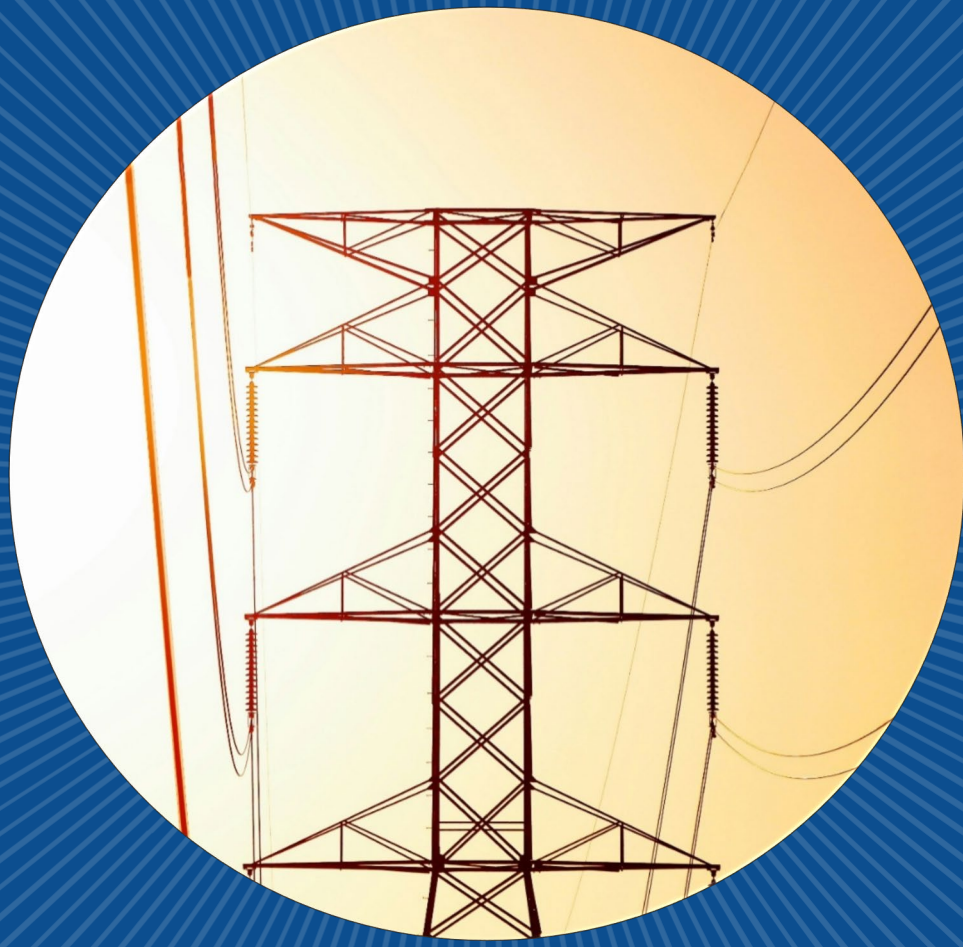
NPCC

NERC CIP Virtualization Standards Update



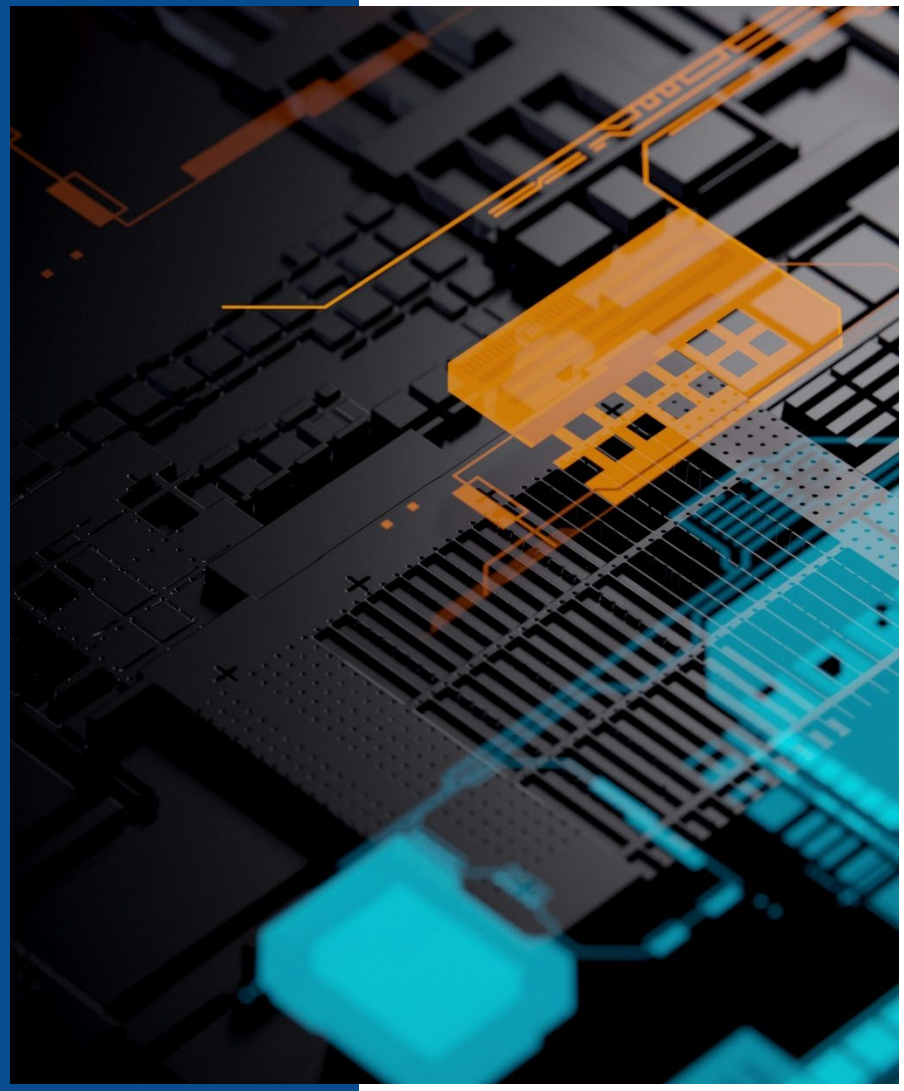
NPCC Standards and Criteria

September 2026

Public

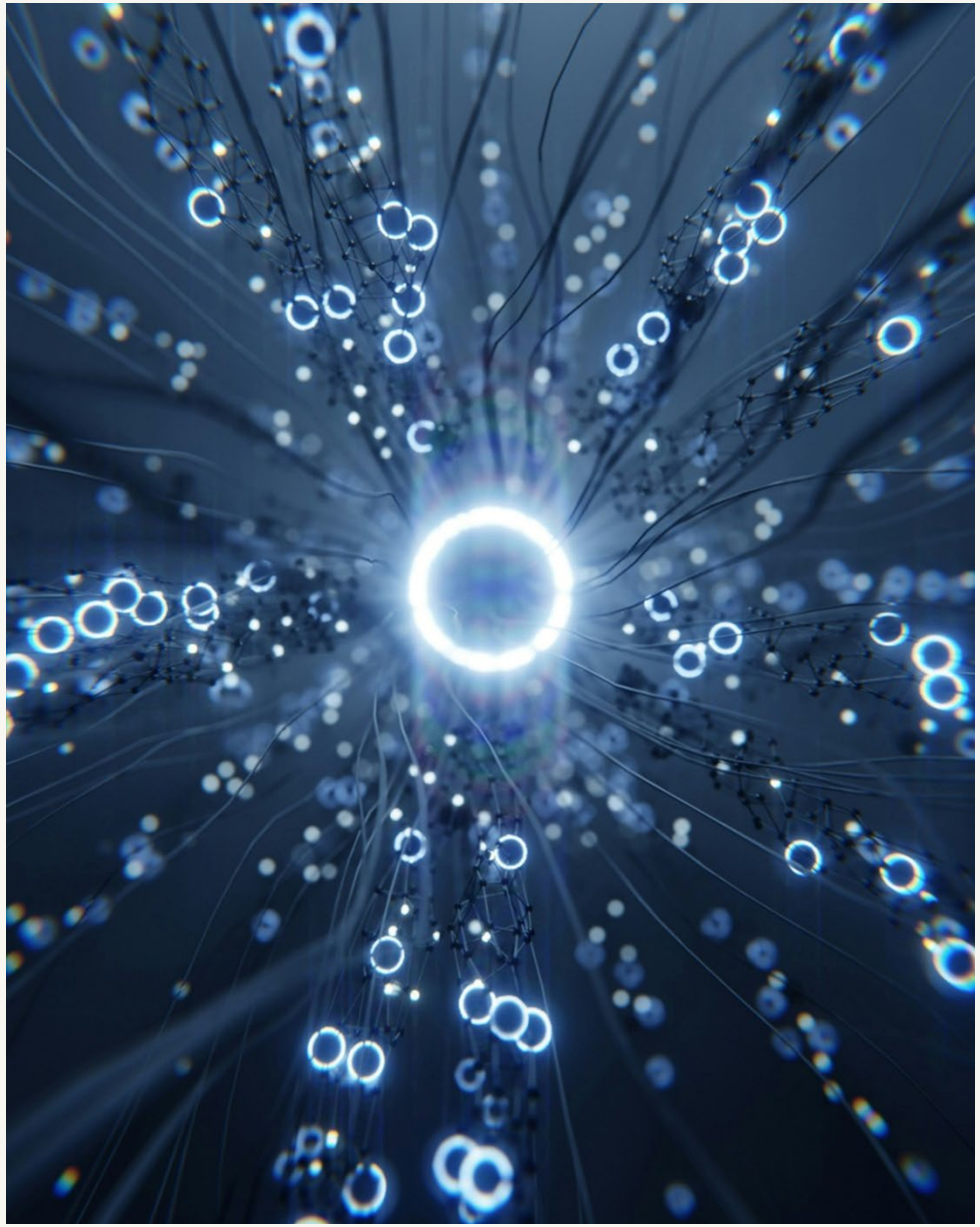
Agenda

- Background
- Introduction to Virtualization
- Definitions
- Overarching Changes
- CIP-005-8
- CIP-007-7
- CIP-010-5
- Implementation Plan
- CIP-002-8 – Transmission Owner Control Center Clarification
- CIP-003-11
- Additional Resources



Background

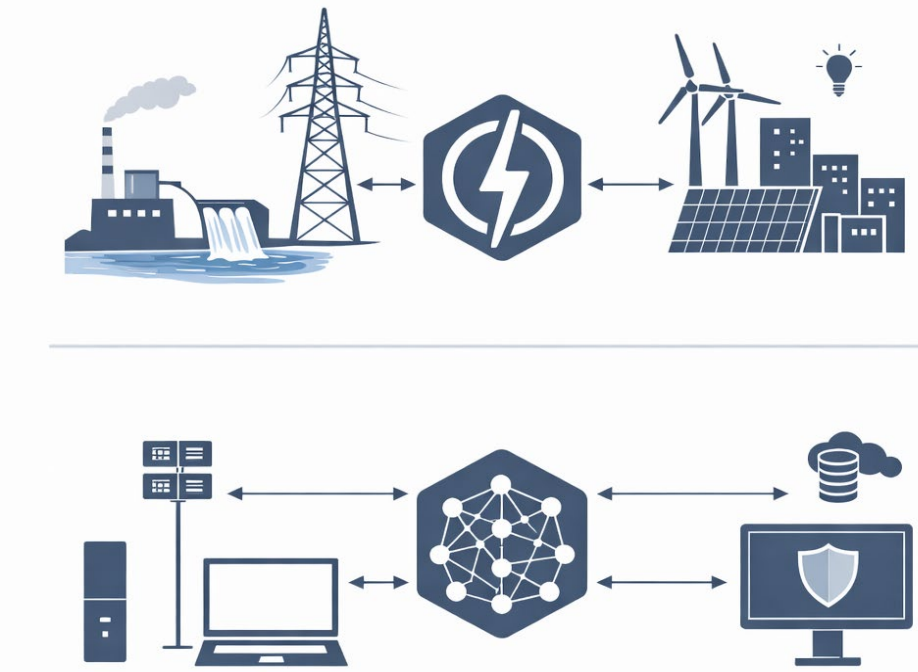
- CIP Version 5 Transition Advisory Group:
  - Consider permitted architecture and security risks
- Industry need:
  - Constraints of CIP V5 architecture
  - Ambiguity in application to standards
  - Uncertainty and difficulty implementing compliant strategies
- Project 2016-02 Modifications to CIP Standards



Virtualization

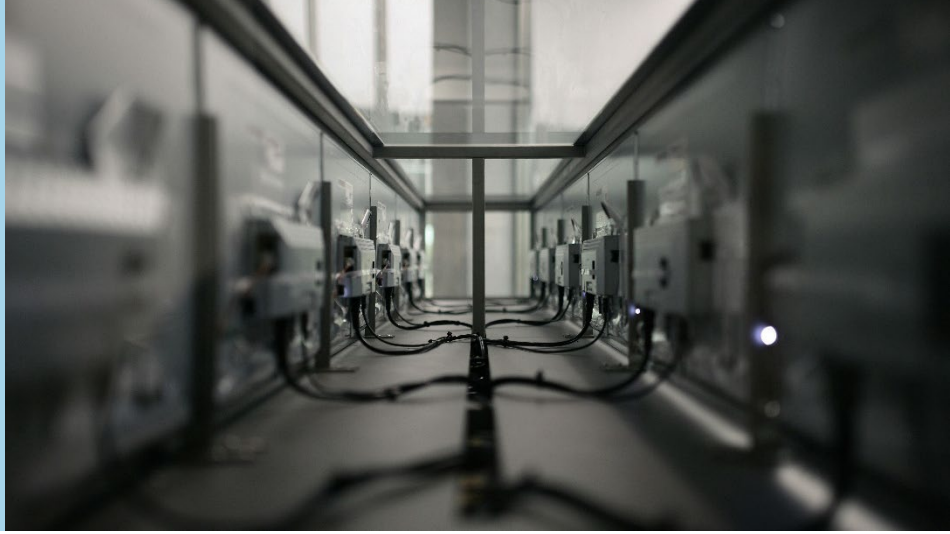
Introduction

- Abstraction of physical computing resources
  - Allows multiple systems to run on a single server
  - Virtual machines operate independently
  - All virtual machines share underlying hardware
- CIP standards changes are to enable but not require
  - Flexibility in the use of new technology
  - Requires technology-enforced controls as alternatives



AI-generated image created using Microsoft Copilot, Microsoft Corporation, April 2026

Implications of Virtualization



Benefits

- Reduced outages
- Reduced cost
- Increased uptime
- Very fast recovery
- Flexible architecture
- Increased security

Challenges

- Classification of cyber assets
- Scoping of requirements based on asset classes
- Application of prescriptive requirements
- Virtual data storage
- Production environment and remediation VLANs

Required Changes

- Address unique risks
- Provide categorization clarity
- Flexibility in choice of technology usage

Definitions

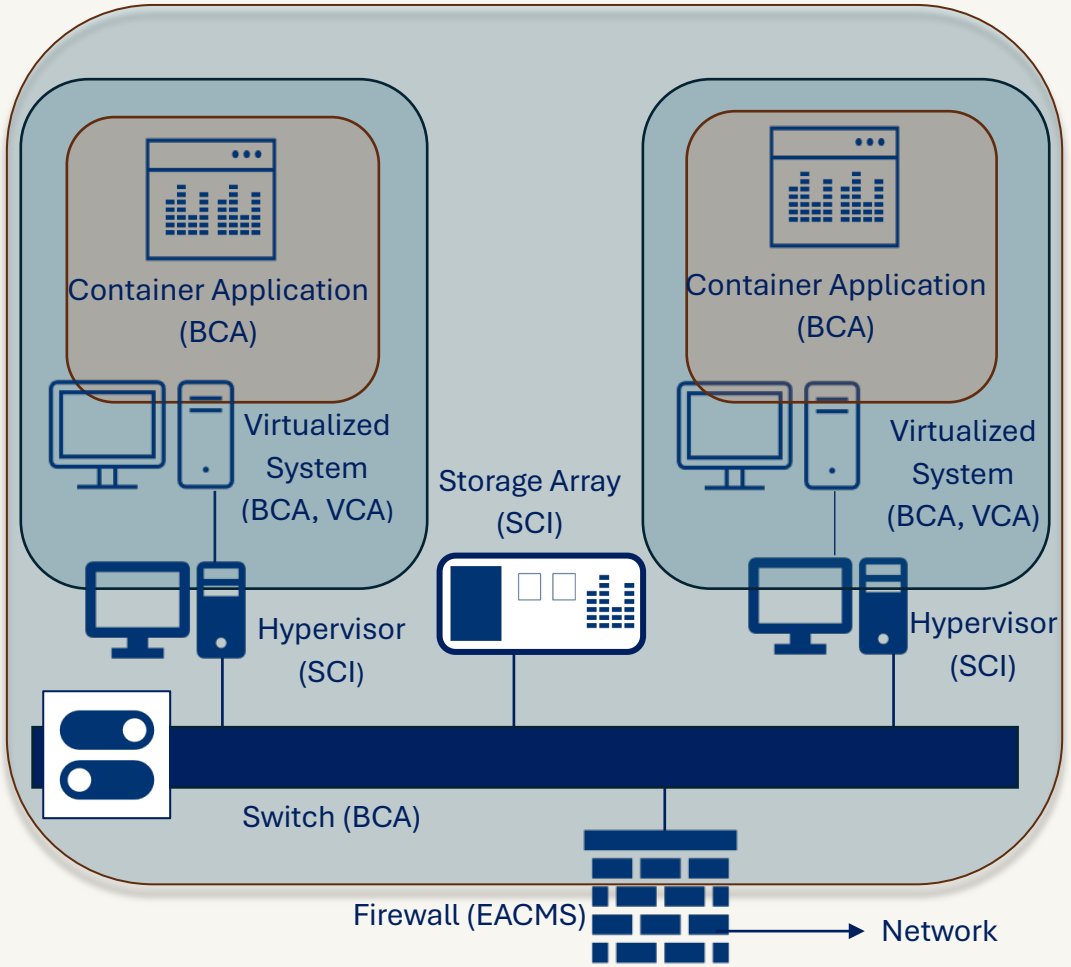
Themes and Rationale Overview

Virtualization Integration	• Affected terms: BCA, Cyber Asset, PCA, TCA, PACS, EACMS
Shift to scope-agnostic, architecture-neutral definitions	• Affected terms: ESP, EAP, ERC, IRA, EACMS, Intermediate System
Clarification of access concepts	• Affected terms: ERC, IRA, ESP, EAP, Intermediate System
Alignment of definitions with virtualized risk models	• Affected terms: PCA, TCA, SCI
Conforming changes for consistency and clarity	• Affected terms: CIP Senior Manager, BSCI, Removeable Media, Reportable Cyber Security Incident

Virtual Cyber Asset

A logical instance of an operating system or firmware, currently executing 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 (SCI).

- Virtual Cyber Assets (VCAs) do not include:
  - Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems;
  - Dormant file-based images that contain operating systems or firmware; or
  - SCI or Cyber Assets that host VCAs. Application containers are considered software of VCAs or Cyber Assets.



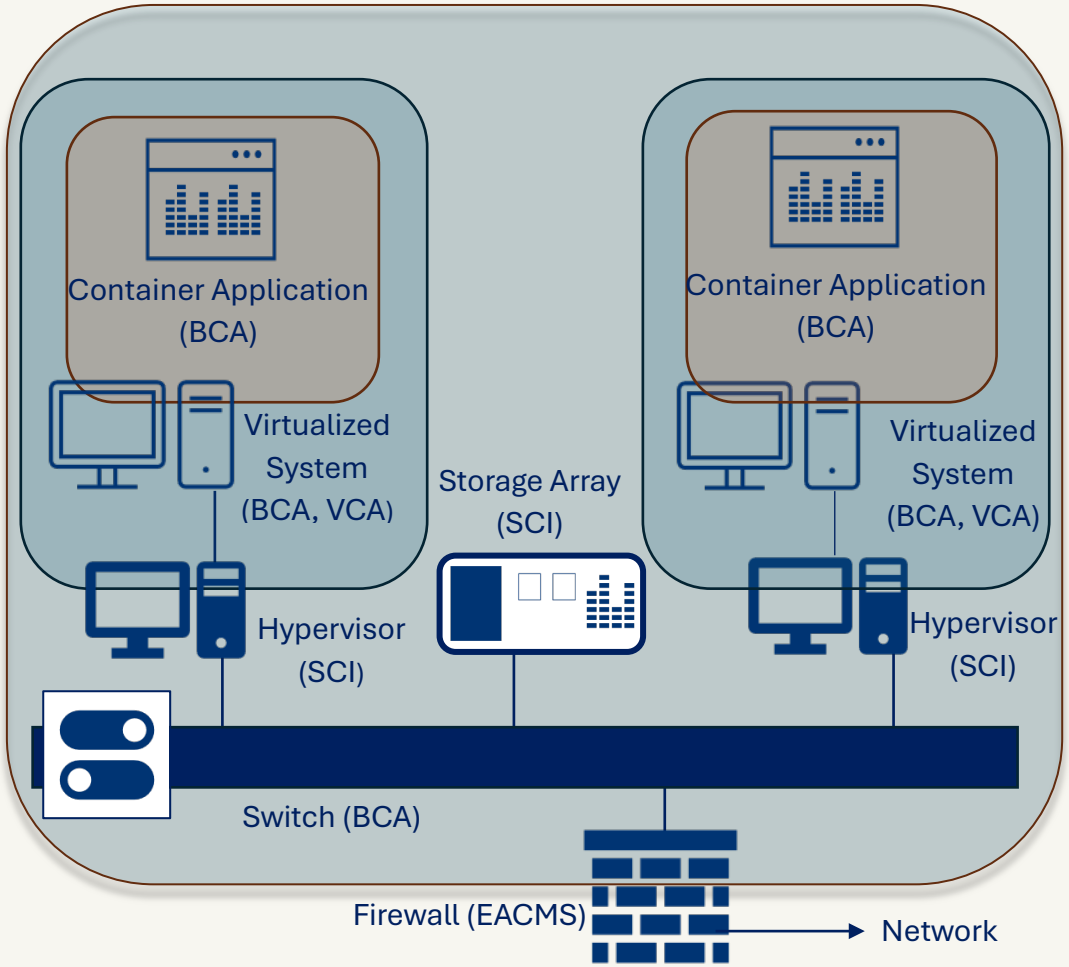
Adapted from [September 30, 2020 NERC Virtualization Workshop]

Shared Cyber Infrastructure

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

- 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.



Adapted from [September 30, 2020 NERC Virtualization Workshop]

New Definitions

Cyber System

One or more Cyber Assets, Virtual Cyber Assets or Shared Cyber Infrastructure

Management Interface

An administrative interface that:

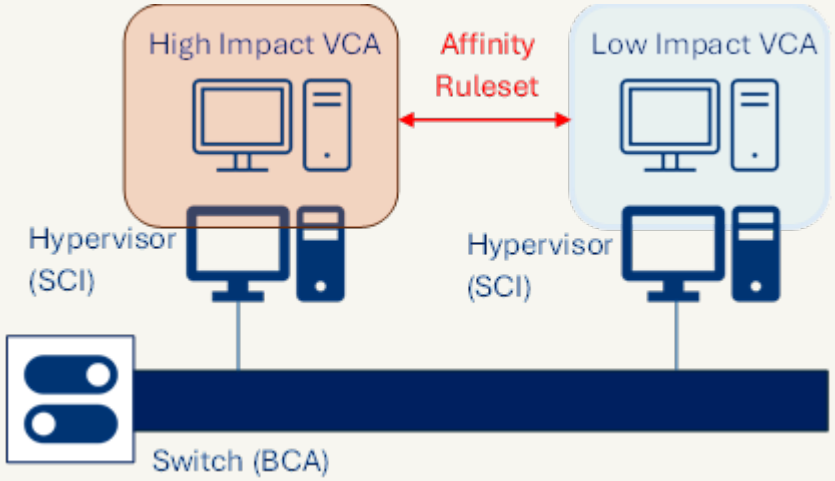
- Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure;
- Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or
- Configures an Electronic Access Point.

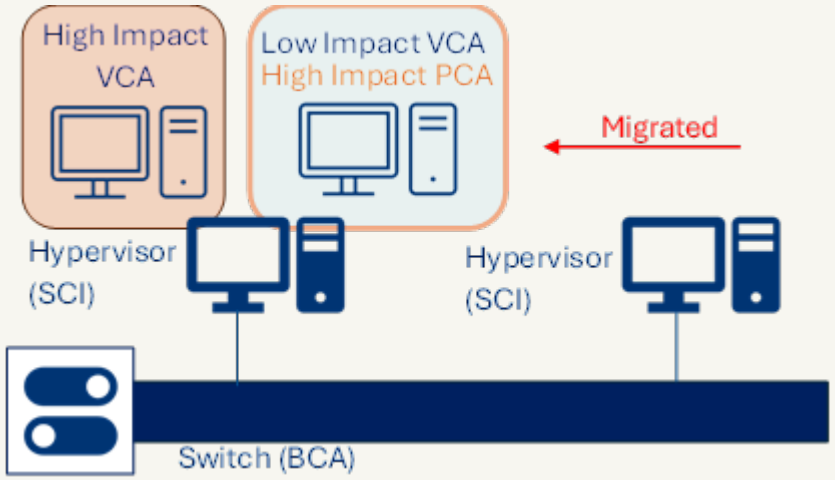
Core Asset Definition Updates

Virtualization-driven changes to asset classification

BES Cyber Asset (BCA)	Cyber Assets	Protected Cyber Asset (PCA)	Transient Cyber Asset (TCA)
• Now includes VCAs as potential BCAs • Clarifies relationship between SCI and impact categorization	• Explicitly excludes SCI • Clarifies treatment of application containers as software	• Adds CPU/memory sharing as a new PCA trigger • Addresses hypervisor-level vulnerabilities and mixed-impact co-residency • Excludes VCAs in remediation VLANs	• Now includes VCAs as TCAs • Adds SCI as a valid connection target • Clarifies treatment of VM “player” environments on laptops

Protected Cyber Asset





Adapted from March 14, 2022 NERC Project 2016-02 webinar.

CIP V5 Definition

- 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.

Virtualization Definition

- One or more Cyber Assets or Virtual Cyber Assets (VCA) that:
  - Are protected by an Electronic Security Perimeter (ESP) that are not part of the highest impact BES Cyber System (BCS) protected by the same ESP: or
  - Share CPU resources or memory with any part of the BCS, excluding VCA that are being actively remediated in an environment that isolates routable connectivity from BCS;
- Excludes Transient Cyber Assets

Access and Perimeter Model Modernization

Electronic Security Perimeter (ESP)	• Expanded to include logical boundaries defined by EAPs • Supports dynamic, session-level, and resource-level perimeters
Electronic Access Point (EAP)	• Now includes electronic policy enforcement points • No longer tied to a single network-edge interface
External Routable Connectivity (ERC)	• Reframed as access “through its ESP” • Removes assumptions about inside/outside network borders
Interactive Remote Access (IRA)	• Adds access to Management Interfaces • Includes routable-to-non-routable conversion scenarios (e.g., IP-to-serial) • Removes ownership references for remote clients (entity vs 3rd party)
Intermediate System	• Now defined as EACMS performing IRA restriction • Removes prescriptive placement requirements
Electronic Access Control or Monitoring Systems (EACMS)	• Expanded to include VCAs and SCI • Clarifies when protocol converters qualify as EACMS

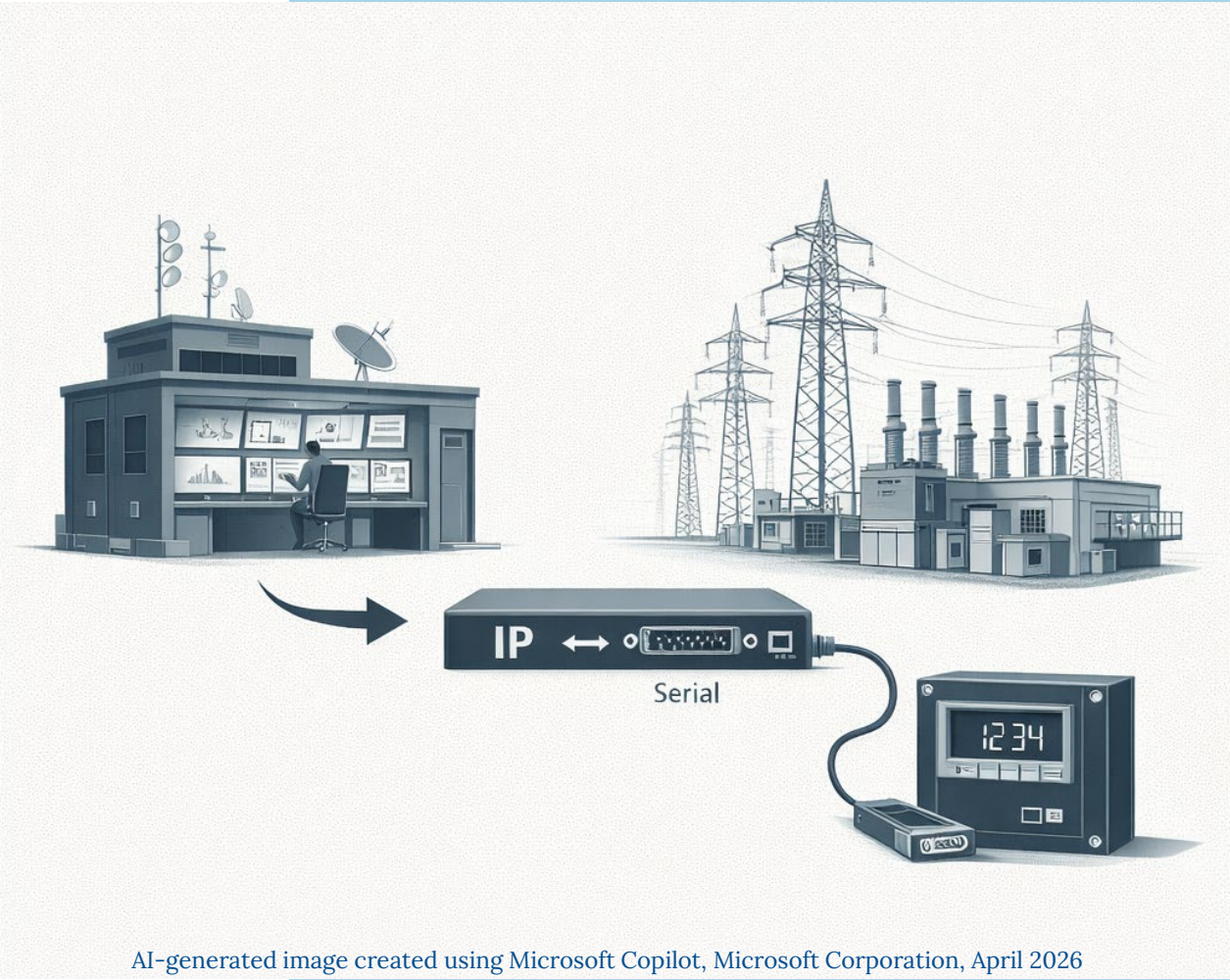
Electronic Access Control or Monitoring System

New Definition:

- Cyber System(s) that perform electronic access control or electronic monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems, including those not protected by an ESP used by the responsible entity to convert routable protocol communications to non-routable communication to a BCS.

Of Note:

- Shift from identifiable perimeter components to embedded and logical functionality
- Not always a standalone device
- Protocol conversion does not negate need for access control or monitoring
- Cyber Assets performing protocol conversion and access enforcement are EACMS



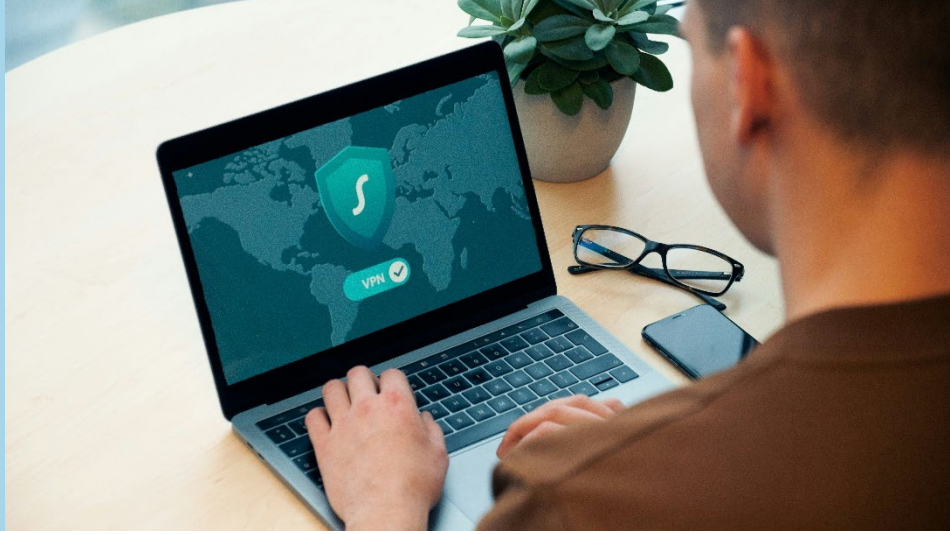
AI-generated image created using Microsoft Copilot, Microsoft Corporation, April 2026

Electronic Access Point & Electronic Security Perimeter

- Electronic Access Point
  - An electronic policy enforcement point or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets.
- 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 Electronic Access Points.
- Key Points
  - ESPs: logical and aggregated
  - EAPs: logical, virtual, and management access paths
  - Controlled access at defined entry points
  - Allowance for zero trust

External Routable Connectivity and Interactive Remote Access

Changes to definitions and how they relate



Changes to ERC

- Reframed to support other architectures
- Avoids prescribing a perimeter model
- ERC is not required for IRA
- Retains function as a scoping mechanism

Changes to IRA

- Simplified definition
- Types of access
- Removes reverence to ownership of remote client
- Removes embedded requirements
- No longer excludes serial connections

Interrelationship

- IRA can exist without ERC
- ERC remains scoping-level
- IRA now access-type
- Shift in CIP-005 applicability
- Zero Trust alignment
- Unified treatment of interactive access

Supporting Systems and Perimeters

Virtualization and Shared Cyber Infrastructure relates updates

Physical Access Control Systems (PACS)	Updated to include Cyber Systems (not just Cyber Assets) Adds SCI and VCA applicability
Physical Security Perimeter (PSP)	Now includes SCI as a protected system type
Removable Media	Adds SCI as a valid connection target Updates ESP language to “protected by” rather than “within”

Information and Incident-Related Terms

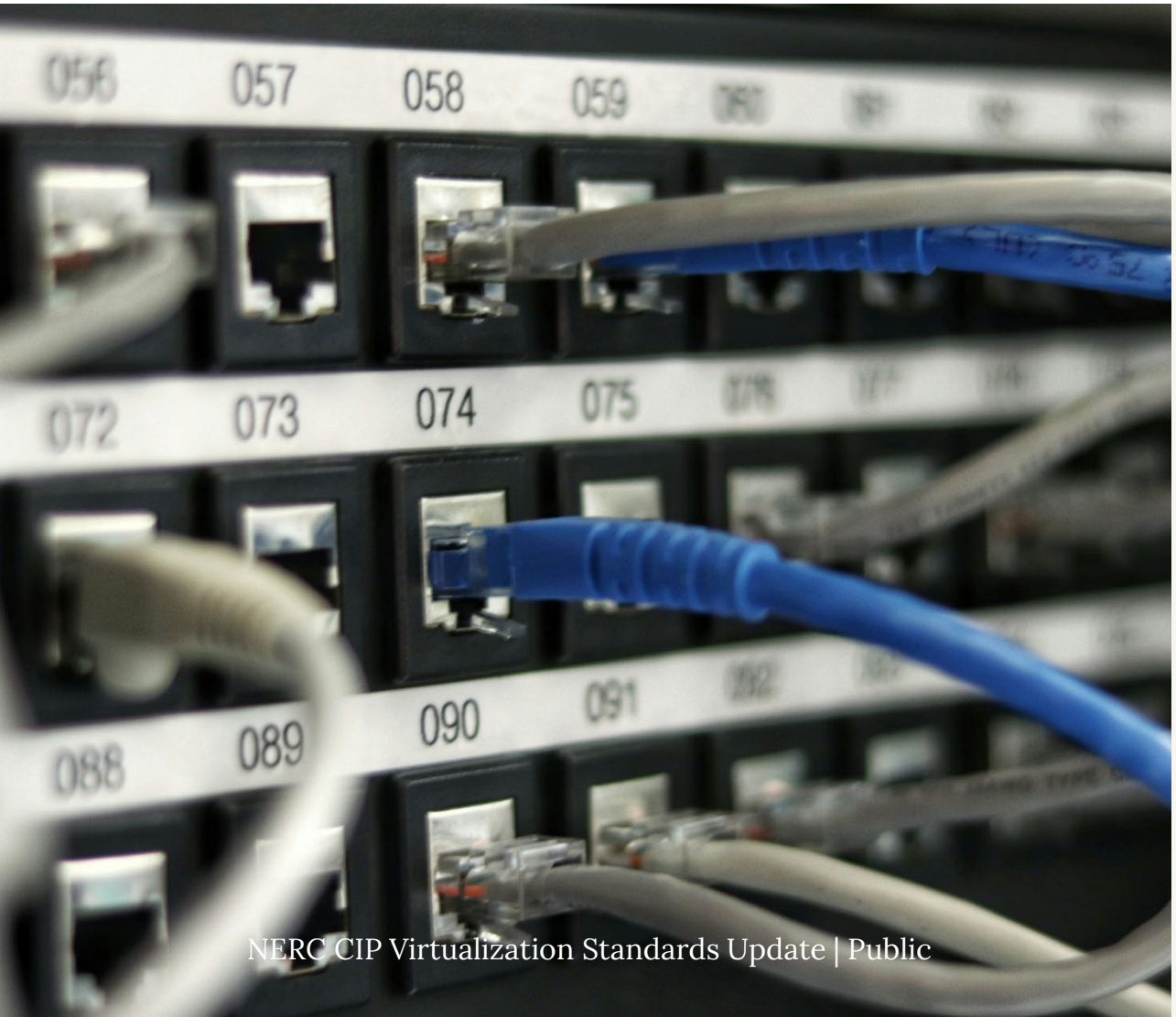
Conforming changes to information protection and incident reporting

BES Cyber System Information (BCSI)	• Adds SCI-related information as potential BCSI • Updates examples and terminology for consistency
Cyber Security Incident	• Adds SCI as a compromise target
Reportable Cyber Security Incident	• Adds SCI supporting a BCS as a reportable condition
CIP Senior Manager	• Removes outdated reference to CIP-002 through CIP-011 • Now applies to all CIP Cyber Security Standards

Overarching Changes

- Acronyms are now spelled out on first use in each standard, then abbreviated for each further use.
- Removed reference to Special Protection Systems from Functional Entities and Facilities sections.
- Removed Interchange Coordinator or Interchange Authority from Functional Entities section.
- “Technical Feasibility” removed in favor of “Per System Capability”.

Overarching Changes



- Exemptions
  - “Cyber Assets” changed to new term “Cyber Systems” in 4.3.2.1, 4.3.2.2.
  - New 4.3.2.3 Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.
  - Allows virtualization across multiple sites without discrete ESPs at each site.

Overarching Changes

- Wholesale formatting changes to conform with current NERC guidelines in Standards Process Manual and Reliability Standards Development Procedures.
- Applies to:
  - CIP-002
  - CIP-004
  - CIP-006 through CIP-011

Effective Dates section now references the Implementation Plan.

Background section removed from standard and preserved in Technical Rationale.

Guidelines and Technical Basis sections removed from standard and preserved in Technical Rationale.

C. Compliance section modified to match current NERC standard boilerplate language.

CIP-005-8

Electronic Security Perimeters

Requirement 1

Modified R1.1

"All applicable Cyber Assets" changed to "Applicable Systems".

"Shall reside within a defined ESP" changed to "must be protected by an ESP".

Requirement 1

New R1.2 (replaces old R1.3)

Applicable Systems

- High/Medium BCS with ERC replaces High/Medium EAP

New Requirement Language

- Permit only needed routable protocol communications, documenting the reason, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems.

Requirement 1

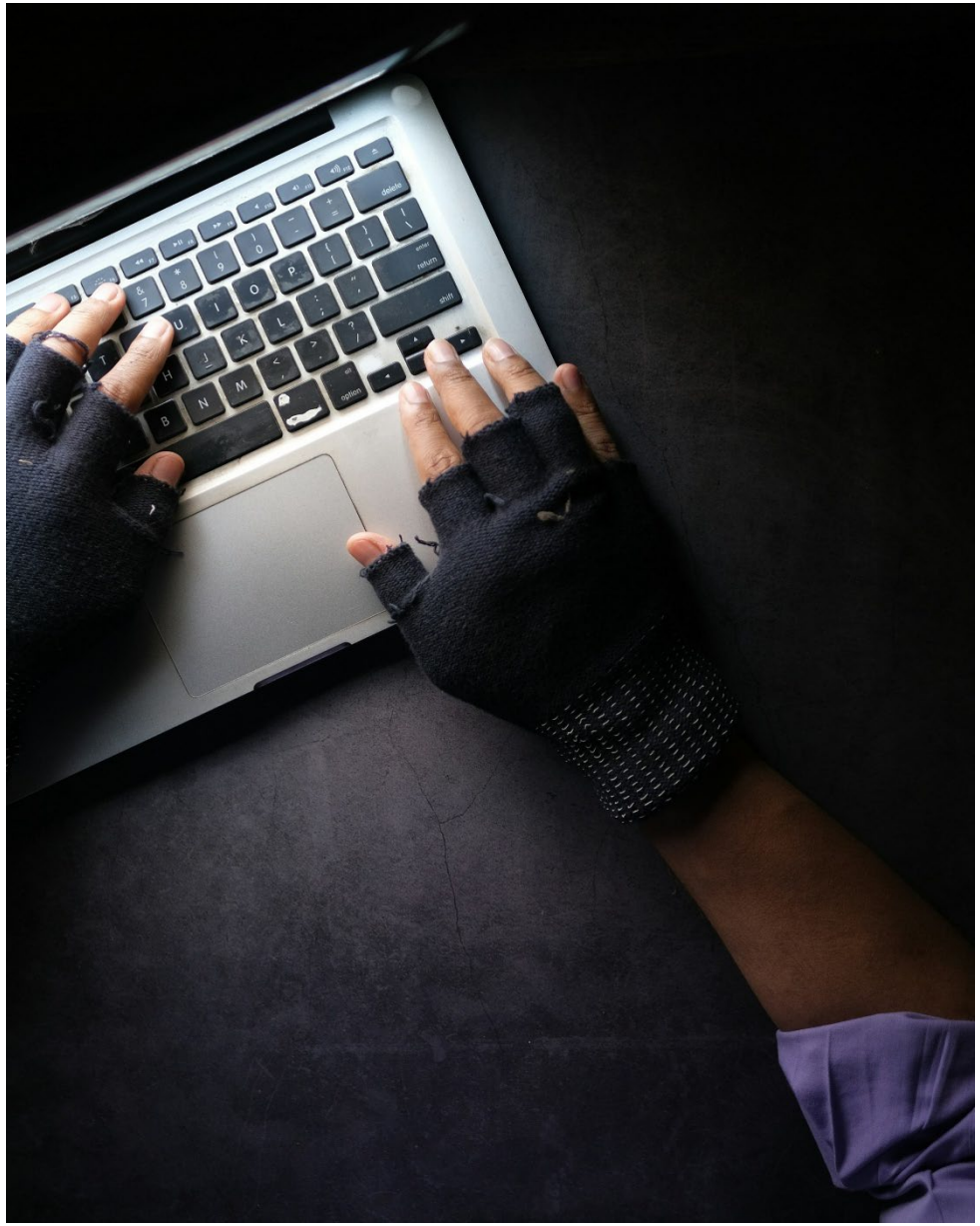
- New requirement **R1.3**
  - Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.
- Applicable to:
  - SCI supporting an Applicable System from Part 1.1.
  - EACMS, and their supporting SCI, that control an ESP for an Applicable system in Part 1.1.

Requirement 1

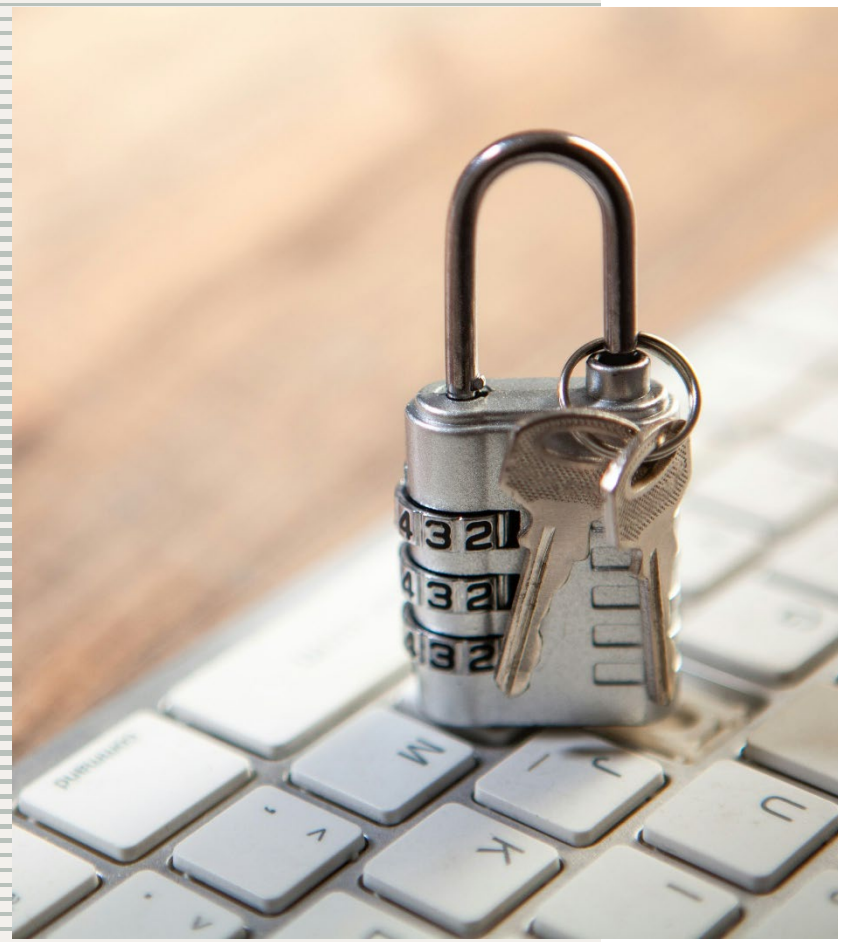
- New requirement **R1.4**
  - Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, and per system capability.
- Applicable to:
  - High impact BCS and their associated PCA
  - Medium impact BCS and their associated PCA
  - SCI supporting an Applicable System in this Part

Requirement 1

- New requirement **R1.5**
  - Have one or more methods for detecting known or suspected malicious routable protocol communications entering or leaving an ESP.
- Applicable to:
  - High impact BCS
  - Medium impact BCS at Control Centers



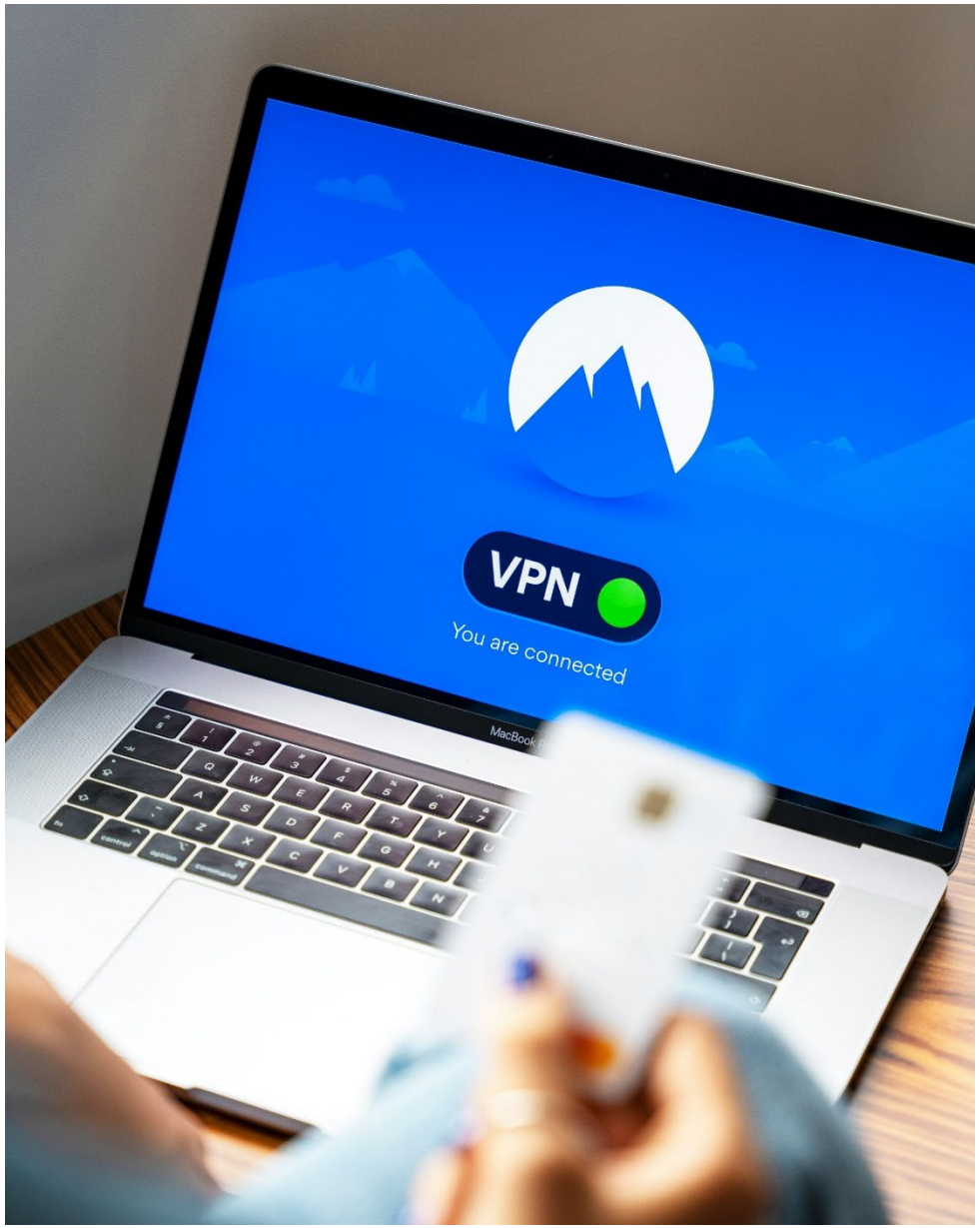
Requirement 1



- New requirement **R1.6** (modification of old requirement **R1.2**).
  - Protect the data traversing communication links used to span a single ESP between PSPs through the use of:
    - Confidentiality and integrity controls, 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.
- Applicable to:
  - High impact BCS
  - Medium impact BCS at Control Centers

Requirement 2

- Modified **R2.1**
  - Permit Interactive Remote Access (IRA), if any, only through an Intermediate System.
- Applicable to:
  - High Impact BCS and their associated PCA
  - Medium Impact BCS and their associated PCA
  - SCI supporting an Applicable System in this Part



Requirement 2

- Modified **R2.2**
  - Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.
- Applicable to:
  - Intermediate System(s) used to access an Applicable System in Part 2.1

Requirement 2

- Modified **R2.3**
  - Require multi-factor authentication to the Intermediate System for IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.
- Applicable to:
  - Intermediate System(s) used to access an Applicable System in Part 2.1

Requirement 2

Modified R2.4 and R2.5

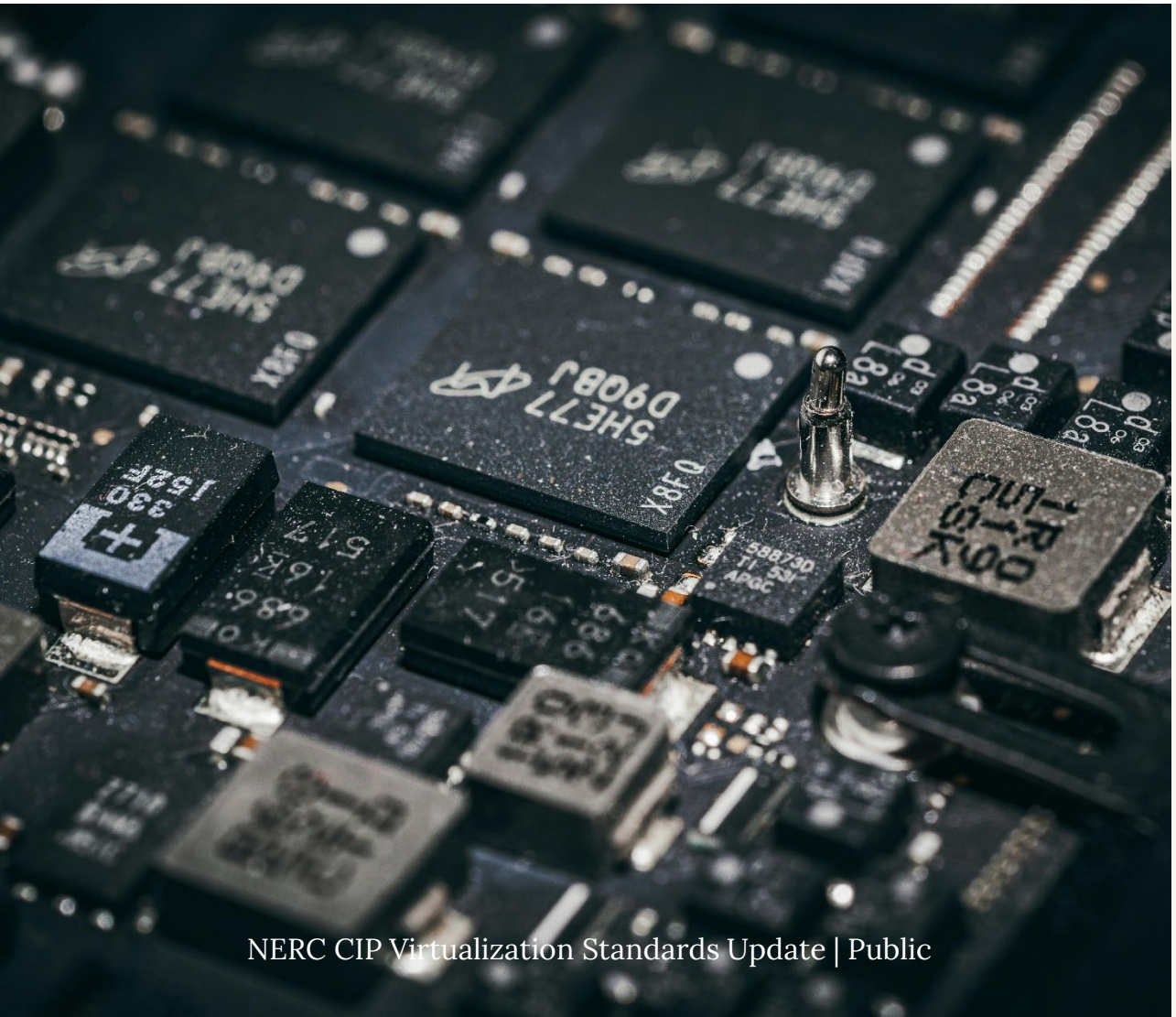
R2.4 & R2.5

- Requirement language unchanged.

Applicable to:

- High Impact BCS and their associated PCA,
- Medium Impact BCS and their associated PCA,
- SCI supporting an Applicable System in this Part.

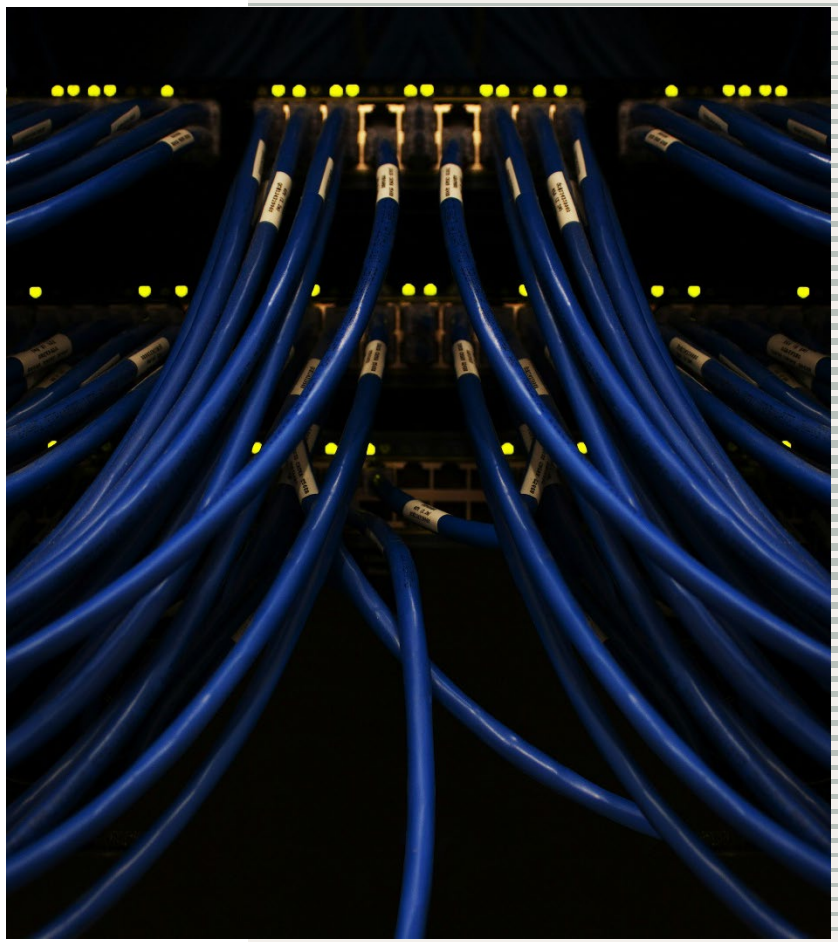
Requirement 2



- New **R2.6**
  - Prevent Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs.
- Applicable to:
  - Intermediate System(s) used to access an Applicable System in Part 2.1.

Requirement 2

- New **R2.7**
  - Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.
- Applicable to:
  - Intermediate System(s) used to access an Applicable System in Part 2.1.



Requirement 3

Modified **R3.1** & **R3.2**

- Requirement language unchanged.

Applicable to:

- EACMS and PACS associated with high impact BCS,
- EACMS and PACS associated with medium impact BCS with ERC,
- SCI supporting an Applicable System in this Part.

CIP-007-7

Systems Security Management

Requirement 1

Table R1

- Renamed “Ports and Services” to “System Hardening”.

Modified **R1.1**

- Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.

Applicable to:

- High impact BCS and their associated:
  - 1. EACMS; 2. PACS; and 3. PCA
- Medium impact BCS with ERC and their associated:
  - 1. EACMS; 2. PACS; and 3. PCA
- SCI supporting an Applicable System in this Part.

Requirement 1

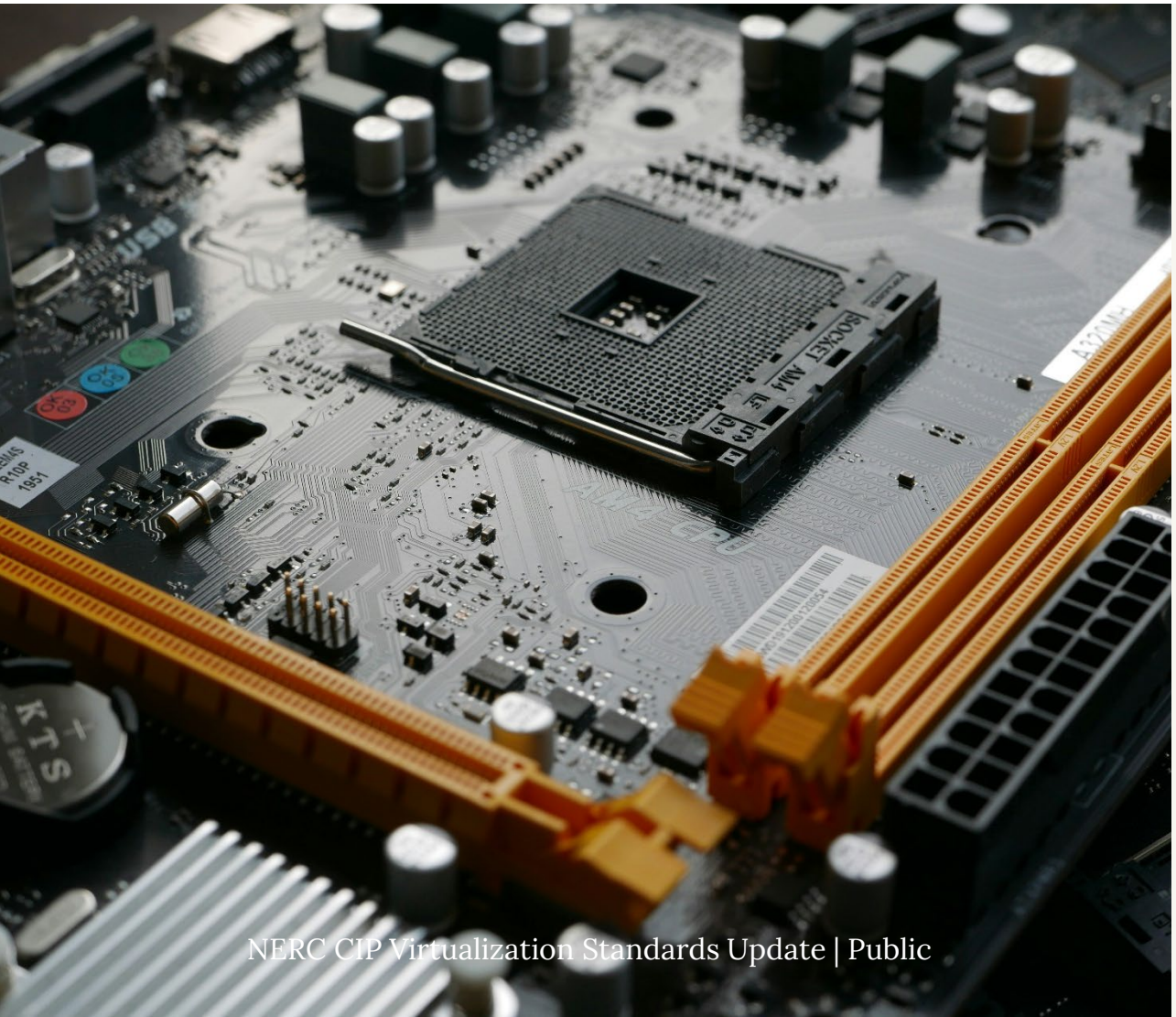
Modified **R1.2**

- Requirement language unchanged.

Applicable to:

- High impact BCS and their associated:
  - 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.
- Medium impact BCS at Control Centers and their associated:
  - 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.
- SCI supporting an Applicable System in this Part.

Requirement 1



- New **R1.3**
  - Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are, or are associated with, a medium or high impact BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.
- Applicable to:
  - SCI supporting either:
    - High impact BCS or their associated PCA.
    - Medium impact BCS or their associated PCA.

Requirement 2

R2.1 – R2.4

Modified **R2.1**	• “applicable cyber assets” changed to “Applicable Systems”.
Modified **R2.2** & **R2.3**	• “cyber” added before “security patch”.
R2.4	• Requirement language unchanged.
Added Applicability **R2.1** – **R2.4**:	• SCI supporting an Applicable System in this Part.

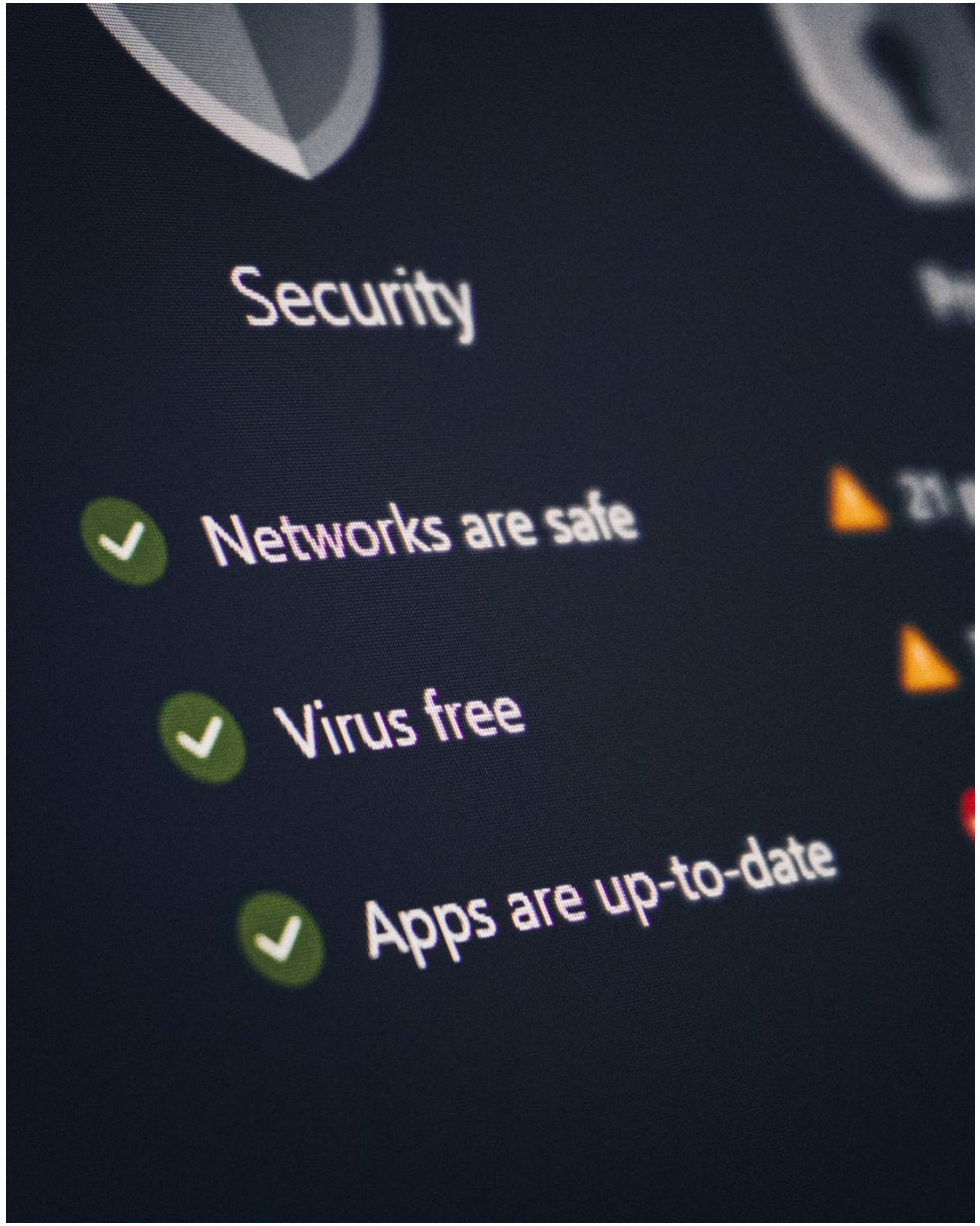
Requirement 3

R3.1 – R3.3

- Requirement language unchanged.

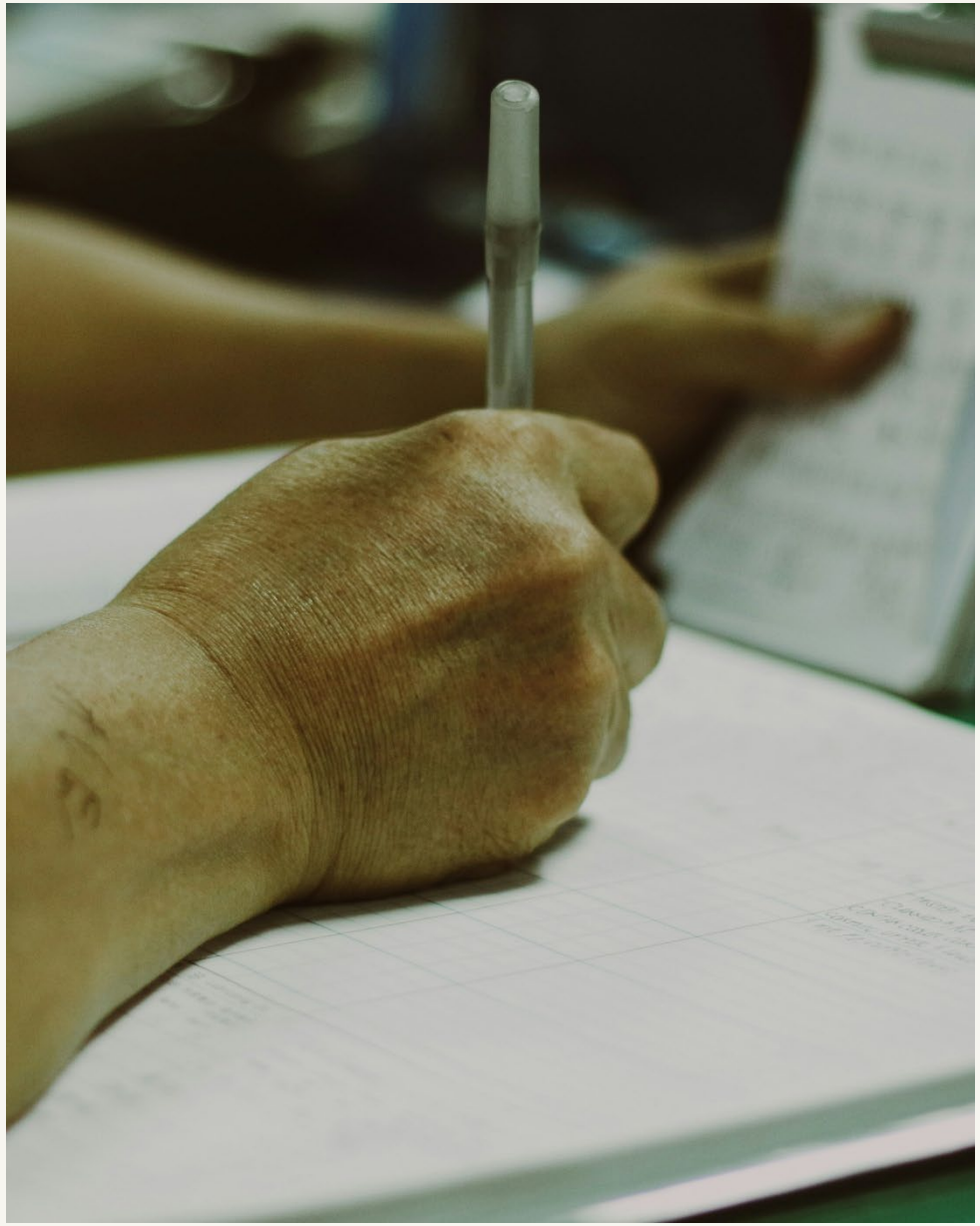
Added Applicability R3.1 – R3.3:

- SCI supporting an Applicable System in this Part.



Requirement 4

- Modified **R4.1**
  - Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events:
    - 4.1.1. Detected successful login attempts;
    - 4.1.2. Detected failed access attempts and failed login attempts; and
    - 4.1.3. Detected malicious code.
- Added Applicability:
  - SCI supporting an Applicable System in this Part.



Requirement 4

R4.2 - R4.4

Modified **R4.2**	Modified R4.3	Modified R4.4	Added Applicability R4.2 – R4.4
• Generate alerts for security events that the Responsible Entity determines necessitates an alert that includes, as a minimum, each of the following types of events, per system capability: • 4.2.1. Detected malicious code from Part 4.1; and • 4.2.2. Detected failure of Part 4.1 event logging.	• Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	• Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	• SCI supporting an Applicable System in this Part

Requirement 5

Modified **R5.1**, **R5.6**, & **R5.7**

- Changed “where technically feasible” to “per system capability”.

R5.2 – R5.4

- Requirement language unchanged.

Modified **R5.5**

- “Cyber Asset” changed to “Applicable System”.

Added Applicability **R5.1 – R5.7**

- SCI supporting an Applicable System in this Part.

CIP-010-5

Configuration Change Management & Vulnerability Assessments

Requirement 1

Added clarifying language “to manage configuration changes, individually or by group,” to R1.

Previous version of R1.1, R1.2, & R1.3 were removed.

Requirement 1

- New **R1.1** (modified previous **R1.4**)
  - Authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.
- Added Applicability:
  - SCI supporting an Applicable System in this Part.

Requirement 1

- New **R1.2** (modified previous **R1.5**)
  - **1.2.1**. Prior to implementing any change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and
  - **1.2.2**. Document the results of the testing and, 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 between the test and production environments.

Requirement 1

New **R1.3** (modified previous **R1.6**)

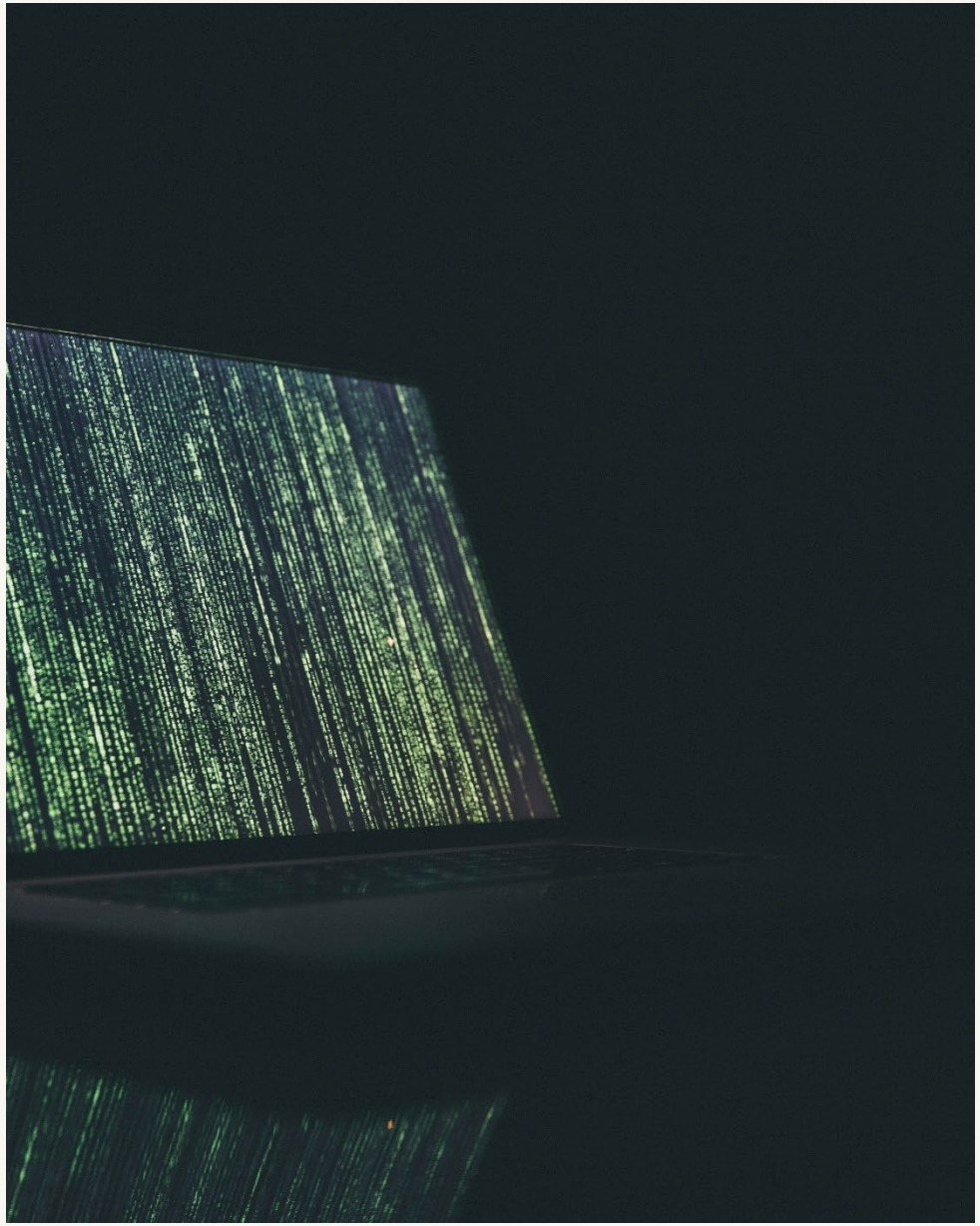
- Prior to the installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source:
  - 1.3.1. Verify the identity of the software source; and
  - 1.3.2. Verify the integrity of the software obtained from the software source.

Added Applicability:

- SCI supporting an Applicable System in this Part.

Requirement 1

- New **R1.4**
  - As a part of the changes authorized per Part 1.1, verify that the behavior(s) of the altered cyber security controls were not adversely affected.
- Applicable to:
  - 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
  - SCI supporting an Applicable System in this Part.



Requirement 2

Modified **R2.1**

- Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following:
  - 2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility;
  - 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI;
  - 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches.
  - 2.1.4. Configuration of malicious code protection methods;
  - 2.1.5. Configuration of security event logging or alerting;
  - 2.1.6. Configuration of authentication methods; and
  - 2.1.7. Changes to the enabled or disabled status of accounts.
  - Document and investigate detected unauthorized changes.

Added Applicability:

SCI supporting an Applicable System in this Part.

Requirement 3

R3.1

- Requirement language unchanged.

Modified **R3.2**

- At least once every 36 calendar months, per system capability:
  - 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and
  - 3.2.2 Document the results of the testing and, 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 between the test and production environments.

Added Applicability:

- SCI supporting an Applicable System in this Part.

Requirement 3

- Modified **R3.3**
  - Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for:
    - Like replacements or additions with a previously assessed configuration of an existing Applicable System; or
    - CIP Exceptional Circumstance
- **R3.4**
  - Requirement language unchanged.
- Added Applicability:
  - SCI supporting an Applicable System in this Part.

Requirement 4 & Attachment 1 & 2

Modified **R4**	• Added “associated SCI” to requirement language.
Attachment 1	• “Live operating system…” moved from **1.3** to **1.4**. • “System hardening; or” added to **1.4**. • Clarifying language and formatting changes.
Attachment 2	• Example language added to reflect changes in **Attachment 1**.

Implementation Plan

- Standards and Definitions subject to enforcement July 1, 2028
- Entities may choose to comply earlier
  - Select an Early Adoption Date
  - Notify Regional Entity with 15 calendar days
- CIP-002-8 supersedes CIP-002-7 Implementation Plan
  - Phased-in implementation for higher impact level categorization
  - If no impact changes: July 1, 2028

Early Adoption Dates	
Option 1	January 1, 2027
Option 2	July 1, 2027
Option 3	January 1, 2028

CIP-002-8

BES Cyber System Categorization

CIP-002-8 Overview and Implementation

CIP-002-8 modifications from Project 2021-03:

- Control Center definition and Attachment 1 Criterion 2.12 modified
- Addresses the categorization of Transmission Owner Control Centers (TOCCs) performing the functional obligations of a Transmission Operator (TOP)

Implementation Plan

- Effective date is July 1, 2028
- Comply with Requirement 2 within 15 months of its last performance
- BES Cyber Systems that result in higher impact level – July 1, 2030

CIP-003-11 Security Management Controls

CIP-003-11 Updates and Implementation

CIP-003-10

- Updated to support virtualization, more system-centric than asset-centric
- No new Requirements

CIP-003-11

- Built upon the modernized framework of CIP-003-10 and added enhanced electronic access controls requirements in R2, Attachment 1;
  - Permit only necessary inbound and outbound electronic access.
  - Detect known or suspected malicious communications.
  - User authentication prior to permitting user access to a network containing a low impact BCS or SCI that supports a low impact BCS.
  - Protection of user authentication information while in transit between Cyber Systems outside the asset.
  - One or more method of determining vender electronic access.
  - One or more method of disabling vendor electronic access.

Implementation Plan

- Effective Date is July 1st, 2029.
  - 36 months was used considering that entities would need to implement new controls to meet R2, Attachment 1, including potentially; revised policies, new staffing, system reconfigurations, and new equipment.

Additional Resources

Project 2016-02 Modifications to CIP Standards				Project 2021-03 CIP-002
Implementation Plan				CIP-002-8
CIP-002-7	Technical Rationale	CIP-003-10	Technical Rationale	Implementation Plan
CIP-004-8	Technical Rationale	CIP-005-8	Technical Rationale	Technical Rationale
CIP-006-7	Technical Rationale	CIP-007-7	Technical Rationale	**Project 2023-04 Mods to CIP-003**
CIP-008-7	Technical Rationale	CIP-009-7	Technical Rationale	CIP-003-11
CIP-010-5	Technical Rationale	CIP-011-4	Technical Rationale	Implementation Plan
CIP-013-3	Technical Rationale	Definitions	Technical Rationale	Technical Rationale

NPCC

Questions?

Contact Us: npcc.org/contact

NPCC Standards and Criteria