NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Virtualization Draft 3

Project 2016-02 Modification to CIP Standards

Project 2016-02 SDT
March 2022

RELIABILITY | RESILIENCE | SECURITY




Agenda

- Administrative
  - NERC Antitrust and Open Meeting Notice
  - SDT Members
  - Opening Remarks
- Standards Overview

Administrative Items

- NERC Antitrust 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.
- Notice of Open Meeting
  - Participants are reminded that this webinar is public. The access number was widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

The CIP Standards Drafting Team

	Name	Entity
Co-chair	Jay Cribb	Southern Company
Co-chair	Matthew Hyatt	Georgia System Operations Corporation
Members	Jake Brown	ERCOT
	Norman Dang	Independent Electricity Systems Operator of Ontario
	Robert Garcia	SPP, Inc.
	Scott Klauminzer	Tacoma Public Utilities
	Sharon Koller	ATC, LLC
	Heather Morgan	EDP Renewables
	Mark Riley	Associated Electric Cooperative, Inc.

Opening Remarks

- **Webinar Purpose:** High level overview of modifications for Project 2016-02 Modification to CIP Standards
- **Draft 3 Posting Duration:** February 18– April 11, 2022
  - 45-day comment and ballot period
- **Standards Affected:** CIP-002 through CIP-011, and CIP-013
  - Standards with substantial changes: CIP-005, CIP-007, and CIP-010
  - Conforming changes: CIP-002, CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013

Draft 3 Redlines and "-Y" Versions

- Draft 3 Standard Versions
  - Clean
  - Redline to last posted
  - Redline to last approved

- CIP-003-Y posted in Draft 3.
  - Project 2020-03, Supply Chain Low Impact Revisions, is also working on CIP-003 and posted as CIP-003-X

Remaining Scope from SAR

- V5TAG Items
  - 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 the CIP V5 standards and the associated definitions regarding permitted architecture and the security risks of virtualization technologies."
  - Clarification of ERC/IRA
- CIP Exceptional Circumstances (CEC)
- Standard Template Conformity
  - Removal of Guidelines and Technical Basis (GTB) and Background sections to Technical Rationale documents.
  - Incorporate approved RFI concerning 'discrete' Shared BES Cyber Systems

What We Heard From Draft 2

- Definitions
  - SCI, ERC, ESP, CIP Systems, IRA, PCA
- CIP-010 Change Management and Baselines
- CIP-007 Ports and services
- Burden and complexity

Shared Cyber Infrastructure

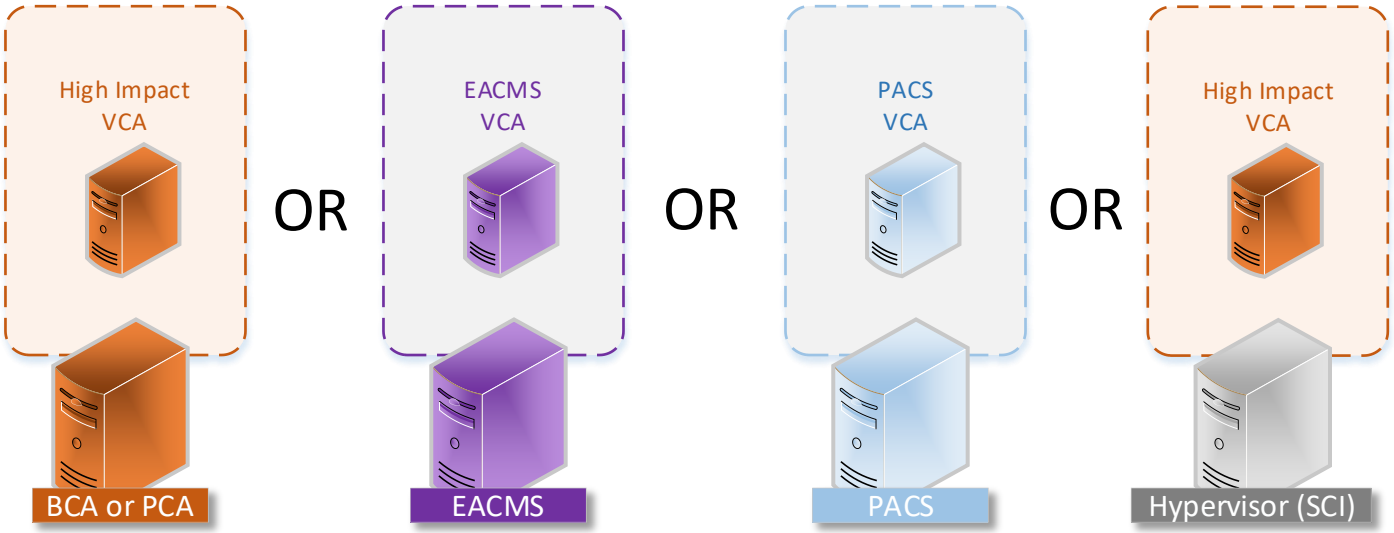
- SCI Related Modifications
  - New definition focuses on where Virtual Cyber Assets of multiple impact ratings are hosted by the same programmable electronic devices.
  - Identification in CIP-002 has been reverted to approved language with only conforming changes
  - Reduced complexity in applicable systems column
  - Focus on making backward compatibility easier

Virtual Cyber Assets

- Used as a form (like CA)
- Can exist on other system types (not just SCI)

Virtual Cyber Assets

A non-dormant logical instance of an operating system or firmware, on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure; excluding logical instances that are being actively remediated.



Shared Cyber Infrastructure

Shared Cyber Infrastructure (SCI)

One or more programmable electronic devices, including the software that shares the devices' resources, that:

- In a clustered configuration, hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or
- Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization.

SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.

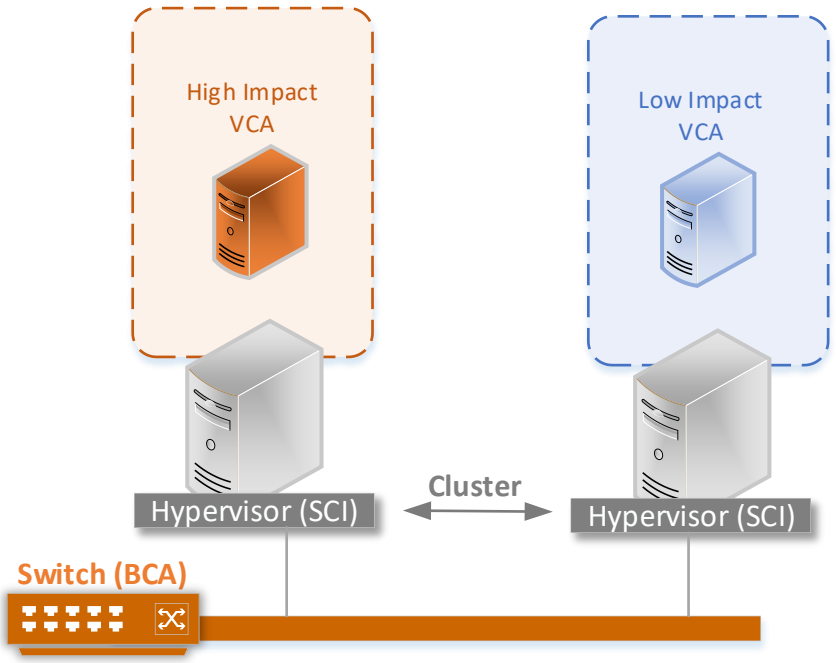
SCI – Hypervisor Cluster Example

Shared Cyber Infrastructure (SCI)

One or more programmable electronic devices, including the software that shares the devices' resources, that:

- In a clustered configuration, hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or
- Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization.

SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.



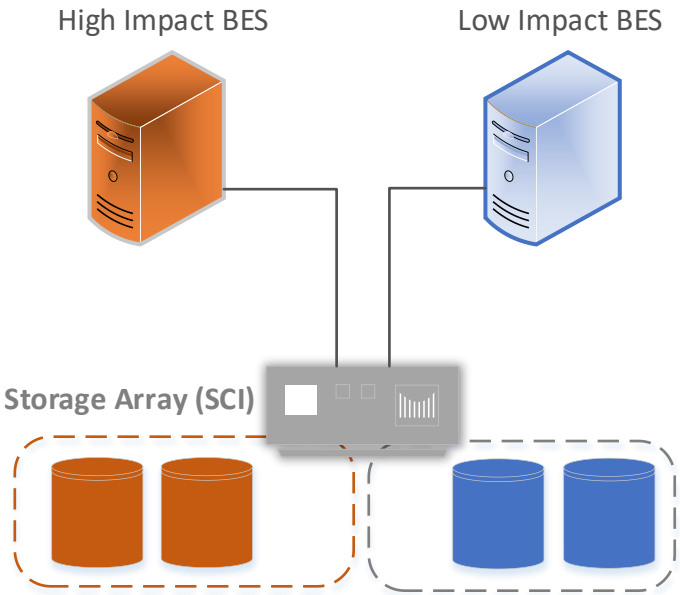
SCI – Storage Array Example

Shared Cyber Infrastructure (SCI)

One or more programmable electronic devices, including the software that shares the devices' resources, that:

- In a clustered configuration, hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or
- Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization.

SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.



Shared Cyber Infrastructure Requirements

- Requirements for SCI
  - Included in applicability throughout the standards as appropriate using "SCI supporting an Applicable System in this Part" in the applicability column.
    - Some exclusions in CIP-006 and CIP-009
  - CIP-005 R1 Part 1.3 – Restricts access to management interface
  - CIP-007 R1 Part 1.3 – Enforces affinity requirements for SCI

SCI - CIP-005 R1 Part 1.3

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI supporting an Applicable System from Part 1.1. EACMS, and their supporting SCI, that enforce an ESP for an Applicable System in Part 1.1	Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.	Examples of evidence may include, but are not limited to, documentation of the access enforcement configuration or settings to or from the Management Interfaces, including documented reasons such as: • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the management plane resources (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).

SCI - CIP-007 R1 Part 1.3

CIP-007-7 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI supporting: High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources between VCAs that are not of, or associated with, the same impact categorization.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared.

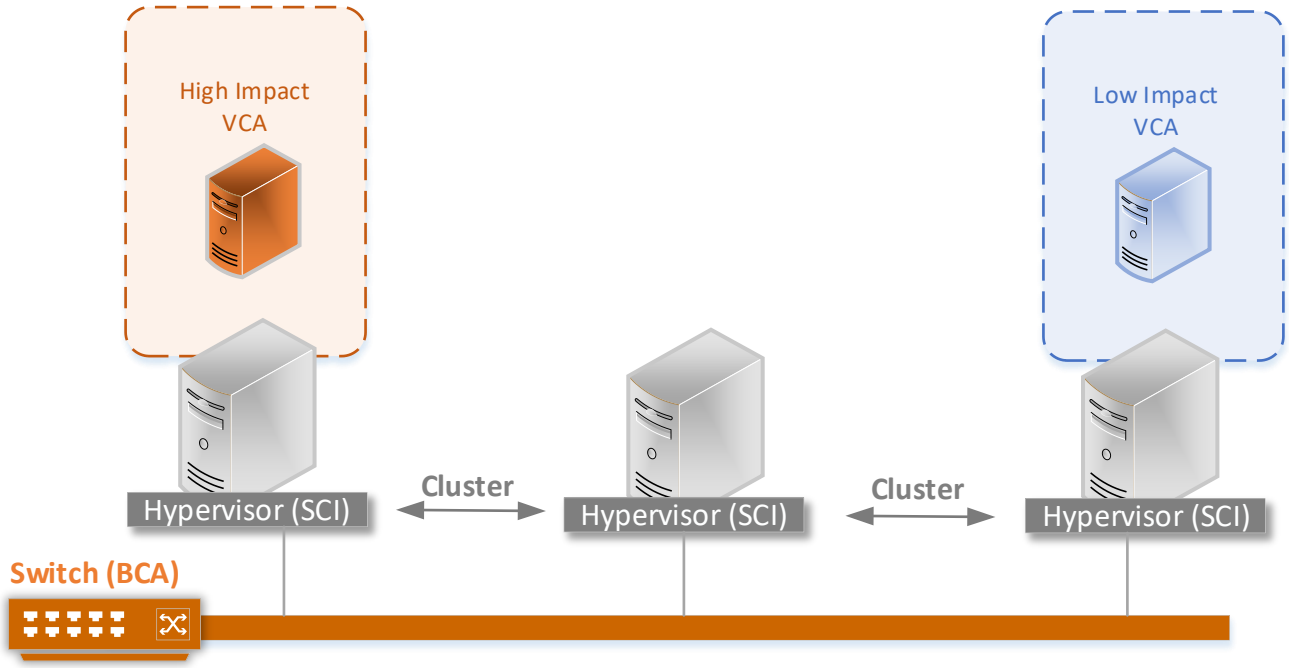
Protected Cyber Asset

- How does PCA Interact with SCI?
- No PCA's in the drawing below (yet)

Protected Cyber Asset

One or more Cyber Assets or Virtual Cyber Assets that:

- Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System protected by the same ESP; or
- Share CPU or memory with any part of the BES Cyber System, excluding Virtual Cyber Assets that are being actively remediated prior to introduction to an ESP.



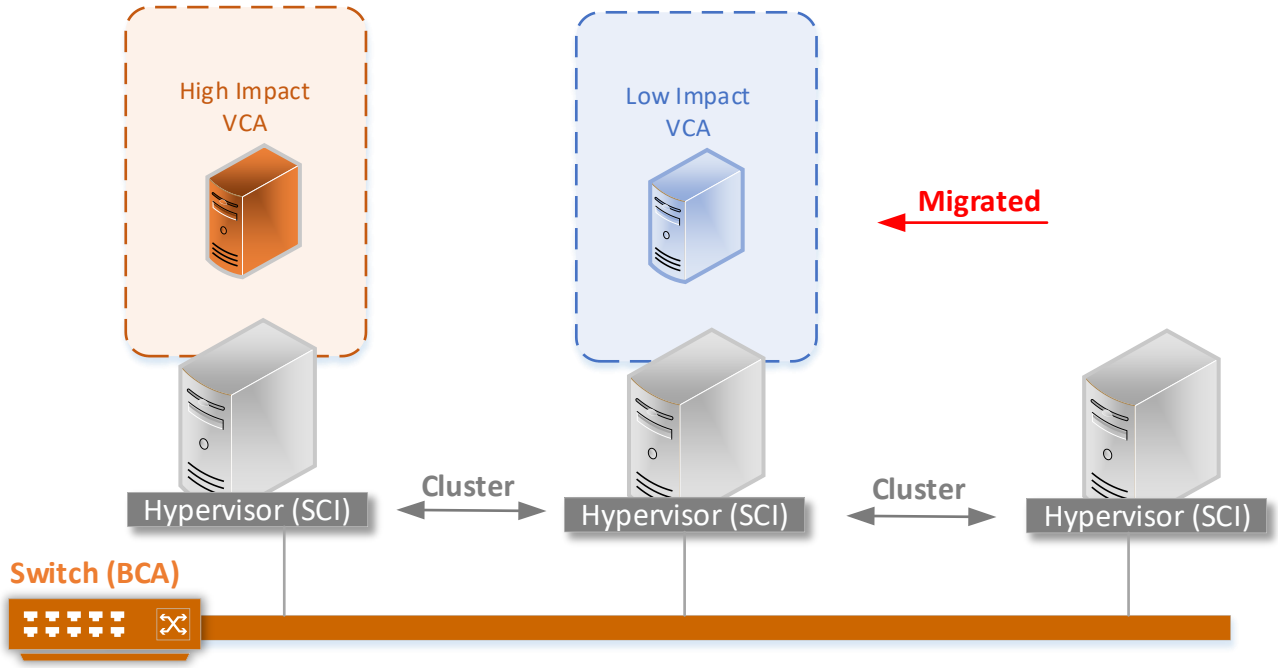
Protected Cyber Asset

- If the Low Impact VCA Migrates, No PCA's exist (yet)

Protected Cyber Asset

One or more Cyber Assets or Virtual Cyber Assets that:

- Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System protected by the same ESP; or
- Share CPU or memory with any part of the BES Cyber System, excluding Virtual Cyber Assets that are being actively remediated prior to introduction to an ESP.



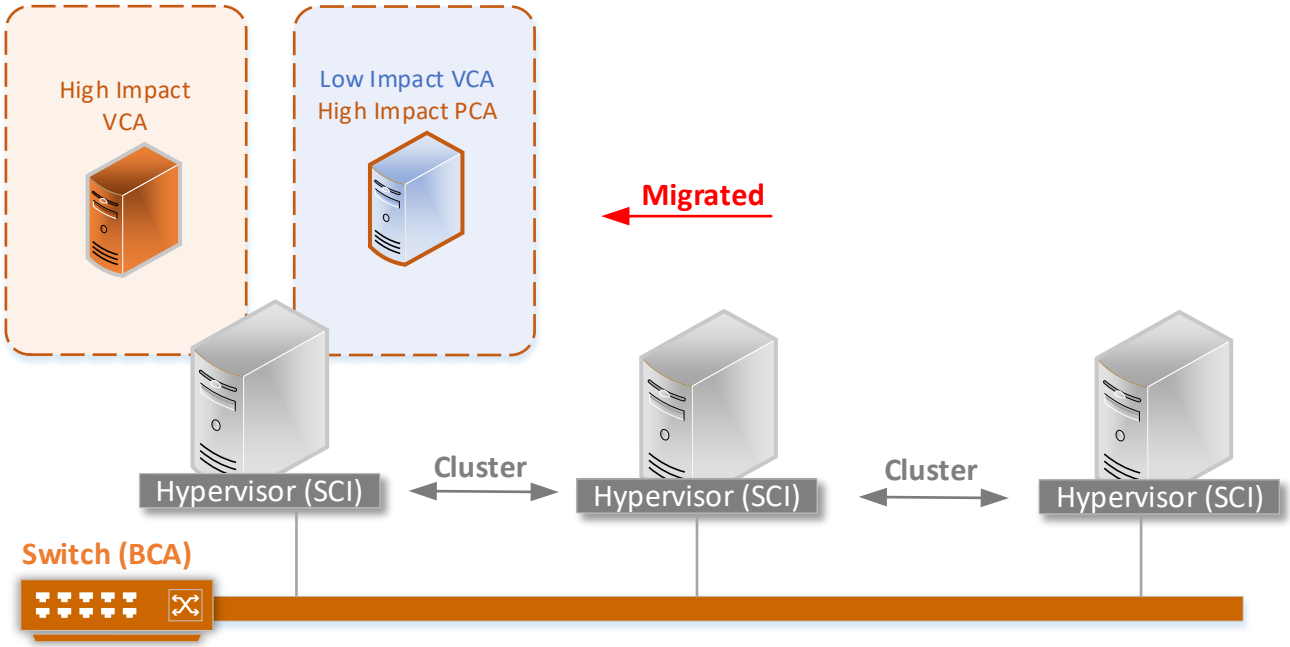
Protected Cyber Asset

- If the Low Impact VM moves to the same host as the High Impact, it becomes a PCA.

Protected Cyber Asset

One or more Cyber Assets or Virtual Cyber Assets that:

- Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System protected by the same ESP; or
- Share CPU or memory with any part of the BES Cyber System, excluding Virtual Cyber Assets that are being actively remediated prior to introduction to an ESP.



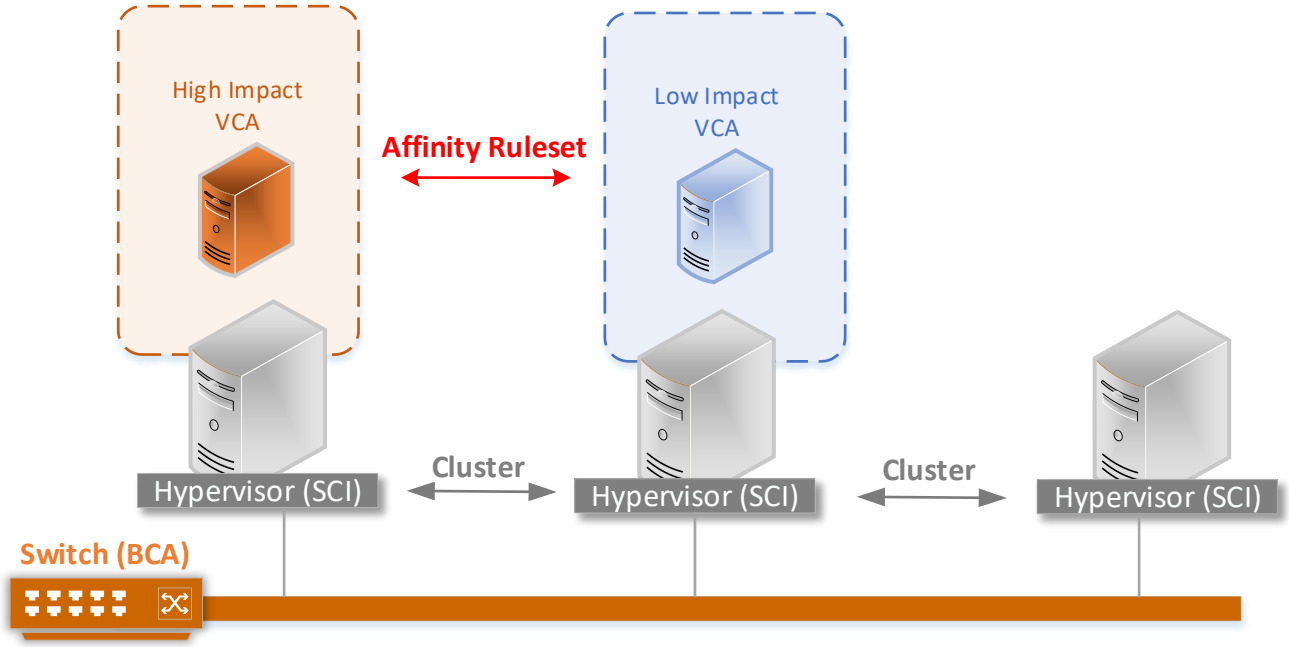
Protected Cyber Asset

- Affinity rulesets can be used to ensure different Impact Categorizations are kept separated

Protected Cyber Asset

One or more Cyber Assets or Virtual Cyber Assets that:

- Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System protected by the same ESP; or
- Share CPU or memory with any part of the BES Cyber System, excluding Virtual Cyber Assets that are being actively remediated prior to introduction to an ESP.

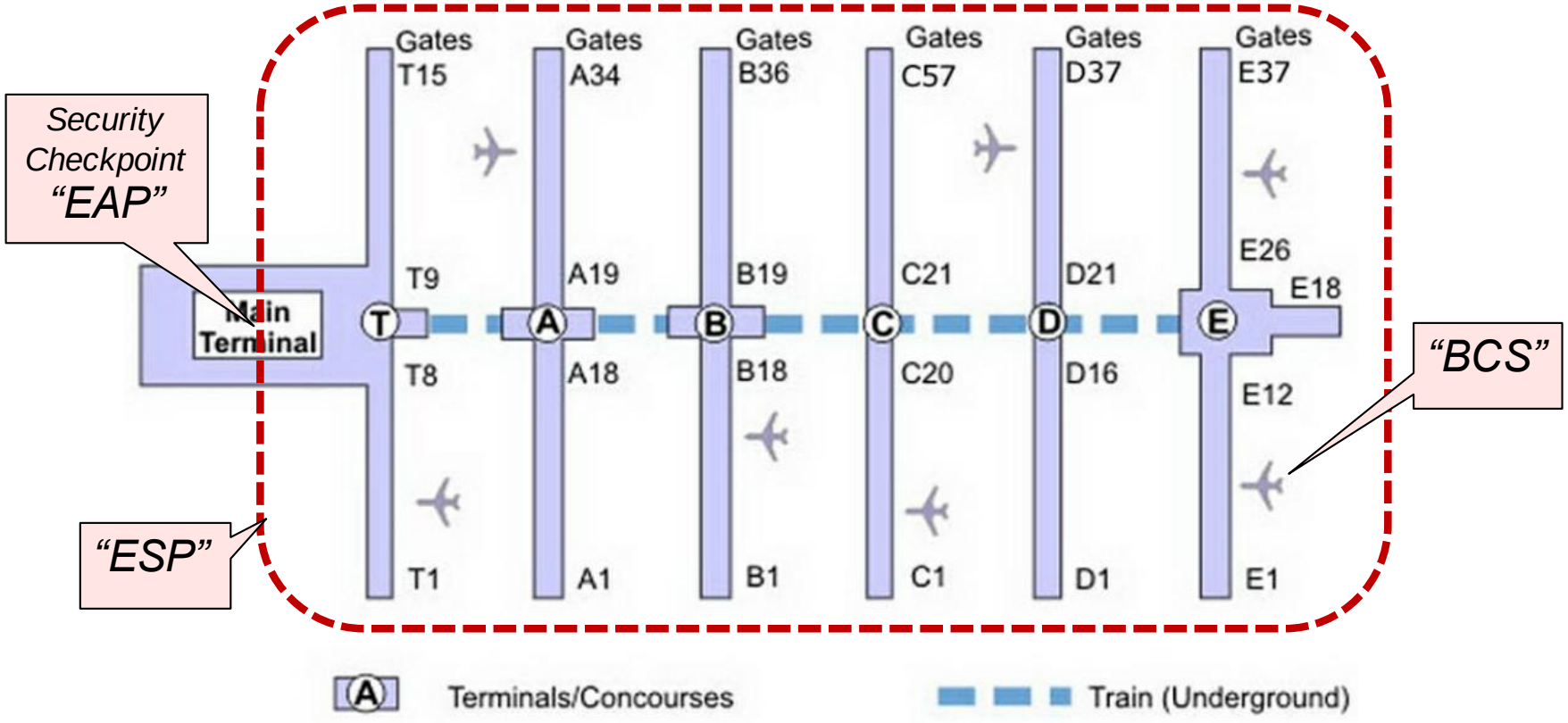


CIP System/Cyber System

- ~~CIP System~~
  - Was created to include all the function classes of in-scope CIP systems (BCA, EACMS, PACS, PCA, etc.) in one term.
  - Embedded in other definitions in draft 2
  - It is no longer used in draft 3 and is ***deleted from proposed new terms***.

- Cyber System
  - Was created to include the three forms of CA, VCA, and SCI.
  - Avoids changing all instances of CA to all 3 forms.
  - Simplifies standard changes if new forms added in the future.

Airport Analogy



ESP's and Zero Trust

- Virtualization and Hypervisors allow for easier implementation of Zero Trust based architectures
- Modifying ESP/EAP to allow other architectures that address the cyber security risks

ESP/EAP

- Electronic Security Perimeter

The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more EAPs.

- Electronic Access Point

An electronic policy enforcement point or a Cyber Asset interface that ~~on an Electronic Security Perimeter that allows~~controls routable communication to and from a BES Cyber System ~~between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter~~.

Other ESP/EAP Items

- "Super ESP"
  - Single ESP but across a WAN
  - Often used to migrate VCAs or replicate data between geographic locations (primary/backup data centers)
- New 4.2.3.3 exemption equivalent to 4.2.3.2 exemption
  - However, its tied with a new CIP-005 R1.4 for data protection (e.g., encryption)
- CIP-006 Part 1.10 incorporated

External Routable Connectivity

- External to what?

	Approved	Proposed
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~~through its ~~Electronic Security Perimeter~~ ESP via a bi-directional routable protocol connection.

- Inside/outside ESP does not translate for zero trust environments
- Also need to consider environments without ERC
- Restored ESP - changed reference to “access through it’s ESP”

Interactive Remote Access

	Approved	Proposed
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 using a Cyber Asset or VCA, not protected by any of the ~~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) (ESP) and using a routable protocol: • To a Cyber System protected by an ESP; • That is converted to a non-routable protocol to a Cyber System not protected by an ESP; or • To a Management Interface of Shared Cyber Infrastructure.

Intermediate System

	Approved	Proposed
Intermediate Systems~~s~~	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.	One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users. ~~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.~~

CIP-005 R2.1

Part	Applicable Systems	Requirements	Measures
2.1	High ~~l~~impact ~~BES Cyber Systems~~BCS and their associated ~~:~~ PCA Medium ~~l~~impact ~~BES Cyber Systems~~ BCS ~~with External Routable Connectivity~~ and their associated ~~:~~ PCA SCI supporting an Applicable System in this Part	Permit authorized Interactive Remote Access (IRA), if any, only through an Intermediate System. ~~For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.~~	Examples of evidence may include, but are not limited to, network diagrams, ~~or~~ architecture documents, configuration, or settings that show all IRA is through an Intermediate System.

- IRA needs to be through an Intermediate System
- Hall of mirrors issue addressed (Management Interface of EACMS)
- SCI added to Applicable Systems
- Note that ERC removed in Applicable System – serial converters

CIP-005 R2.6

2.6	Intermediate System used to access Applicable Systems of Part 2.1	Routable protocol communications between Intermediate Systems and Applicable Systems of Part 2.1 must be through an ESP.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System.

- Applicable Systems – references back to those from Part 2.1
- Affinity requirement for Intermediate Systems – removed
- ESP positioning requirement for Intermediate Systems - routable protocol communications must be through an ESP

CIP-003/CIP-004

- Minimal changes
- CIP-003-Y
  - R2 (Low Impact) – SCI added
  - Attachment 1 (Low Impact)
    - SCI added
    - IEC 61850 GOOSE – changed to communications of Protection Systems
- CIP-004-8
  - SCI added to Applicable Systems
  - Cyber Assets/Systems – replaced with Applicable Systems
  - CEC added to Requirement R3.5

CIP-005 R1 Part 1.1

Part	Applicable Systems	Requirements
1.1	High ~~l~~impact ~~BES Cyber Systems~~BCS and their associated ~~:~~ PCA Medium ~~l~~impact ~~BES Cyber Systems~~BCS and their associated ~~:~~ PCA	~~All a~~Applicable Systems ~~Cyber Assets~~ connected to a network via a routable protocol must be protected by an ~~shall reside within a defined~~ ESP.

- Reinstated since Draft 2
- “Protected by”

CIP-005 R1 Part 1.2

Part	Applicable Systems	Requirements
1.2	High ~~l~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated ~~:~~ PCA Medium ~~l~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated~~:~~ PCA	Permit only needed routable protocol communications, and deny all other routable protocol communications, through the ESP, excluding time sensitive communications of Protection Systems. ~~All External Routable Connectivity must be through an identified Electronic Access Point (EAP).~~

- Collapsed previous Parts 1.2 & 1.3

CIP-005 R1 Part 1.4

1.4	High ~~I~~impact ~~BES Cyber Systems~~BCS ~~with Dial-up Connectivity~~ and their associated~~:~~ PCA Medium ~~I~~impact B~~ES Cyber Systems~~CS ~~with Dial-up Connectivity~~at Control Centers and their associated~~:~~ PCA	Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls (such as encryption), or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ii. Time sensitive communication of Protection Systems.

CIP-006

- Minimal Changes
- Requirement R1.10 – Moved to CIP-005 Requirement R1.4 and Applicable Systems issue fixed
- SCI removed from Applicable Systems due to confusion as to whether it supporting the BCS and associated EACMS and PCAs or whether it's supporting the PACS

CIP-007 R1 Part 1.1

1.1	High ~~l~~impact ~~BES Cyber Systems~~BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium ~~l~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability. ~~Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.~~

- Minimal changes in two Requirement Parts

CIP-009-~~6~~7 — Cyber Security — Recovery Plans for BES Cyber Systems

CIP-009-~~6~~7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover ~~BES Cyber~~ Applicable System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover ~~BES Cyber~~Applicable System functionality.

CIP-009-~~6~~7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover ~~BES Cyber~~ Applicable System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover ~~BES Cyber~~Applicable System functionality substitutes for this test.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).

CIP-009

- SCI removed from Applicable Systems – Why?

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems
2. **Number:** CIP-009-~~6~~7
3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the Bulk Electric System (BES).

- Result is Applicable Systems contains the same impact rated BCS and their associated EACMS or PACS as is in current approved.

- EXCEPT for Requirement R1 Part 1.5 on forensics

CIP-009-~~6~~7 — Cyber Security — Recovery Plans for BES Cyber Systems

CIP-009-~~6~~7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this part	One or more processes to preserve data, per ~~Cyber Asset~~system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

- From Baselines to Change Management – Why?
  - Overcoming Virtualization challenges
    - Automated change capability (including failover and recovery)
    - Order of operations when making change is different for CA vs VCA
    - Dormant VMs
    - Parent/Child images
    - Remediation VLANs
  - Not a fundamental change, just removal of a prescriptive 'how' and the extremely limited list of system attributes (AKA baseline: OS, apps, ports/services etc.).
  - Focuses on the security objective – define change, authorize change, test changes to ensure CIP-required security controls are not impacted.
  - Maintaining baseline configs is 'one' way to help manage change.

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Define types of changes that may impact CIP-005 or CIP-007 security controls. For those changes: 1.1.1. Prior to change implementation, identify impacted security controls in CIP-005 and CIP-007, except during CIP Exceptional Circumstances; 1.1.2. Authorize those changes; and 1.1.3. Verify cyber security controls from CIP-005 and CIP-007 are not adversely affected.	Examples of evidence may include, but are not limited to, a documented process that defines changes that may impact security controls in CIP-005 and CIP-007, such as but not limited to: • Operating system (OS) software; • Firmware, where no independent OS exists; • Commercially available or open-source application software, including application containers; • Custom software installed, including application containers; • Configuration that modifies network accessible logical ports or network accessible services on an Applicable System; • SCI configuration of host affinity control between systems with different impact ratings; • Changes to configurations or settings for an ESP between systems with different impact ratings; • Changes to parent images from which individual child images are derived, such as in virtual desktop infrastructure (VDI) implementations; or • Any other configuration or setting determined by the Responsible Entity. (1.1.1.) • Documentation of the impacted security controls in CIP-005 and CIP-007; (1.1.2.) • A change request record and associated authorization for applicable changes; or • Records from a change management system that identifies applicable changes and records of authorization for changes. (1.1.3.) • A list of cyber security controls verified or tested along with the dated test results; or • An output from cyber security testing tools such as a vulnerability scanner.

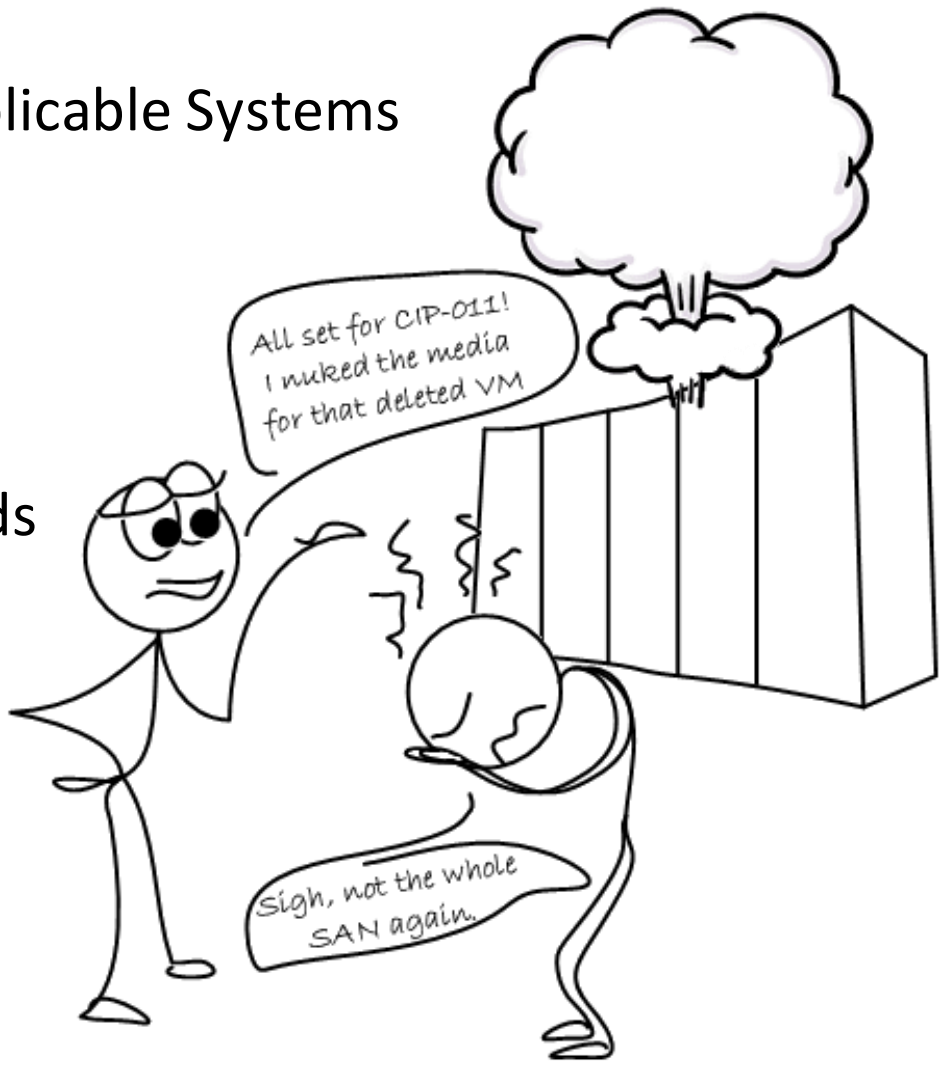
was 1.4.1 was 1.2 was 1.4.2 was 1.3 30 day baseline update was 1.4.3 document verification results was 1.1

CIP-011

- Minimal changes from draft 2
- R1 conforming changes to Applicable Systems

Applicable Systems
SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part

- R2 remains an objective level requirement for “Methods to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the Applicable Systems column).”



CIP-013

- Minimal changes from draft 2
- R1 conforming changes to add SCI as an applicable system
- Streamlining overall applicability in R1

CIP-013-3 – Cyber Security - Supply Chain Risk Management

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact ~~BES Cyber Systems (~~BCS~~)~~, their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI). ~~identified independently supporting these BCS or their associated EACMS and PACS.~~ The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of applicable systems listed in R1 to identify and assess cyber security risk(s) to the ~~Bulk Electric System (~~BES~~)~~ from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring applicable systems listed in Requirement R1 that address the following, as applicable:

Violation Severity Levels (VSL)

- VSL Clarifying changes, cleanup, and simplification
  - Removal of verbose compliant aspects; Focus on non-compliant aspects

CIP-013-3 – Cyber Security - Supply Chain Risk Management
Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity ~~developed one or more documented~~ supply chain cyber security risk management plan(s) ~~which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Part 1.2, but the plans do~~did not include one of the parts in ~~Requirement R1 Part~~ 1.2.1 through Part 1.2.6.	The Responsible Entity ~~developed one or more documented~~ supply chain cyber security risk management plan(s) did not include two or more of the parts in ~~which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Part 1.2, but the plans do not include two or more of the parts in Requirement R1~~ Part 1.2.1 through Part 1.2.6.	The Responsible Entity's ~~developed one or more documented~~ supply chain cyber security risk management plan(s)~~, but the plan(s)~~ did not include the use of process(es) in planning for procurement of applicable systems ~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES~~ as specified in Part 1.1., ~~or~~OR -The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2.~~the plan(s) did not include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2.~~	The Responsible Entity's ~~developed one or more documented~~ supply chain cyber security risk management plan(s)~~, but the plan(s)~~ did not include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES~~ as specified in Part 1.1, and the supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified ~~plan(s) did not include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1~~ Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the RequirementR1.

CIP-013-3 – Cyber Security - Supply Chain Risk Management
Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity's supply chain cyber risk management plan(s) did not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement of applicable systems as specified in Part 1.1. OR The Responsible Entitiy's supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement applicable systems as specified in Part 1.1, and the supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in Requirement R1.

Implementation Plan

- 24 month implementation plan with provisions for early adoption.
- Early adoption – Entity and Regional Agreement to implement
  - Permits Registered Entities to work directly with their Region(s) to identify a date in advance of the 24 months to be compliant with the virtualization-enabled standards.
  - Responsible Entities must continue to comply with current enforceable CIP Standards and Definitions until that agreed upon Early Adoption date.

Resources Continued

- This slide deck and other information relative to the CIP Modifications SDT may be found on the Project 2016-02 Project Page under Related Files:

  https://www.nerc.com/pa/Stand/Pages/Project-2016-02-Modifications-to-CIP-Standards-RF.aspx

Questions and Answers