6 Table R1 – Logical Isolation Zones			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Have one or more methods to logically isolate applicable systems, either individually or as a group, by only allowing: 1.1.1. Communication that has documented inbound and outbound access permissions, including the reason for granting access; and 1.2.1. Serial port connectivity such as RS-232 and RS-485. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Evidence may include, but is not limited to, configuration of systems that enforce logical isolation such as network infrastructure configuration (ACL, VLAN, VXLAN, MPLS), compute configuration (e.g., Hypervisor, containers), storage system configuration (e.g., SAN, NAS, DAS).

CIP-005 R1



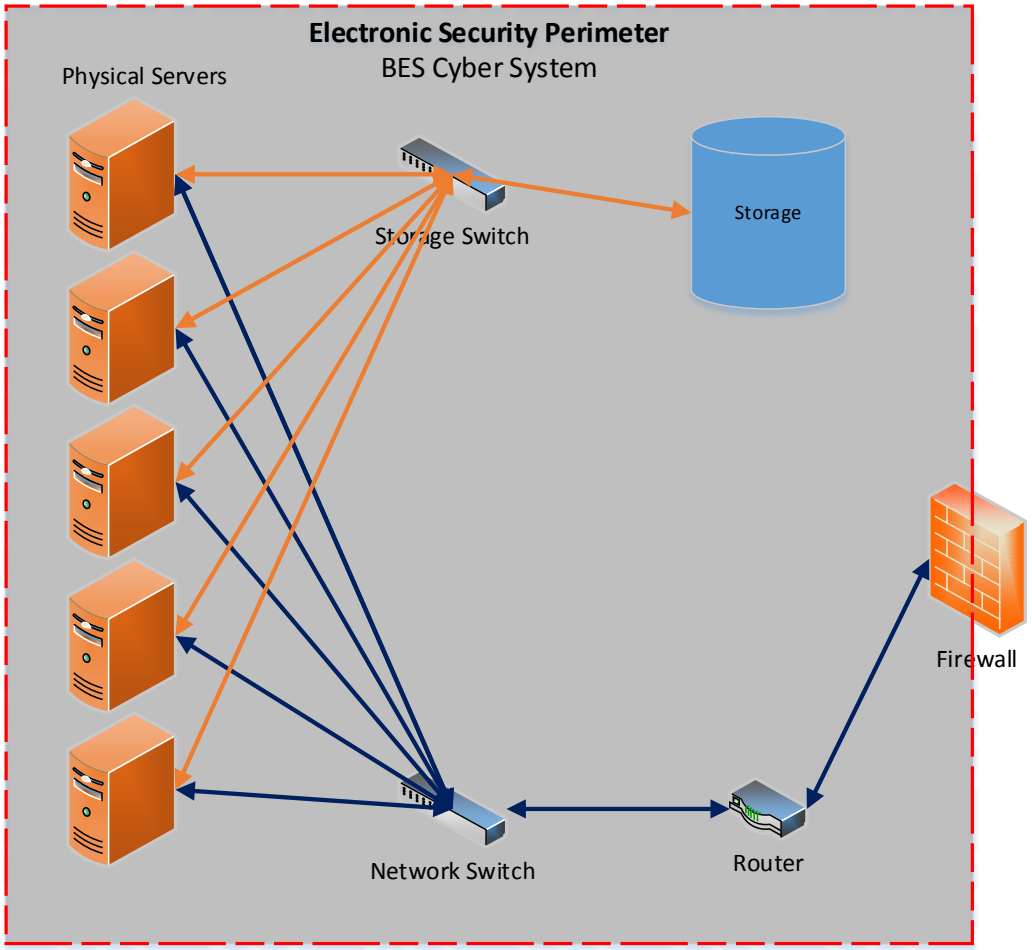
CIP-005 R3

CIP-005-6 Table R3 – Isolation of Management Plane and Data Plane			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACS 2. PCS Medium Impact BES Cyber Systems and their associated PCS: 1. EACS 2. PCS	Have one or more methods per system capability to: 1. Restrict access to the management plane; and 2. Logically isolate the management plane from the data plane.	An example of evidence may include but is not limited to documentation that includes the following: Configuration of systems that enforce authentication and logical isolation such as network infrastructure configuration (ACL, VLAN, VXLAN, MPLS), compute configuration (e.g. Hypervisor, containers), storage system configuration (e.g. SAN, NAS, DAS).



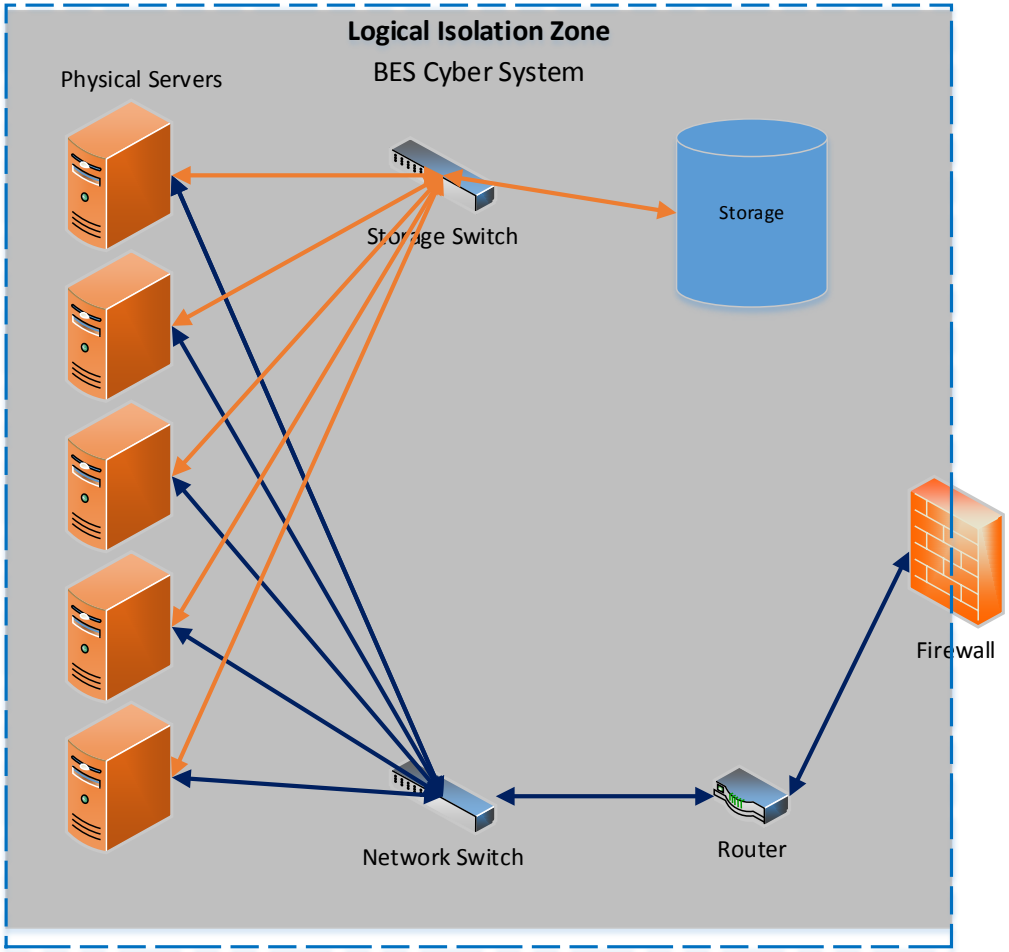
Electronic Security Perimeter

Current Environment



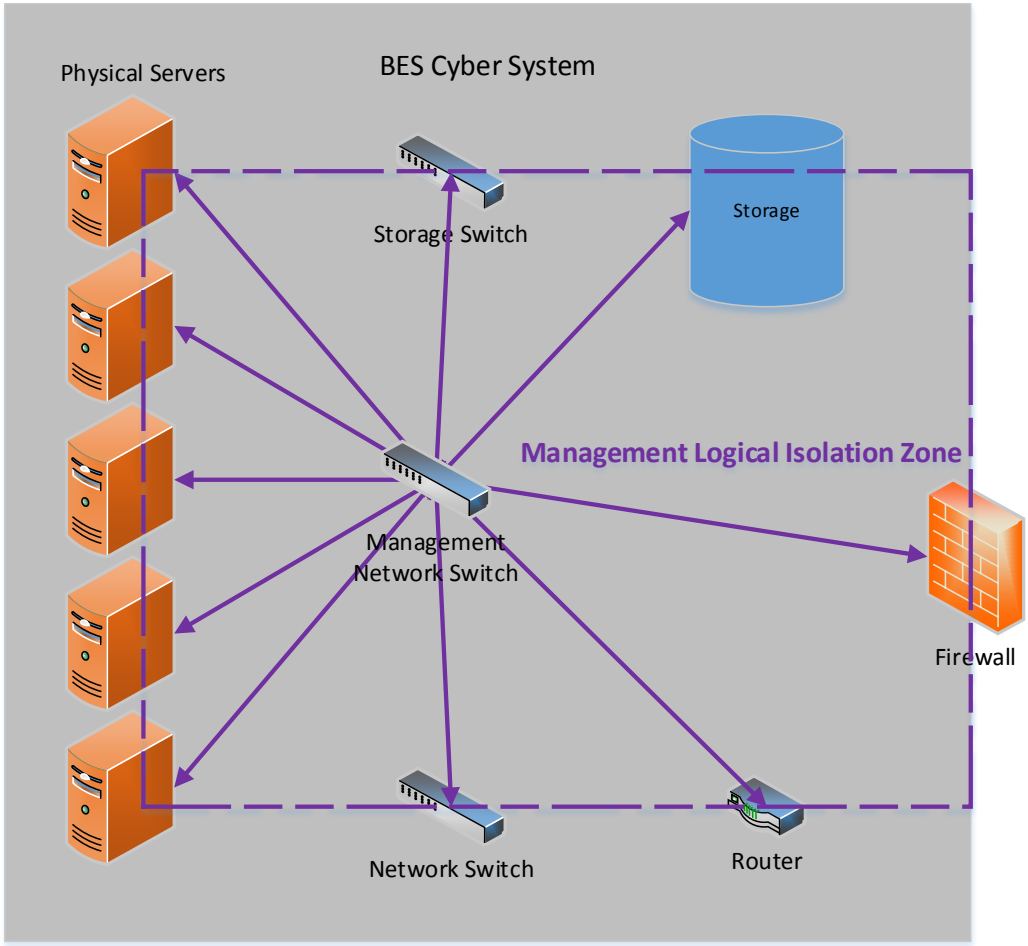
Logical Isolation Zone

Future Environment showing backward compatibility with Logical Isolation Zone only



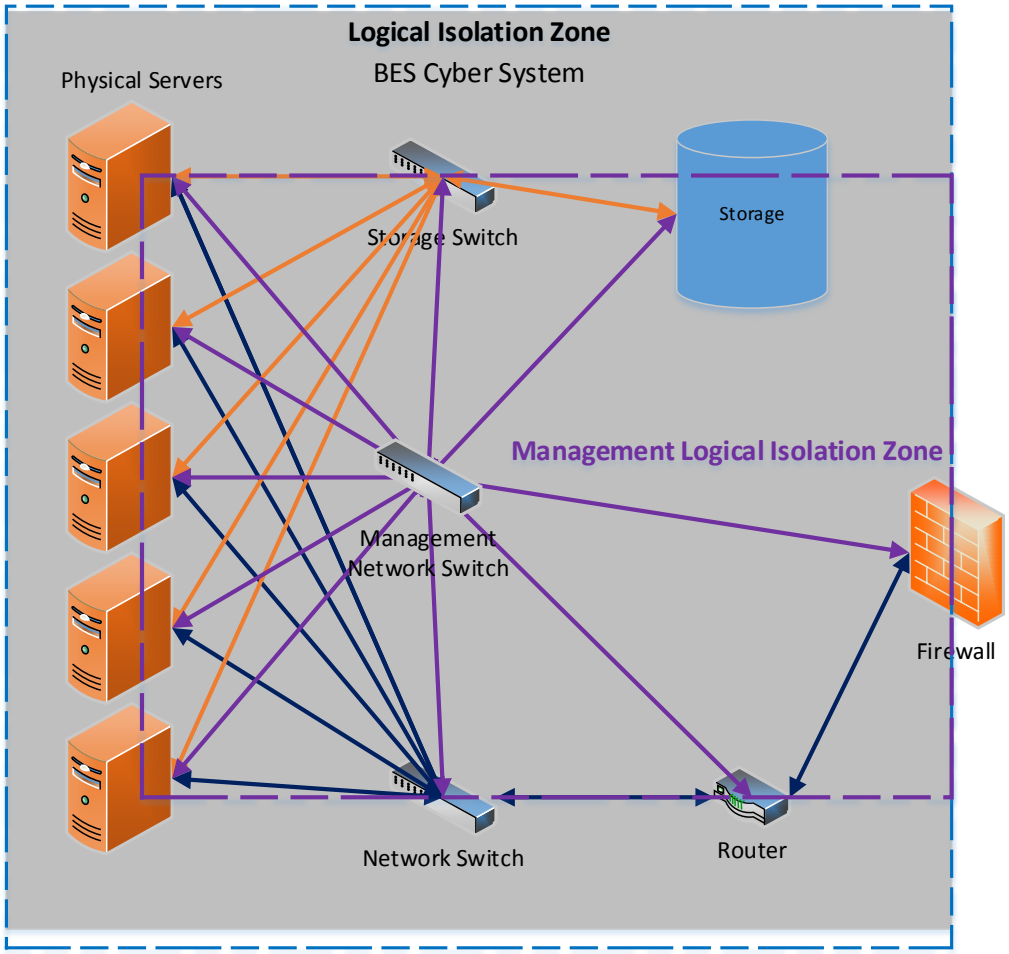
Management Plane Isolation

Future Environment showing backward compatibility with a Management Logical Isolation Zone



Logical Isolation Zones

Future Environment showing backward compatibility with the both Logical Isolation Zones



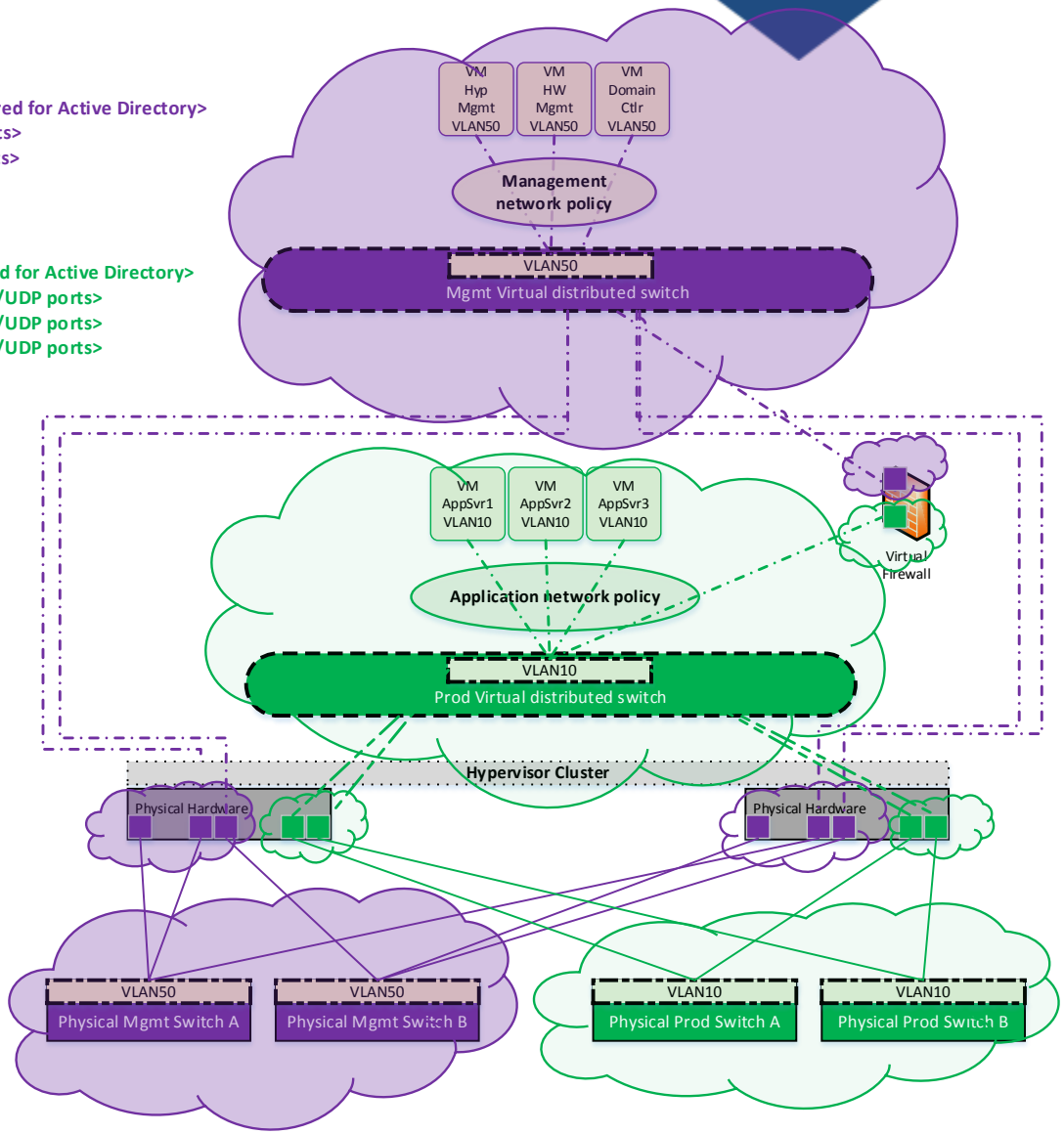
Logical Isolation Zones in Virtualization

Mgmt Logical Isolation Zone

Mgmt Network Policy
Allows communication to and from VLAN50 as follows
Domain Ctlr to VLAN10 and VLAN 50 <TCP/UDP ports required for Active Directory>
Hyp Mgmt to VLAN50 on <Application specific TCP/UDP ports>
HW Mgmt to VLAN50 on <Application specific TCP/UDP ports>
All other communication is blocked

Application Logical Isolation Zone

App Network Policy
Allows communication to and from VLAN10 as follows
VLAN10 to Domain Controller on <TCP/UDP ports required for Active Directory>
AppSvr1 to Appsvr2, AppSvr3 on <Application specific TCP/UDP ports>
AppSvr2 to Appsvr1, AppSvr2 on <Application specific TCP/UDP ports>
AppSvr3 to Appsvr1, AppSvr2 on <Application specific TCP/UDP ports>
All other communication is blocked



CIP-007

- Made conforming changes to applicable systems column: (PCS, EACS, etc.)
- Made conforming changes to ensure the requirements are at the system level (per system capability, remove references to Cyber Asset, etc.)
- Added security objectives to the "Big R" main requirements. Example: Each Responsible Entity shall implement one or more documented process(es) *to mitigate the risk posed by uncontrolled logical and physical connectivity* that collectively include each of the applicable requirement parts in…"
- Modified R1.1 (ports/services) to be more objective oriented. Permits use of east/west IDS, baselining logical connectivity, etc. in addition to documenting required network accessible ports.

CIP-007

- Introduced new requirement for installing only essential software and executable scripts on high and medium impact BES Cyber Systems, EACS, PACS, and PCAs.
- Moved CIP-007 R2 patching requirement to CIP-010 vulnerability management program requirement
- Added CIP Exceptional Circumstances language to apply to all of Requirement 4 (Security Event Monitoring)

CIP-010

- Made conforming changes to applicable systems column: (PCS, EACS, etc.)
- Made conforming changes to ensure the requirements are at the system level (per system capability, remove references to Cyber Asset, etc.)
- Added security objectives to the "Big R" main requirements. Example: Each Responsible Entity shall implement one or more documented process(es) *to mitigate the risk posed by insecure system configuration* that collectively include each of the applicable requirement parts in…"
- Removed the requirement to develop a baseline configuration
- Introduced the concept of a secure configuration. This new concept requires the collective identification of the methods used to comply with the security requirements in CIP-005 R1, CIP-007 R1, R2, R3, R4, R5, and CIP-010 R3.

CIP-010

- Replaced prescriptive timeframes with a risk based evaluation for entity determined timeframes.
- Added specification to the configuration monitoring requirement for hash monitoring, configuration monitoring, or configuration auditing.
- Split obligation to investigate detected unauthorized changes to its own requirement part. Added obligation to remediate detected unauthorized changes.
- Moved patch management requirement from CIP-007 to the CIP-010 Vulnerability Management program. Rephrased requirement in terms of identifying and mitigating software vulnerabilities. Added risk-based entity defined timeframes for implementation.
- Added CIP Exceptional Circumstances to apply to testing of changes prior to implementation

Next Steps

- Informal comment period open through December 18.
- 2019 Standard Drafting Team Meeting Planned Dates:
  - January 8-10, 2019 (Dallas, TX)
  - February 19-21, 2019 (Atlanta, GA)
- Request SC authorization to post March 2019.
- If approved by SC, CIP-002 through CIP-013 will be posted for a 45-day comment and ballot period March 2019.

Resources

- Information relative to the CIP Modifications project and SDT may be found on the Project 2016-02 Project Page under Related Files:

  Project 2016-02 Modifications to CIP Standards

Questions and Answers