NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

# Modifications to CIP Standards - Draft 5

## CIP-003, CIP-004, CIP-005, CIP-007, CIP-010 and Definitions

Project 2016-02 SDT

October 2023

**RELIABILITY | RESILIENCE | SECURITY**

# Agenda

- Administrative
- SDT Overview
- What We Heard
- Standards\Definitions Modifications
  - CIP-010
  - CIP-003
  - CIP-005
  - CIP-004
  - CIP-007
  - Other Definitions
- Topical Discussions
- Implementation Plan
- Q&A

# 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 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 |
| | Scott Klauminzer | Tacoma Public Utilities |
| | Sharon Koller | ATC, LLC |
| | Heather Morgan | EDP Renewables |
| | Mark Riley | Associated Electric Cooperative, Inc. |

# Q&A

*Ask anonymously at anytime!*

*Vote other's questions up/down*

*Answer Polls and Surveys*

**Slido Event Code: 201602f**

RELIABILITY | RESILIENCE | SECURITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Opening Remarks

*Join at Slido.com Slido Event Code: 201602f*

- **Webinar Purpose:** High level overview of modifications for Project 2016-02 Modification to CIP Standards
- **Draft 5 Posting Duration:** October 3, 2023 – November 29, 2023
  - 45-day comment and ballot period
- **Standards Affected for this Posting:** CIP-003, CIP-004, CIP-005, CIP-007, and CIP-010

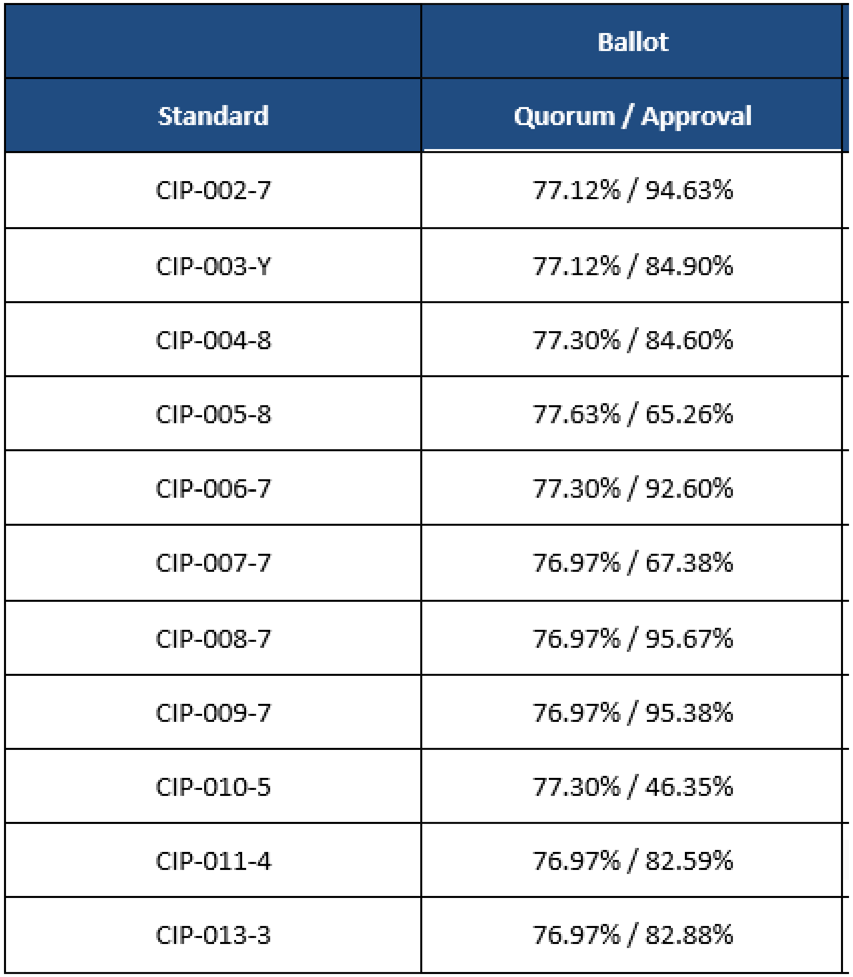
# Overview

*Join at Slido.com Slido Event Code: 201602f*

- Project 2016-02 SAR and Scope
  - FERC Order 822, 843
  - V5TAG Items
    - Virtualization
    - IRA to serial
    - TO Control Center Criteria
  - CEC additions, RFI, etc.

# Draft 4 Ballot Results

*Join at Slido.com Slido Event Code: 201602f*



| | Ballot |
|---|---|
| Standard | Quorum / Approval |
| CIP-002-7 | 77.12% / 94.63% |
| CIP-003-Y | 77.12% / 84.90% |
| CIP-004-8 | 77.30% / 84.60% |
| CIP-005-8 | 77.63% / 65.26% |
| CIP-006-7 | 77.30% / 92.60% |
| CIP-007-7 | 76.97% / 67.38% |
| CIP-008-7 | 76.97% / 95.67% |
| CIP-009-7 | 76.97% / 95.38% |
| CIP-010-5 | 77.30% / 46.35% |
| CIP-011-4 | 76.97% / 82.59% |
| CIP-013-3 | 76.97% / 82.88% |

# Virtualization Overview

*Join at Slido.com Slido Event Code: 201602f*

- New terms – Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI)
- SCI vs. “All-in”
- CIP-010 for dynamic environments
- CIP-005 and Zero Trust models
- Interactive Remote ACCESS to non-routable (serial) BCA/BCS

# What we heard

*Join at Slido.com Slido Event Code: 201602f*

## Major Comment themes

- We are getting close! But still needs some fixes!
- Provide further clarifications for…
  - The scope of change and order of operations in CIP-010
  - Intermediate Systems and handling of IRA in CIP-005
  - Treatment of  Management Interfaces
  - Classifications of Serial to IP Converters
  - Treatment of SCI scenarios that host only EACMS/PACS
  - Handling sharing of CPU / Memory (Affinity)
- Relationship to Cloud Technologies

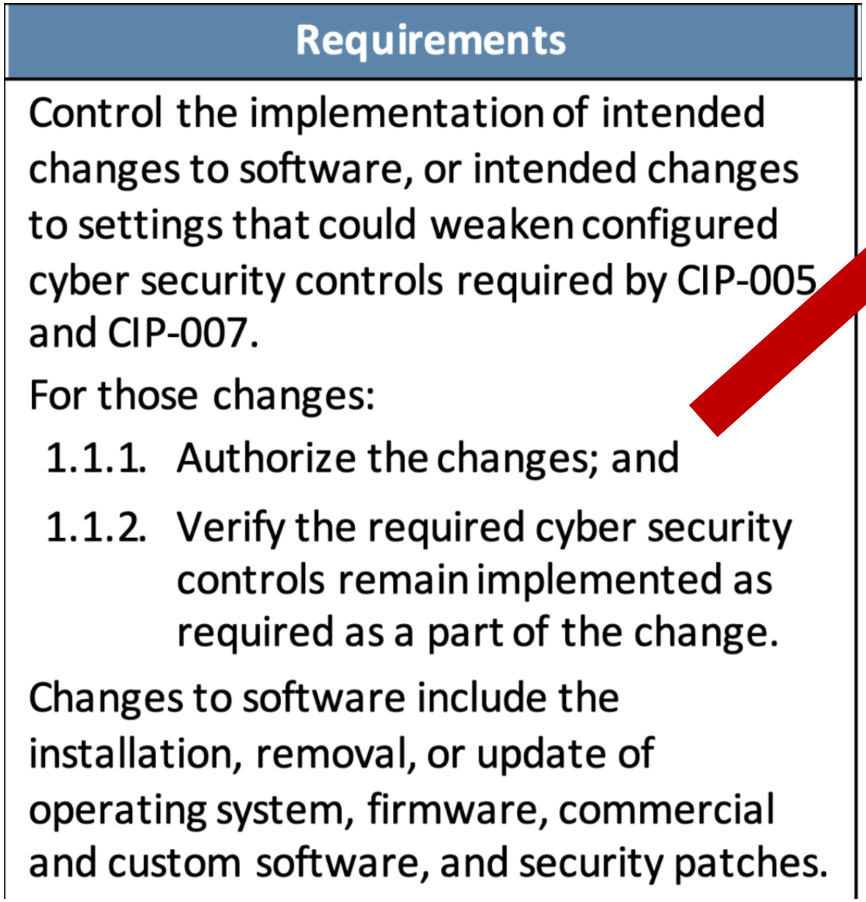
# Standards Updates

# CIP-010 Changes

- *Provide further clarifications for the scope of change in CIP-010.*
- *Clarifications for order of operations issues associated with changes.*
- *Alignment of R1 and R2 Scope.*
- *Modifications to clarify requirements for monitoring changes.*
- *Clarifications for ‘like’ / ‘same kind’ replacements / additions.*
- *Transient Cyber Asset controls – reverting to current approved*

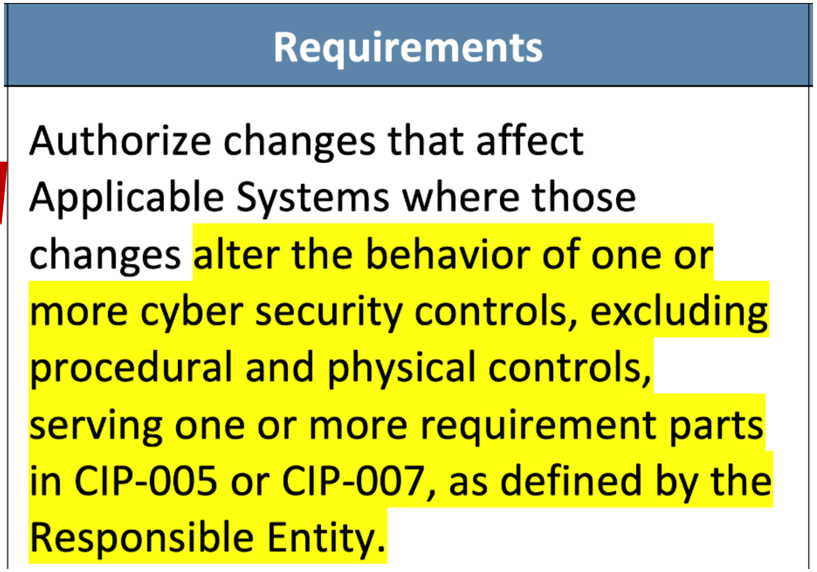
# CIP-010-5 R1 Part 1.1.1 → Part 1.1

## *Draft 4*



| Requirements |
|---|
| Control the implementation of intended changes to software, or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007.<br>For those changes:<br>1.1.1. Authorize the changes; and<br>1.1.2. Verify the required cyber security controls remain implemented as required as a part of the change.<br>Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches. |

## *Draft 5*



| Requirements |
|---|
| 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. |

*Scoping:*

1. *Alter behavior of control*
2. *Exclude physical & procedural*
   - *Not process docs*
3. *Serving one or more CIP R-Ps*
4. *Defined by Entity*

# CIP-010-5 R1 Part 1.1

*Join at Slido.com Slido Event Code: 201602f*

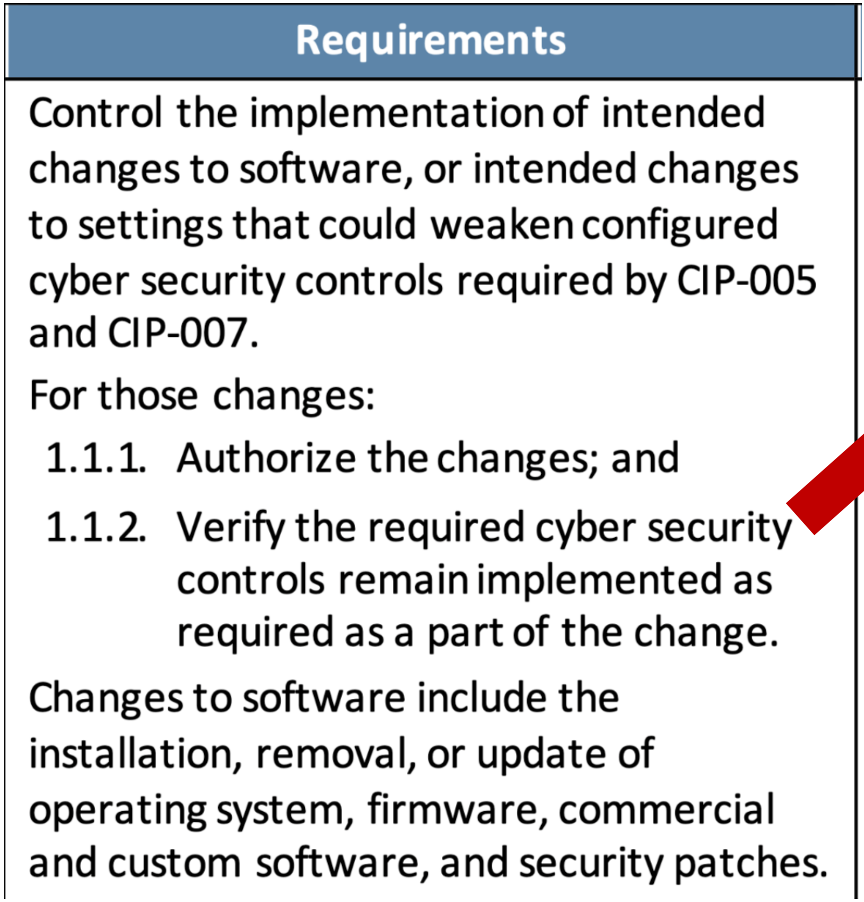
*Examples of changes that may alter the behavior of one or more cyber security controls may include, but are not limited to:*

- *Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from which Applicable Systems will be instantiated (CIP-007 R1.1, R2)*
- *Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1)*
- *Configuration changes affecting the establishment of, or access control through, an ESP (CIP-005 R1, R2)*
- *Configuration of malicious code prevention methods (CIP-007 R3)*
- *Configuration of security event logging/alerting (CIP-007 R4)*
- *Configuration changes to authentication methods (e.g., a password enforcement policy change, but not users changing their password) (CIP-007 R5)*
- *Configuration changes to CPU/memory sharing of VCAs on SCI (CIP-007 R1.3)*

# CIP-010-5 R1
# Part 1.1.2 → Part 1.4

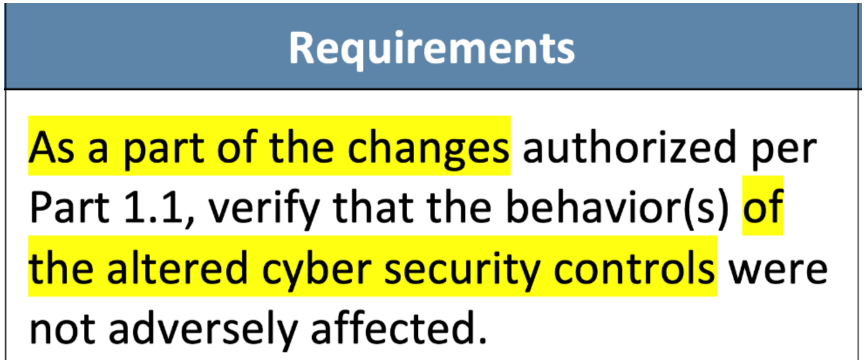
*Join at*
*Slido.com*
*Slido Event*
*Code: 201602f*

## *Draft 4*



| Requirements |
|---|
| Control the implementation of intended changes to software, or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007.<br>For those changes:<br>1.1.1. Authorize the changes; and<br>1.1.2. Verify the required cyber security controls remain implemented as required as a part of the change.<br>Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches. |

## *Draft 5 R1 Part 1.4*



| Requirements |
|---|
| 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. |

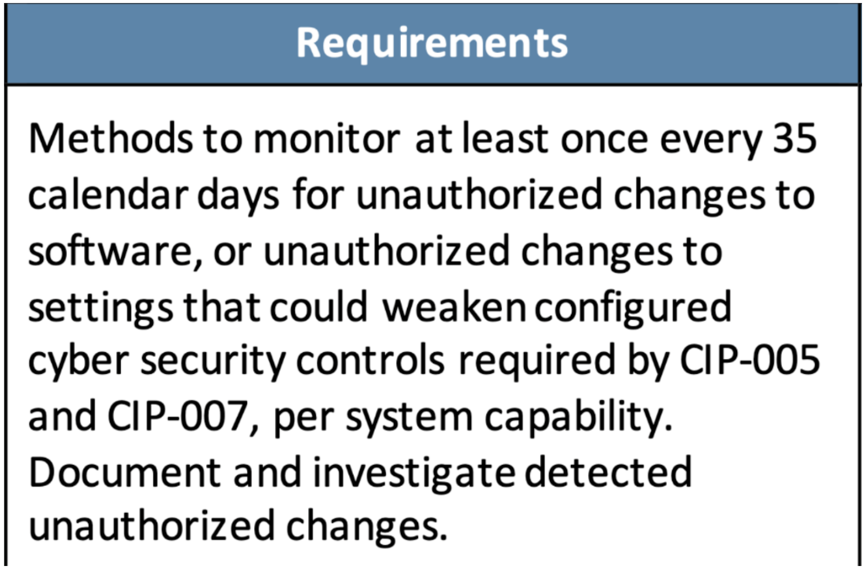
- *As part of change…*
- *From 1.1*
- *Verify behavior of altered controls*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# CIP-010-5 R2

*Join at Slido.com Slido Event Code: 201602f*

## *Draft 4*

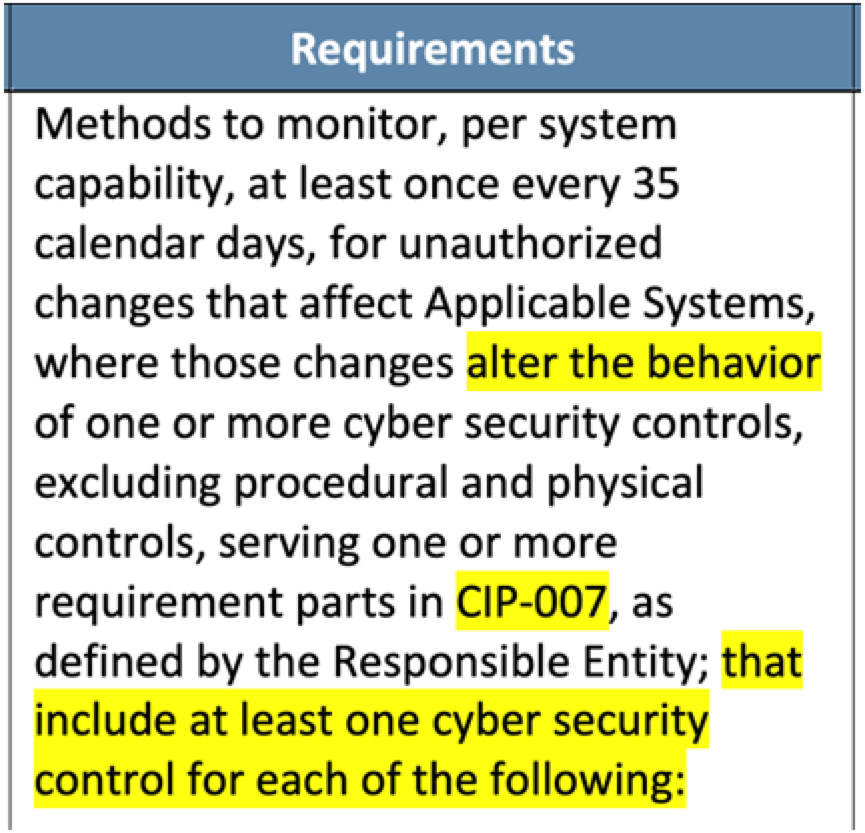


| Requirements |
|---|
| Methods to monitor at least once every 35 calendar days for unauthorized changes to software, or unauthorized changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007, per system capability. Document and investigate detected unauthorized changes. |

*Scoping:*

1. *Alter behavior of control*
2. *Exclude physical & procedural*
    - *Not process docs*
3. *Serving one or more CIP R-Ps*
4. *Defined by Entity*

## *Draft 5*



| Requirements |
|---|
| 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: |

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

# CIP-010-5 R2

*Join at Slido.com Slido Event Code: 201602f*

## *Draft 5 R2 Part 2.1*

**Requirements**

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;

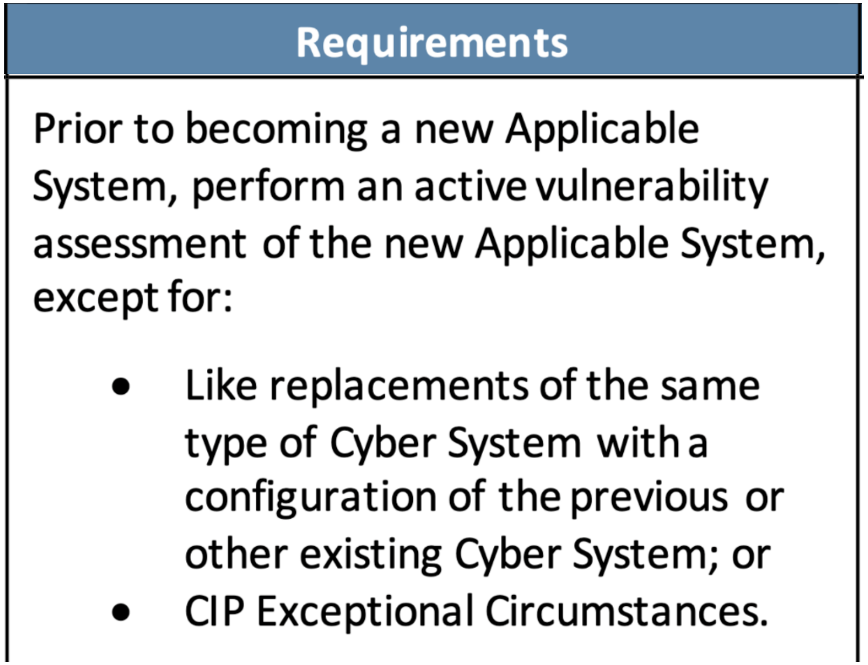
2.1.6. Configuration of authentication methods; and

2.1.7. Changes to enabled or disabled status of accounts.

Document and investigate detected unauthorized changes.

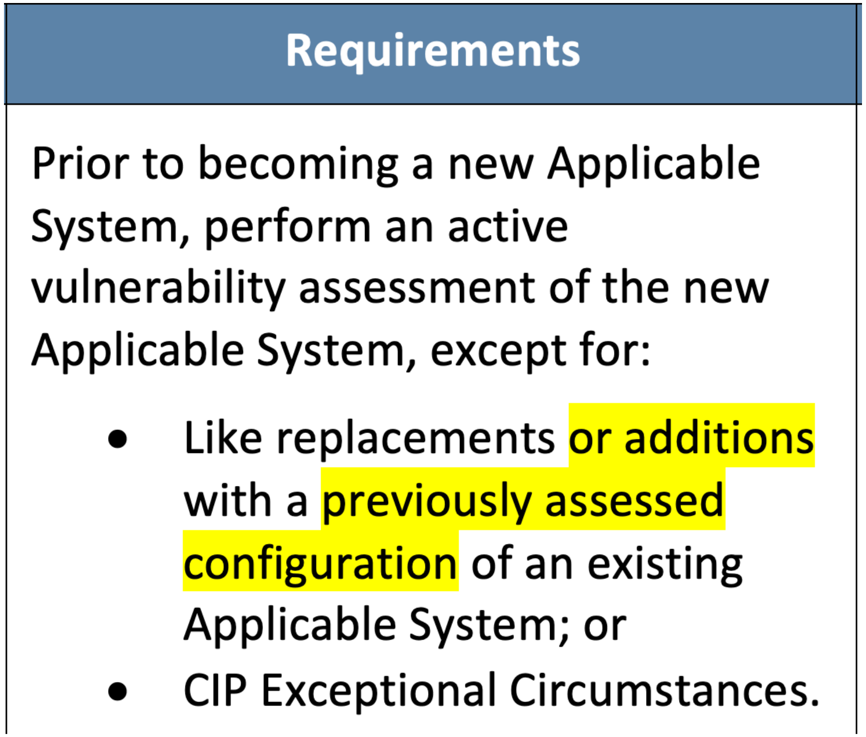
# CIP-010 R3 Part 3.3

## *Draft 4*



| Requirements |
|---|
| Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for:<br>• Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System; or<br>• CIP Exceptional Circumstances. |

## *Draft 5*



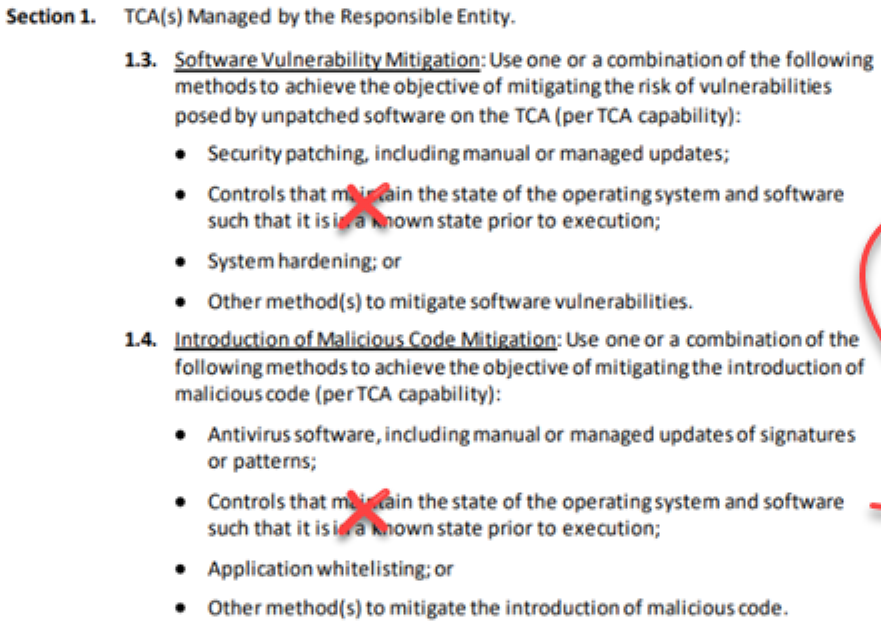
| Requirements |
|---|
| Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for:<br>• Like replacements or additions with a previously assessed configuration of an existing Applicable System; or<br>• CIP Exceptional Circumstances. |

- *Same goes for additions: Do not need to repeat vulnerability assessment if using a configuration you've already assessed.*

# CIP-010-5 R4 Attachment 1 Section 1

*Join at Slido.com Slido Event Code: 201602f*

## *Draft 4*



**Section 1.** TCA(s) Managed by the Responsible Entity.

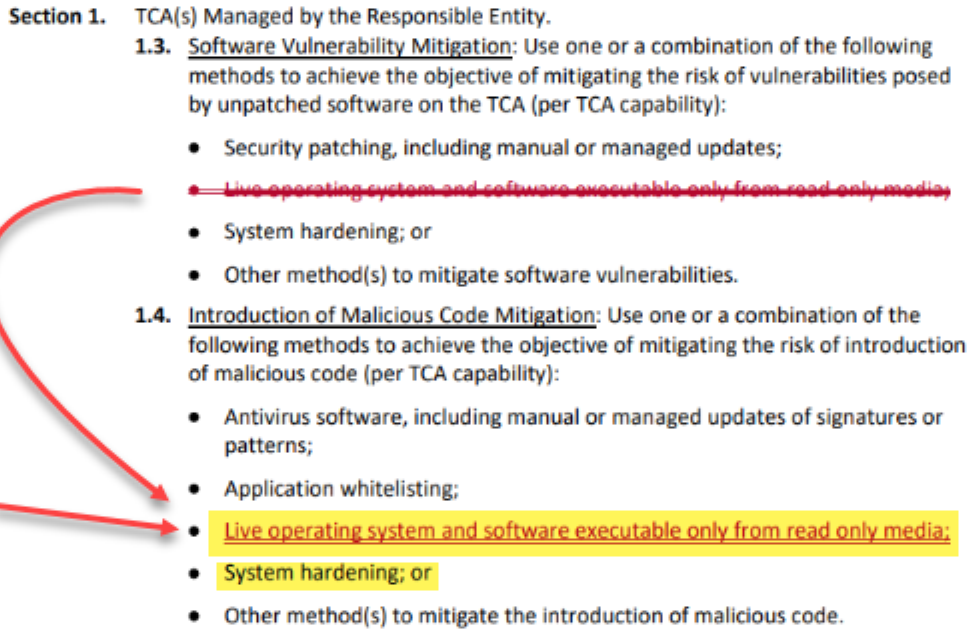
**1.3.** Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Security patching, including manual or managed updates;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

**1.4.** Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

## *Draft 5*



**Section 1.** TCA(s) Managed by the Responsible Entity.

**1.3.** Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Security patching, including manual or managed updates;
- ~~Live operating system and software executable only from read only media;~~
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

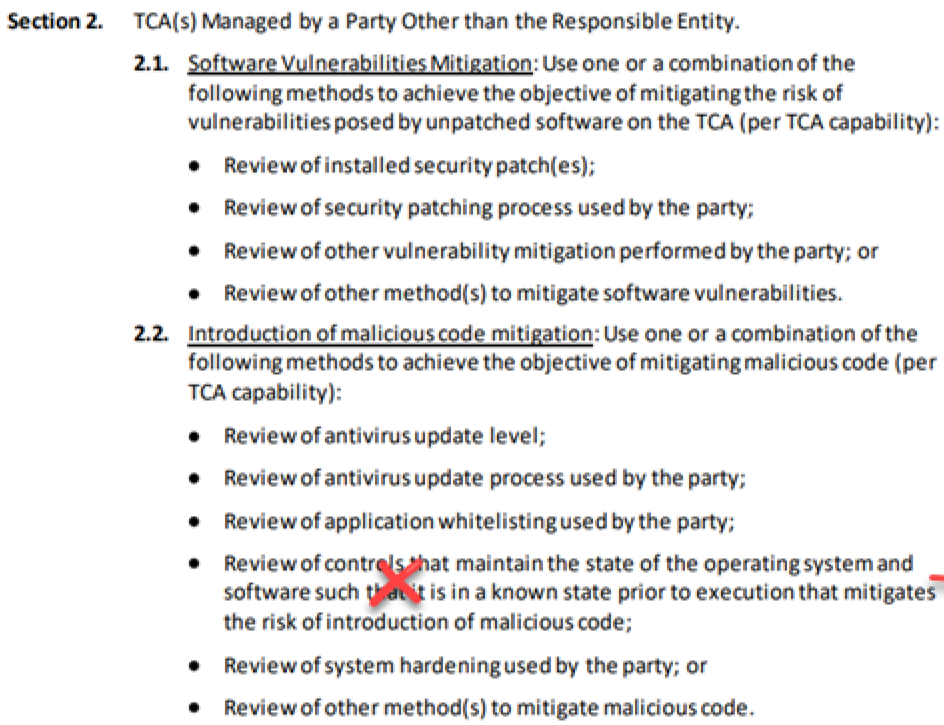
**1.4.** Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting;
- Live operating system and software executable only from read only media;
- System hardening; or
- Other method(s) to mitigate the introduction of malicious code.

# CIP-010-5 R4 Attachment 1 Section 2

*Join at Slido.com Slido Event Code: 201602f*

## *Draft 4*



**Section 2.** TCA(s) Managed by a Party Other than the Responsible Entity.

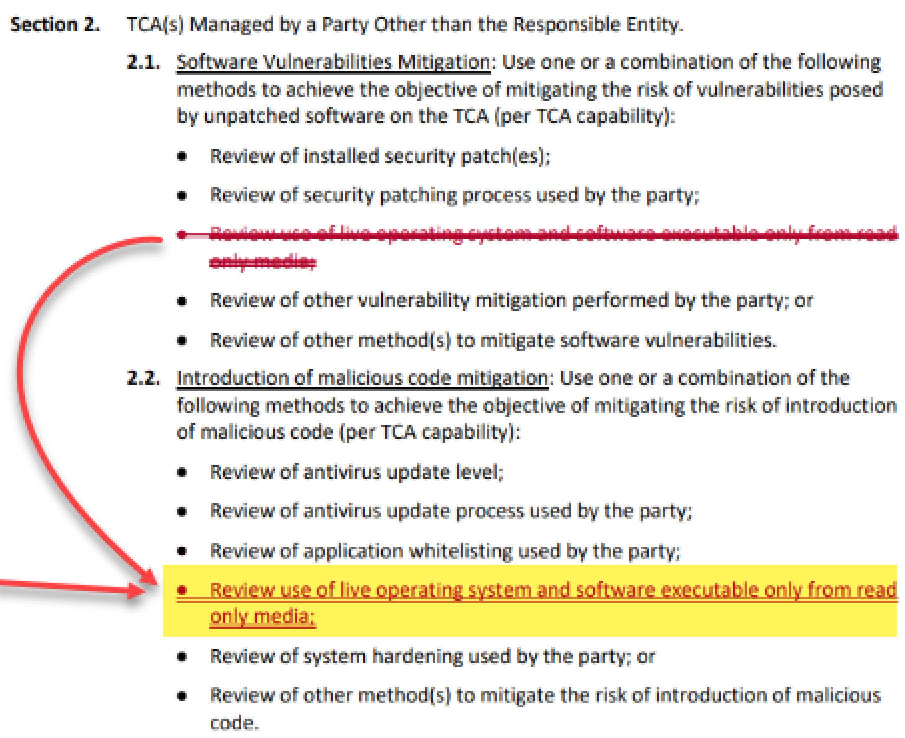
**2.1.** Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Review of other method(s) to mitigate software vulnerabilities.

**2.2.** Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such ~~that~~ it is in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate malicious code.

## *Draft 5*



**Section 2.** TCA(s) Managed by a Party Other than the Responsible Entity.

**2.1.** Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- ~~Review use of live operating system and software executable only from read only media;~~
- Review of other vulnerability mitigation performed by the party; or
- Review of other method(s) to mitigate software vulnerabilities.

**2.2.** Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read only media;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

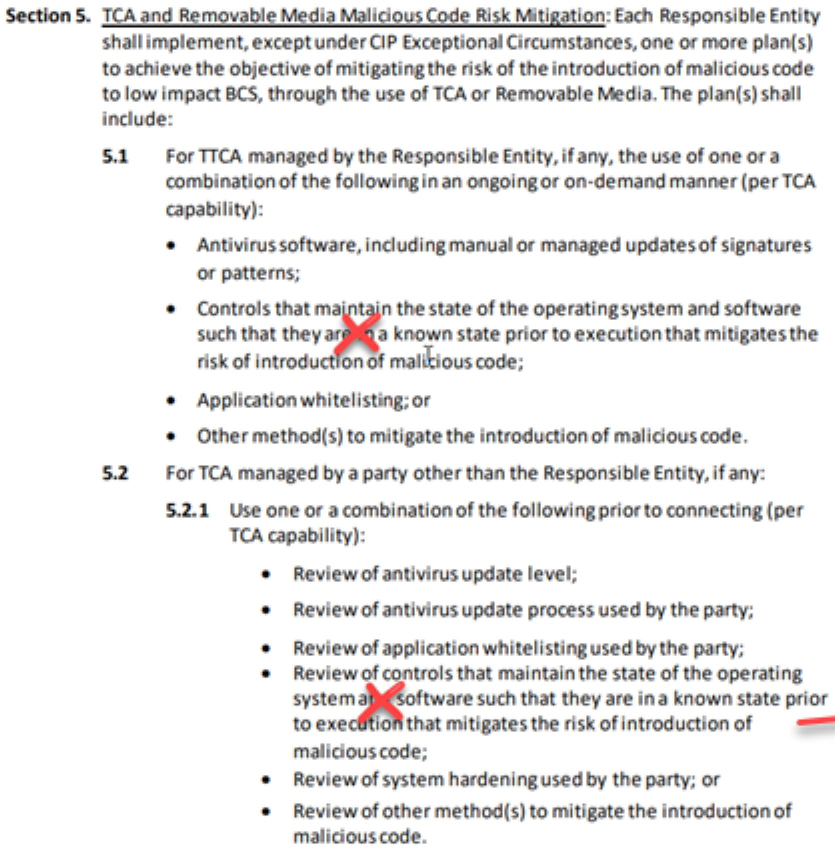
# CIP-003 Changes

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# CIP-003-10 R2 Attachment 1 Section 5

*Join at Slido.com Slido Event Code: 201602f*

## *Draft 4*



**Section 5.** TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

**5.1** For TTCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

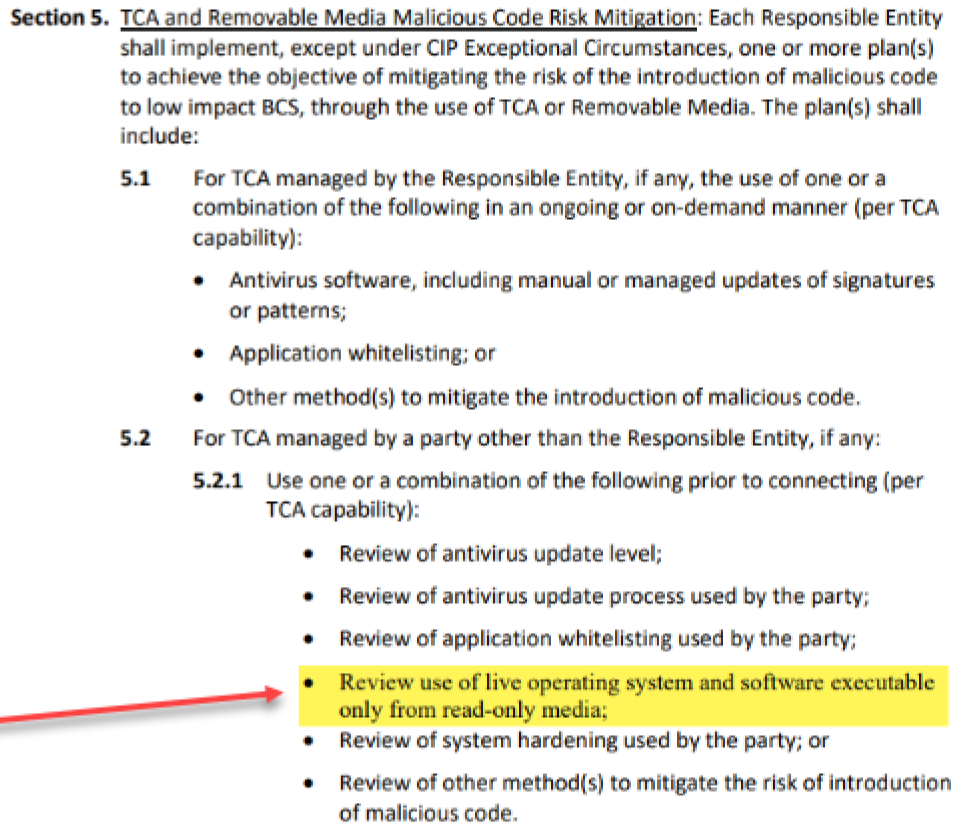
- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

**5.2** For TCA managed by a party other than the Responsible Entity, if any:

**5.2.1** Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the introduction of malicious code.

## *Draft 5*



**Section 5.** TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

**5.1** For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

**5.2** For TCA managed by a party other than the Responsible Entity, if any:

**5.2.1** Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

# CIP-005 Changes

# CIP-005 Changes – Treatment of Interm. Systems

Join at Slido.com Slido Event Code: 201602f

## Draft 4

*Interactive Remote Access Definition*

User-initiated electronic access by a person using a routable protocol:

- To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);
- That is converted by the Responsible Entity to a non-routable protocol to a Cyber System; or
- To a Management Interface of Shared Cyber Infrastructure.

Interactive Remote Access does not include:

- Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs;
- Communication that originates from an Intermediate System; or
- System-to-system process communication

## Draft 5

*Interactive Remote Access Definition*

User-initiated electronic access by a person using a routable protocol :

- To a Cyber System protected by an Entity's Electronic Security Perimeter(s) (ESP);
- That is converted by the Responsible Entity to a non-routable protocol that allows access to a Cyber System; or
- To a Management Interface.

Interactive Remote Access does not include:

- Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs ; or
- System-to-system process communication.

*Key Changes:*

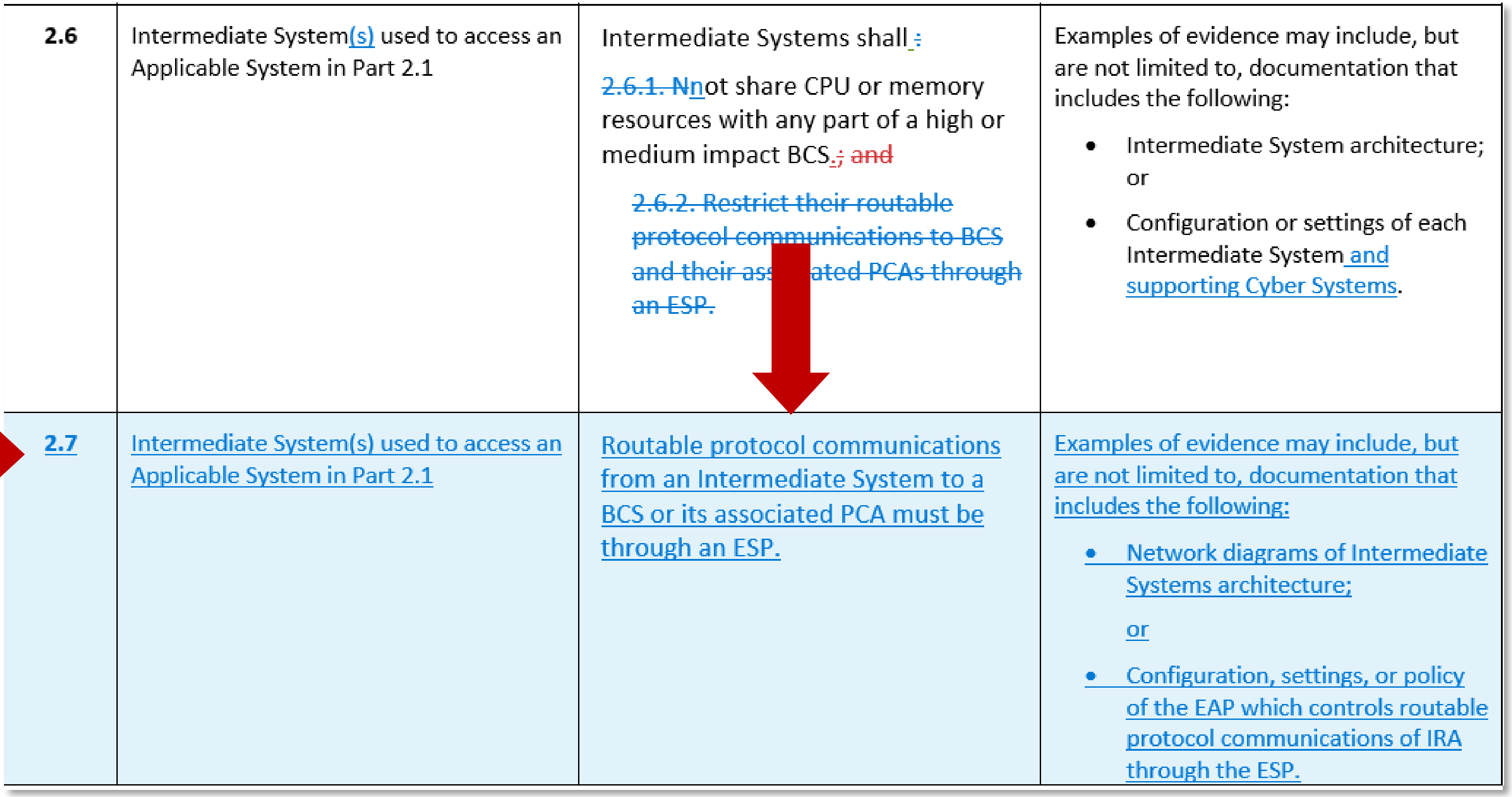
- *IS communications now possible*
- *Management Interface limited by definition*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# CIP-005 Changes – Treatment of Interm. Systems

*Join at Slido.com Slido Event Code: 201602f*

## CIP-005 R2 Part 2.6 & CIP R2 Part 2.7



| | | | |
|---|---|---|---|
| **2.6** | Intermediate System(s) used to access an Applicable System in Part 2.1 | Intermediate Systems shall ~~:~~ <br> ~~2.6.1. N~~not share CPU or memory resources with any part of a high or medium impact BCS.~~; and~~ <br> ~~2.6.2. Restrict their routable protocol communications to BCS and their associated PCAs through an ESP.~~ | Examples of evidence may include, but are not limited to, documentation that includes the following: <br> • Intermediate System architecture; or <br> • Configuration or settings of each Intermediate System and supporting Cyber Systems. |
| 2.7 | Intermediate System(s) used to access an Applicable System in Part 2.1 | Routable protocol communications from an Intermediate System to a BCS or its associated PCA must be through an ESP. | Examples of evidence may include, but are not limited to, documentation that includes the following: <br> • Network diagrams of Intermediate Systems architecture; <br> or <br> • Configuration, settings, or policy of the EAP which controls routable protocol communications of IRA through the ESP. |

*Key Changes:*

- *Split 2.6 for clarity.*
- *Clarifications for handling IS comms*

# CIP-005 Changes – Treatment of Mgmt Interfaces

## *Draft 4*

*CIP-005 R1 Part 1.3*

Permit only needed routable protocol communications to and from Management Interfaces of Applicable Systems, and deny all other routable protocol communications, per system capability.

## *Draft 5*

*CIP-005 R1 Part 1.3*

Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.

*Key Changes:*

- *Added objective for clarity*
- *Shift from “only needed routable connectivity” to “only needed network accessibility” to align with CIP-007*

# CIP-005 Changes – Treatment of Serial Converters

## *Draft 4*

*EACMS Definition – Draft 4*

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

## *Draft 5*

*EACMS Definition Draft 5*

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems or SCI. This includes Cyber Systems, not protected by an ESP, that convert routable protocol communications to non-routable communications to a BES Cyber System or SCI.

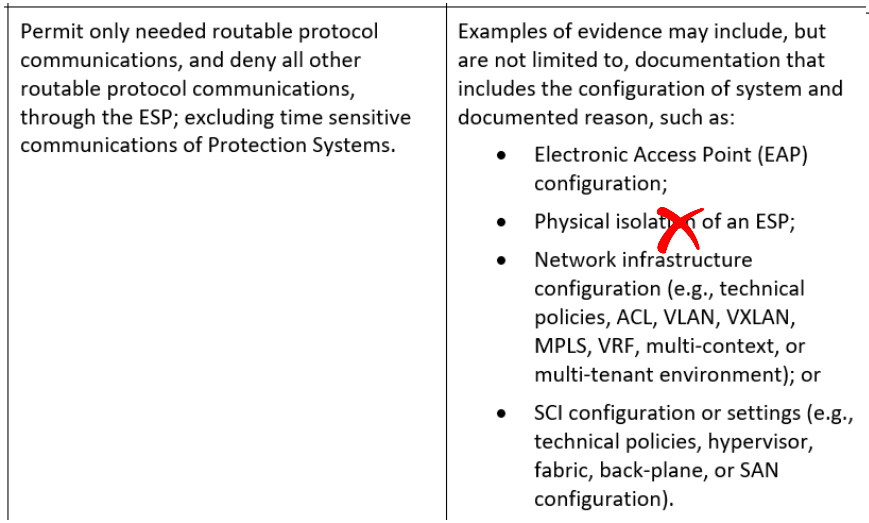
*Key Changes:*

- *Clarify treatment of Serial Converters as EACMS*

# CIP-005-8 Requirement R1.2

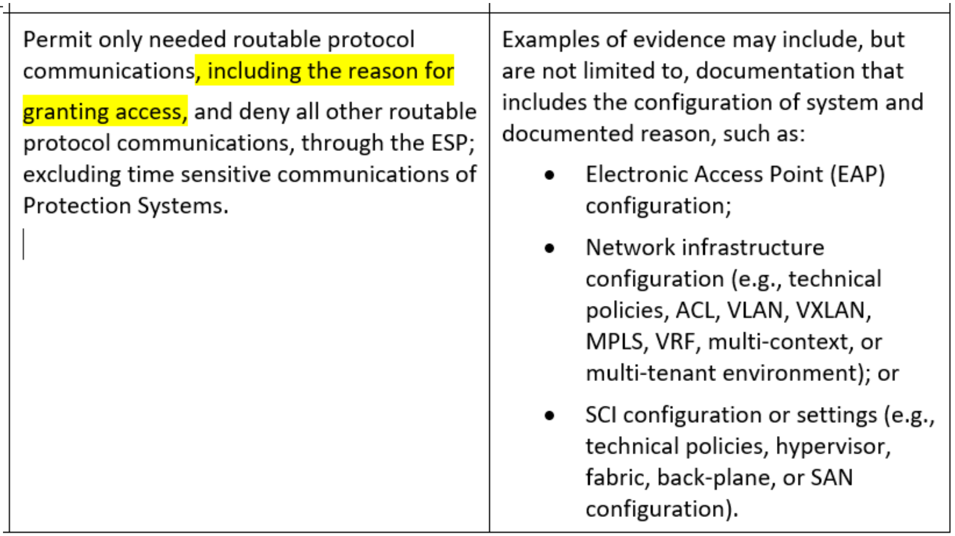
*Join at Slido.com*
*Slido Event Code: 201602f*

## *Draft 4*



| | |
|---|---|
| Permit only needed routable protocol communications, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems. | Examples of evidence may include, but are not limited to, documentation that includes the configuration of system and documented reason, such as:<br>• Electronic Access Point (EAP) configuration;<br>• Physical isolation of an ESP;<br>• Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or<br>• SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN configuration). |

## *Draft 5*

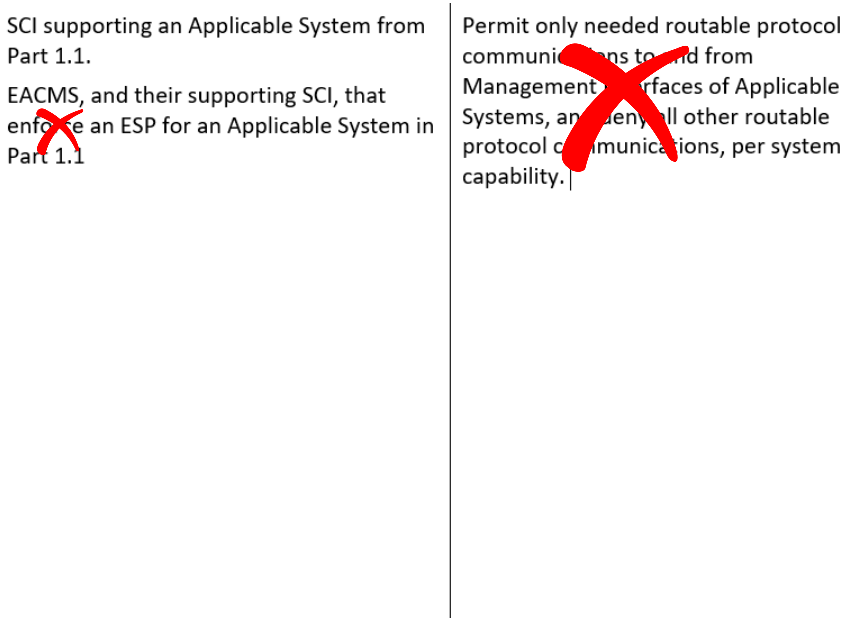


| | |
|---|---|
| Permit only needed routable protocol communications, including the reason for granting access, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems. | Examples of evidence may include, but are not limited to, documentation that includes the configuration of system and documented reason, such as:<br>• Electronic Access Point (EAP) configuration;<br>• Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or<br>• SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN configuration). |

# CIP-005-8 Requirement R1.3

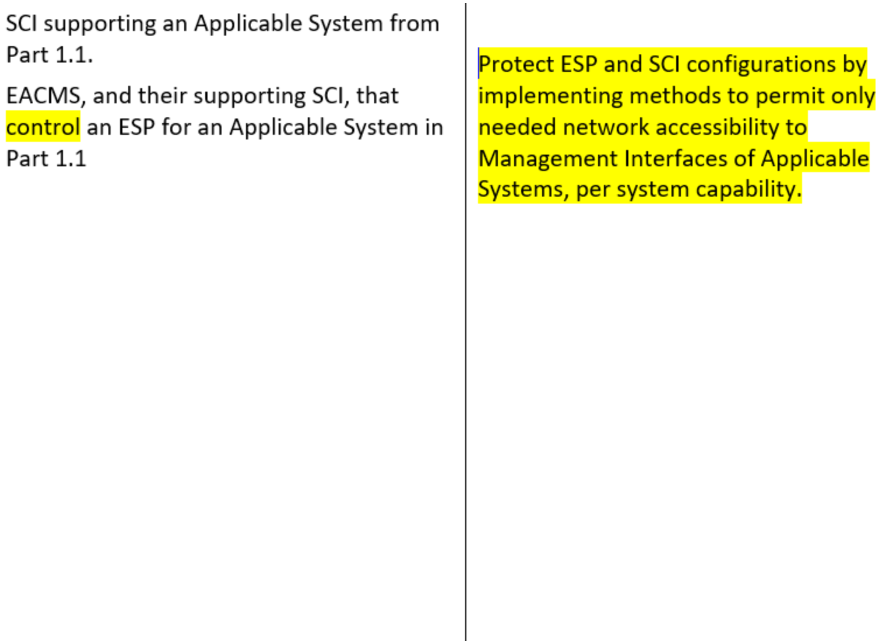
*Join at Slido.com Slido Event Code: 201602f*

## *Draft 4*



| | |
|---|---|
| SCI supporting an Applicable System from Part 1.1.<br>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 of Applicable Systems, and deny all other routable protocol communications, per system capability.~~ |

## *Draft 5*



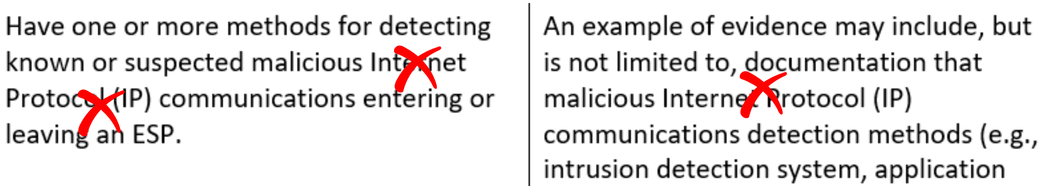
| | |
|---|---|
| SCI supporting an Applicable System from Part 1.1.<br>EACMS, and their supporting SCI, that control an ESP for an Applicable System in Part 1.1 | Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability. |

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# CIP-005-8 Requirement R1.5

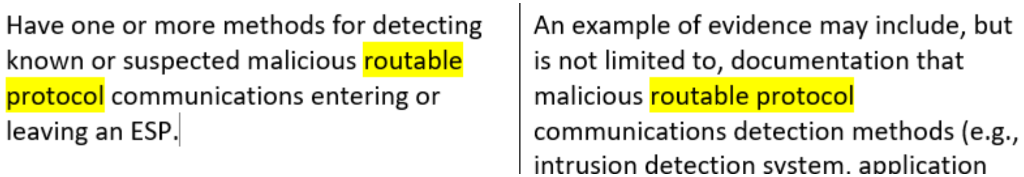
*Join at Slido.com Slido Event Code: 201602f*

## *Draft 4*



| | |
|---|---|
| Have one or more methods for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP. | An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g., intrusion detection system, application |

## *Draft 5*



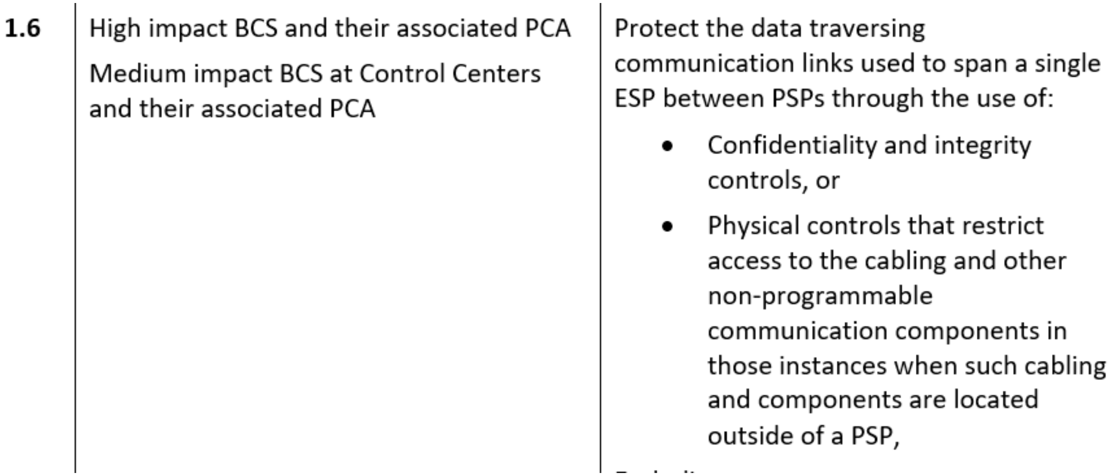
| | |
|---|---|
| Have one or more methods for detecting known or suspected malicious routable protocol communications entering or leaving an ESP. | An example of evidence may include, but is not limited to, documentation that malicious routable protocol communications detection methods (e.g., intrusion detection system, application |

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# CIP-005-8 Requirement R1.6

*Join at Slido.com Slido Event Code: 201602f*

*Draft 4*



| | | |
|---|---|---|
| **1.6** | High impact BCS and their associated PCA<br>Medium impact BCS 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:<br>• Confidentiality and integrity controls, or<br>• 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, |

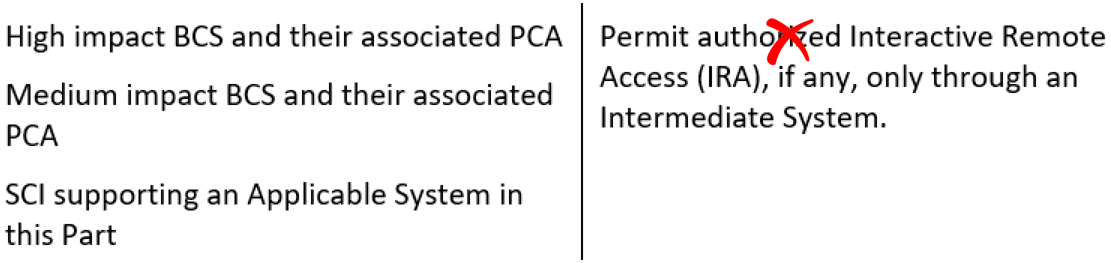
*Draft 5*

*SDT elected not to add SCI to Applicable Systems*

# CIP-005-8 Requirement R2.1

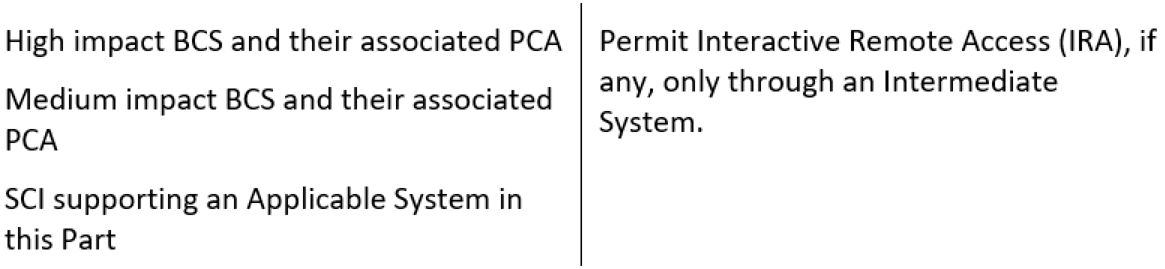
*Join at Slido.com*
*Slido Event Code: 201602f*

*Draft 4*



| | |
|---|---|
| High impact BCS and their associated PCA<br>Medium impact BCS and their associated PCA<br>SCI supporting an Applicable System in this Part | Permit ~~authorized~~ Interactive Remote Access (IRA), if any, only through an Intermediate System. |

*Draft 5*



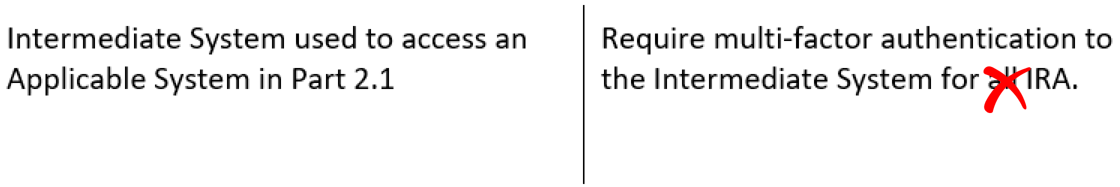
| | |
|---|---|
| High impact BCS and their associated PCA<br>Medium impact BCS and their associated PCA<br>SCI supporting an Applicable System in this Part | Permit Interactive Remote Access (IRA), if any, only through an Intermediate System. |

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# CIP-005-8 Requirement R2.3

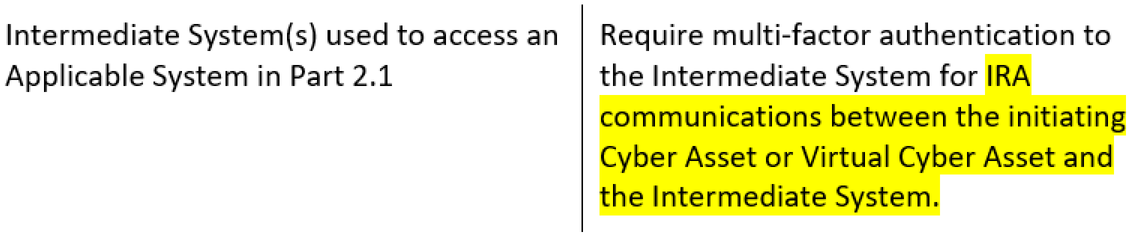
*Join at Slido.com Slido Event Code: 201602f*

## *Draft 4*



| | |
|---|---|
| Intermediate System used to access an Applicable System in Part 2.1 | Require multi-factor authentication to the Intermediate System for ~~all~~ IRA. |

## *Draft 5*



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

# CIP-005-8 Requirement R2.4 and 2.5

*Join at Slido.com Slido Event Code: 201602f*

## *Draft 4*

High impact BCS with vendor ~~remote access~~ and their associated PCA

Medium impact BCS with vendor ~~remote access~~ and their associated PCA

SCI supporting an Applicable System in this Part

## *Draft 5*

High impact BCS and their associated PCA

Medium impact BCS and their associated PCA

SCI supporting an Applicable System in this Part

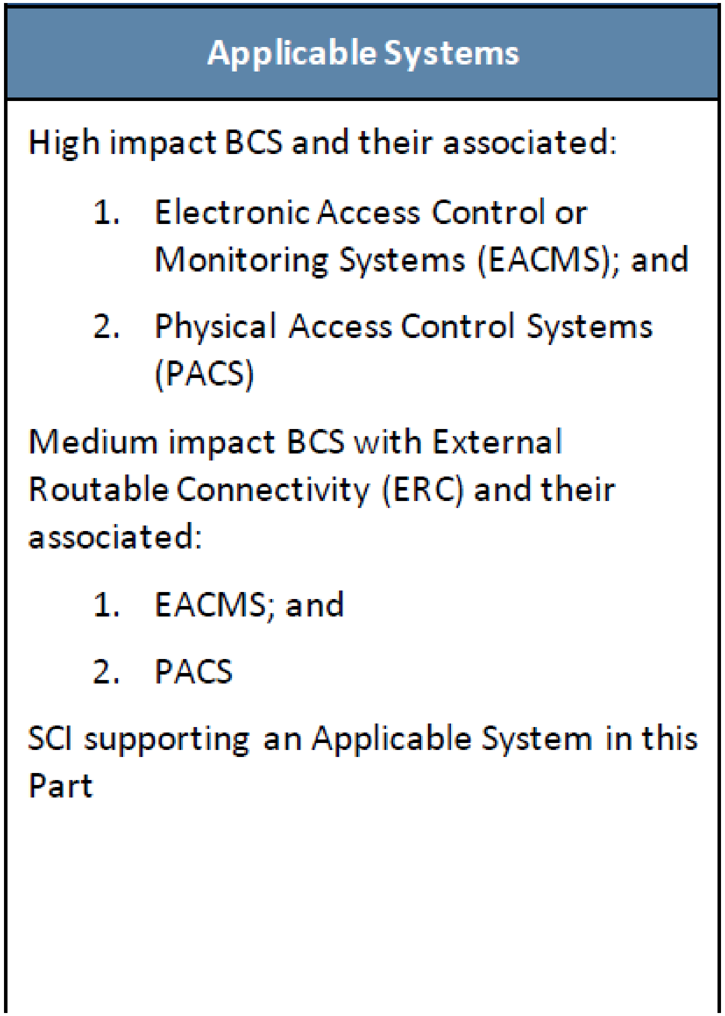
# CIP-004 Changes

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# CIP-004-8 Draft 5 Posting Requirements R2 – R6

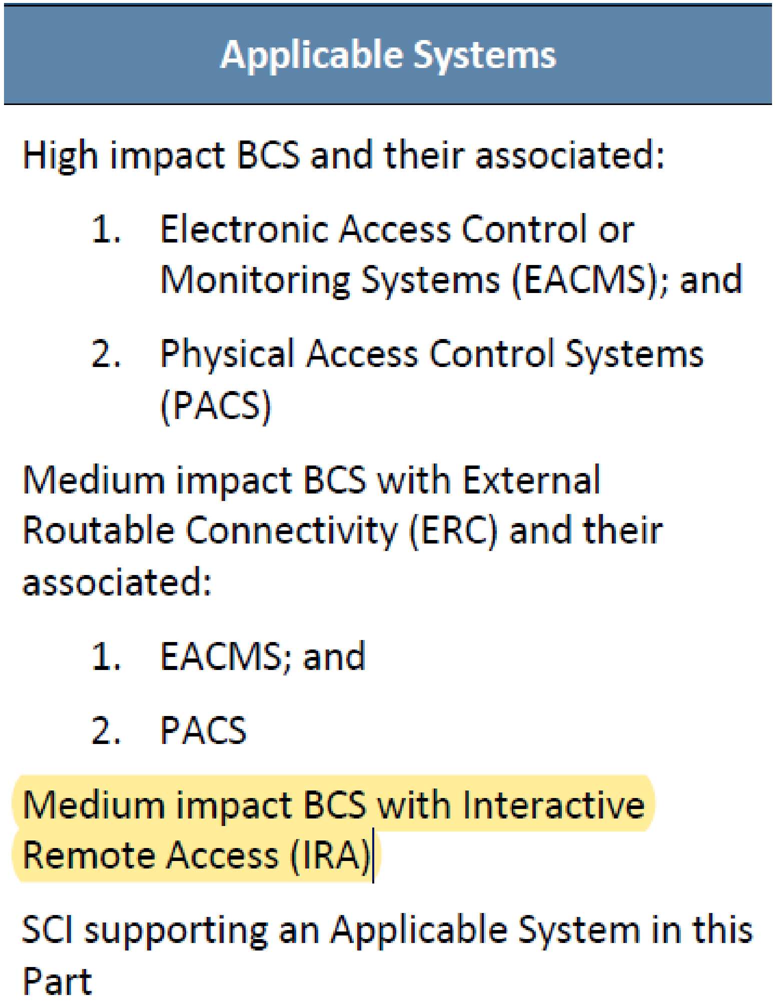
*Join at Slido.com Slido Event Code: 201602f*

## *Draft 4*



| Applicable Systems |
|---|
| High impact BCS and their associated:<br>1. Electronic Access Control or Monitoring Systems (EACMS); and<br>2. Physical Access Control Systems (PACS)<br>Medium impact BCS with External Routable Connectivity (ERC) and their associated:<br>1. EACMS; and<br>2. PACS<br>SCI supporting an Applicable System in this Part |

## *Draft 5*



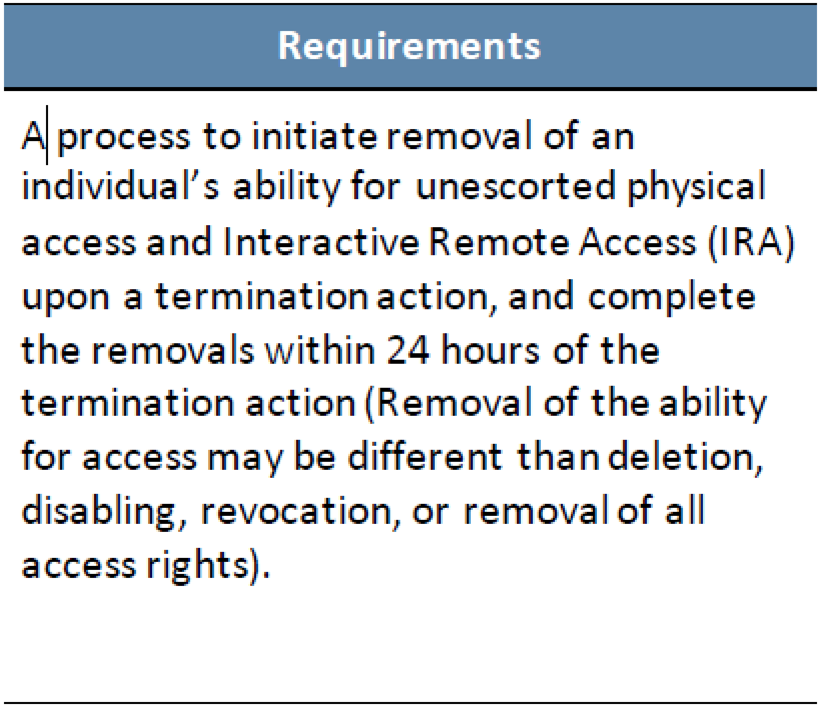
| Applicable Systems |
|---|
| High impact BCS and their associated:<br>1. Electronic Access Control or Monitoring Systems (EACMS); and<br>2. Physical Access Control Systems (PACS)<br>Medium impact BCS with External Routable Connectivity (ERC) and their associated:<br>1. EACMS; and<br>2. PACS<br>Medium impact BCS with Interactive Remote Access (IRA)<br>SCI supporting an Applicable System in this Part |

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# CIP-004-8 Draft 5 Posting

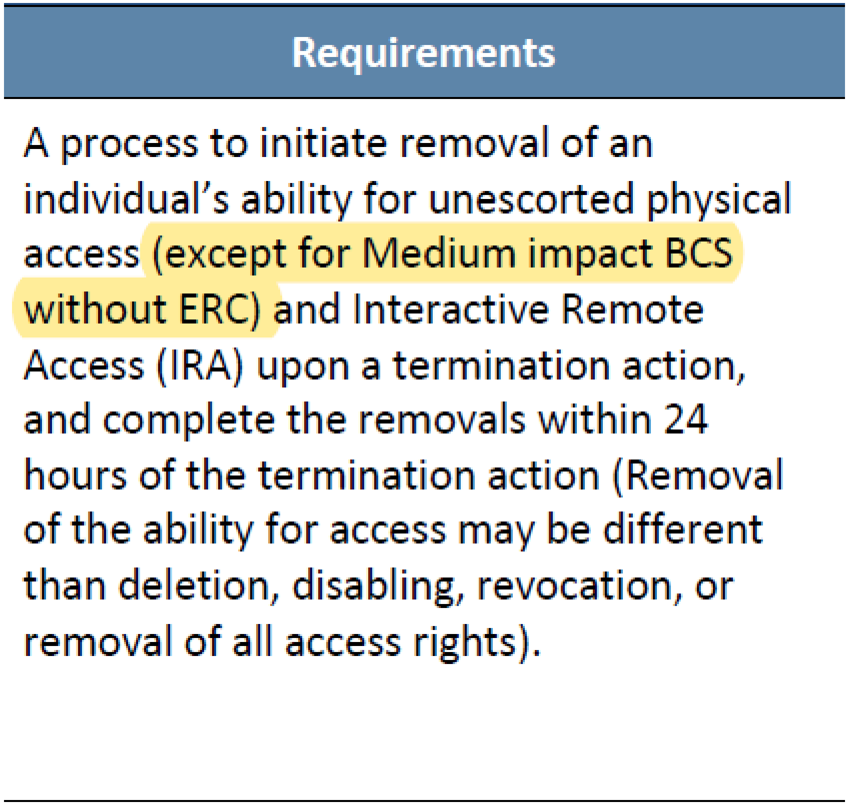
*Join at Slido.com Slido Event Code: 201602f*

## *Draft 4*



| Requirements |
|---|
| A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights). |

## *Draft 5*



| Requirements |
|---|
| A process to initiate removal of an individual's ability for unescorted physical access (except for Medium impact BCS without ERC) and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights). |

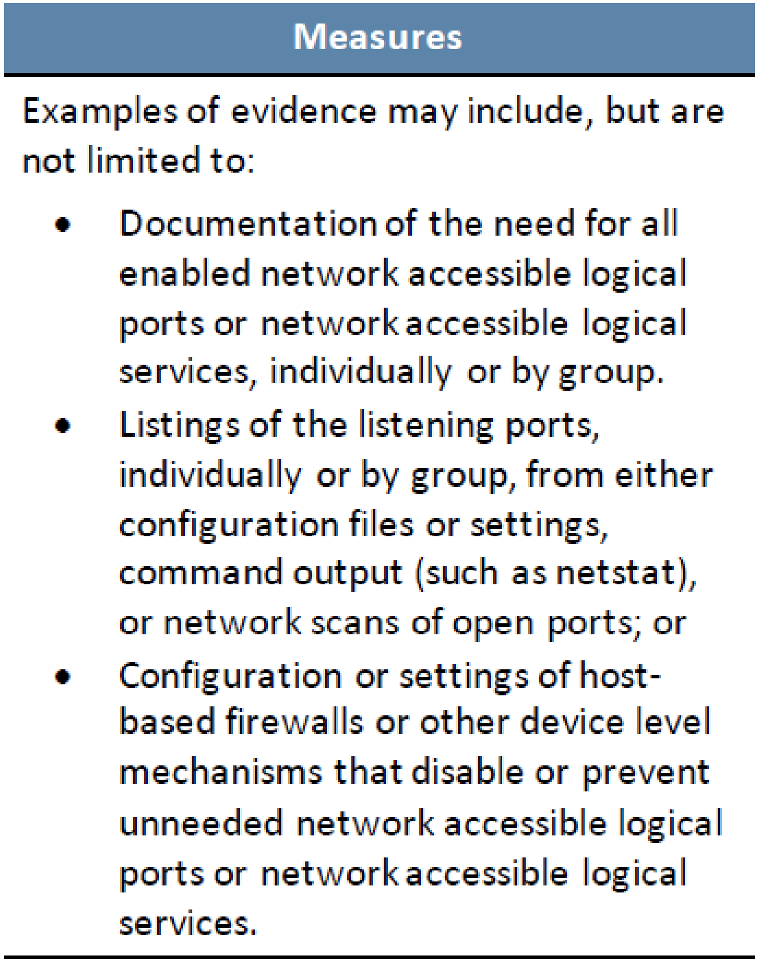
# CIP-007 Changes

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# CIP-007-7 Draft 5 Posting R1.1 Measures

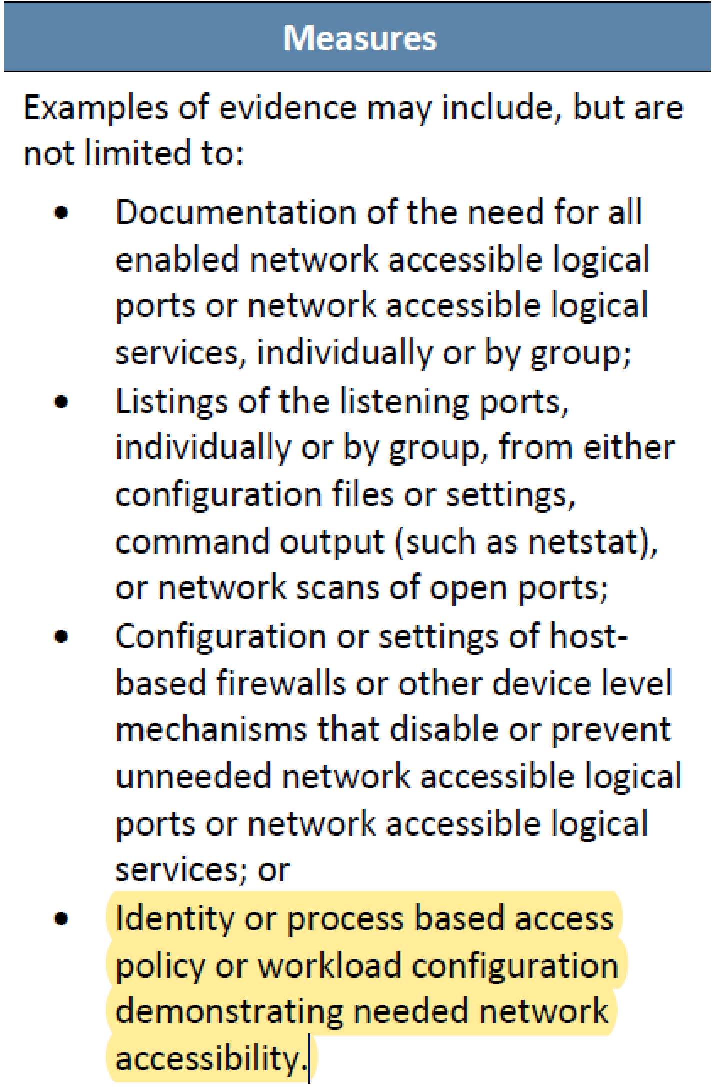
*Join at Slido.com Slido Event Code: 201602f*

## Draft 4



| Measures |
|---|
| Examples of evidence may include, but are not limited to:<br>• Documentation of the need for all enabled network accessible logical ports or network accessible logical services, individually or by group.<br>• Listings of the listening ports, individually or by group, from either configuration files or settings, command output (such as netstat), or network scans of open ports; or<br>• Configuration or settings of host-based firewalls or other device level mechanisms that disable or prevent unneeded network accessible logical ports or network accessible logical services. |

## Draft 5



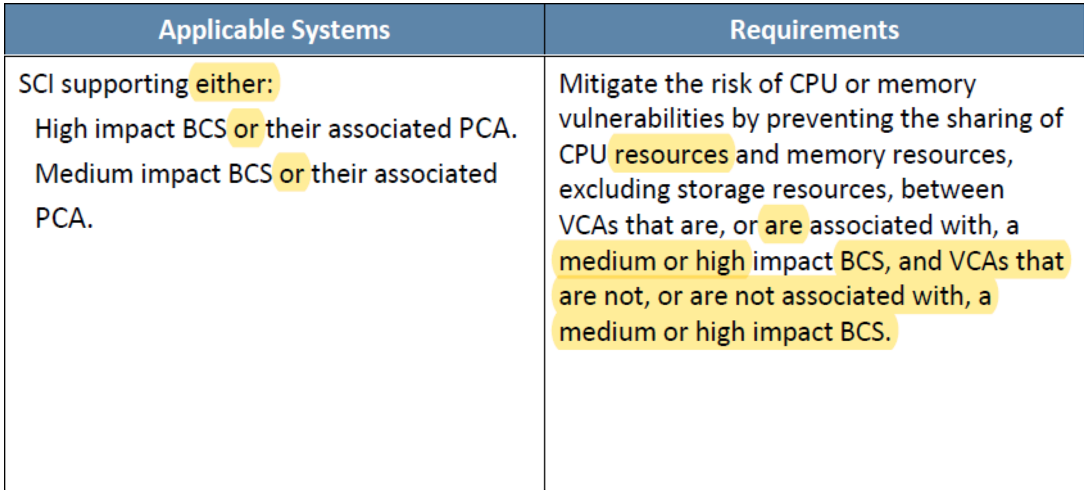
| Measures |
|---|
| Examples of evidence may include, but are not limited to:<br>• Documentation of the need for all enabled network accessible logical ports or network accessible logical services, individually or by group;<br>• Listings of the listening ports, individually or by group, from either configuration files or settings, command output (such as netstat), or network scans of open ports;<br>• Configuration or settings of host-based firewalls or other device level mechanisms that disable or prevent unneeded network accessible logical ports or network accessible logical services; or<br>• Identity or process based access policy or workload configuration demonstrating needed network accessibility. |

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# CIP-007-7 Draft 5 Posting Requirement 1.3

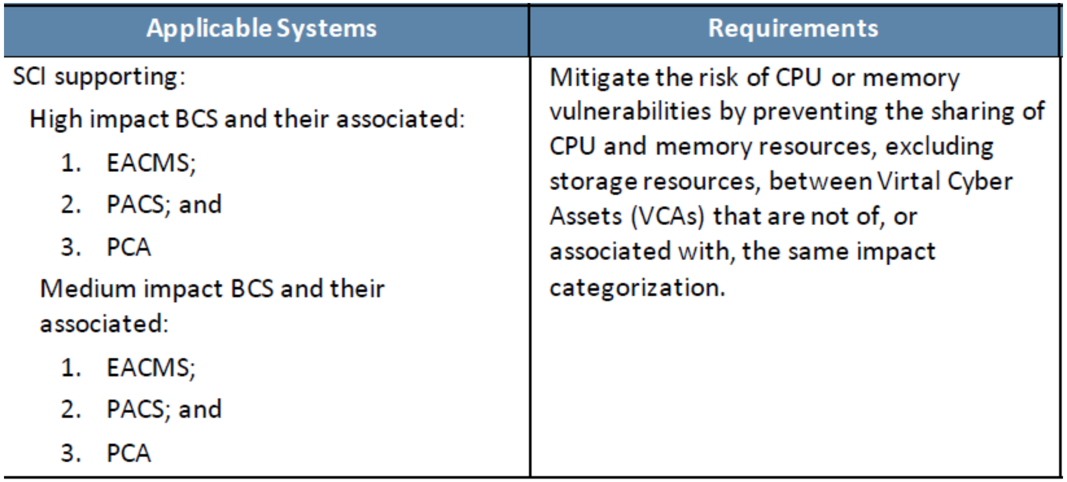
*Join at Slido.com Slido Event Code: 201602f*

*Draft 5*



| Applicable Systems | Requirements |
|---|---|
| SCI supporting either:<br>High impact BCS or their associated PCA.<br>Medium impact BCS or their associated PCA. | 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. |

*Draft 4*

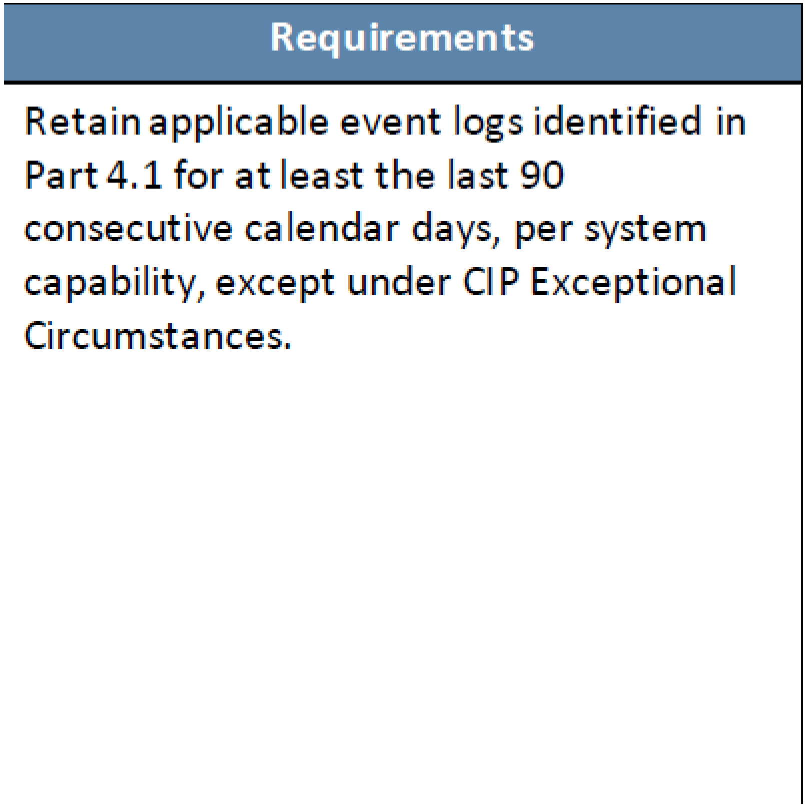


| Applicable Systems | Requirements |
|---|---|
| SCI supporting:<br>High impact BCS and their associated:<br>1. EACMS;<br>2. PACS; and<br>3. PCA<br>Medium impact BCS and their associated:<br>1. EACMS;<br>2. PACS; and<br>3. PCA | Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources, excluding storage resources, between Virtal Cyber Assets (VCAs) that are not of, or associated with, the same impact categorization. |

# CIP-007-7 Draft 5 Posting Requirement 4.3

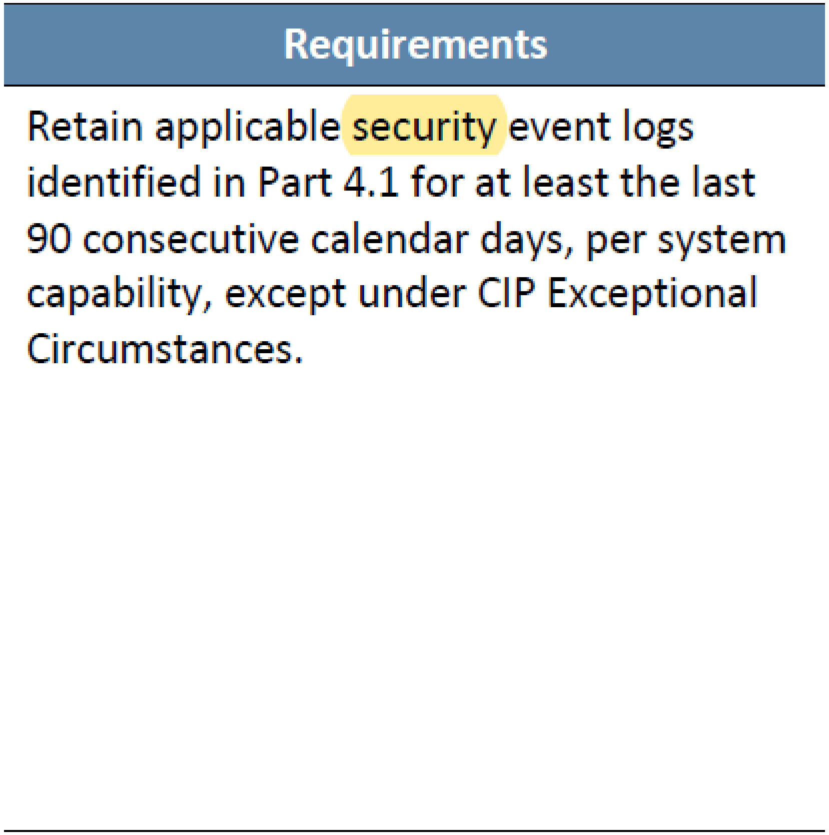
*Join at Slido.com Slido Event Code: 201602f*

## *Draft 4*



| Requirements |
|---|
| Retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances. |

## *Draft 5*



| Requirements |
|---|
| 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. |

# Topical Discussions

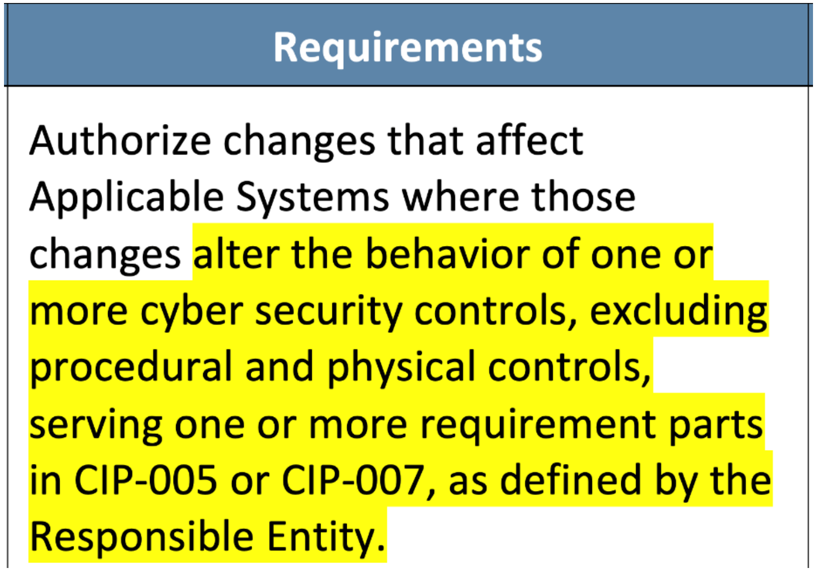
- Scope of Change Management and Monitoring, including:
  - Order of Operations (as part of the change)
  - Monitoring Scope (System Based)
- IS for Management Interfaces (Hall of one mirror)
  - Serial IRA, IRA Authorization
  - Converter capabilities
  - Converted by the Responsible Entity
- Affinity (CIP-007 R1 Part 1.3 & CIP-005 R2 Part 2.6)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Topical: Scope of Change Management

*Join at Slido.com Slido Event Code: 201602f*

## *CIP-010 R1 Part 1.1*

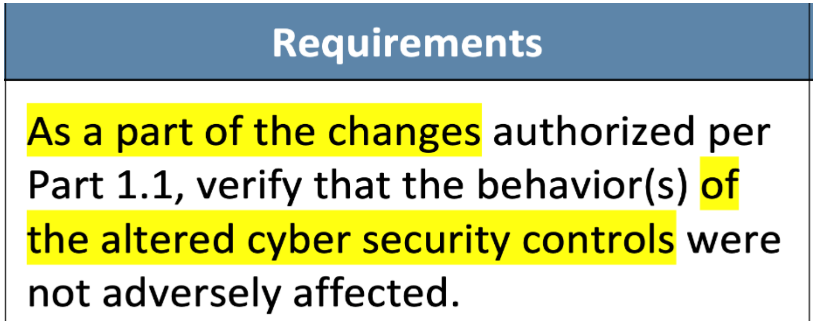


| Requirements |
|---|
| Authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity. |

***Scoping Change Management:***

1. *Alter behavior of control*
2. *Exclude physical & procedural*
   - *Not process docs*
3. *Serving one or more CIP Req Parts*
4. *Defined by Responsible Entity*

## *CIP-010 R1 Part 1.4*



| Requirements |
|---|
| 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. |

***Order of Operations:***

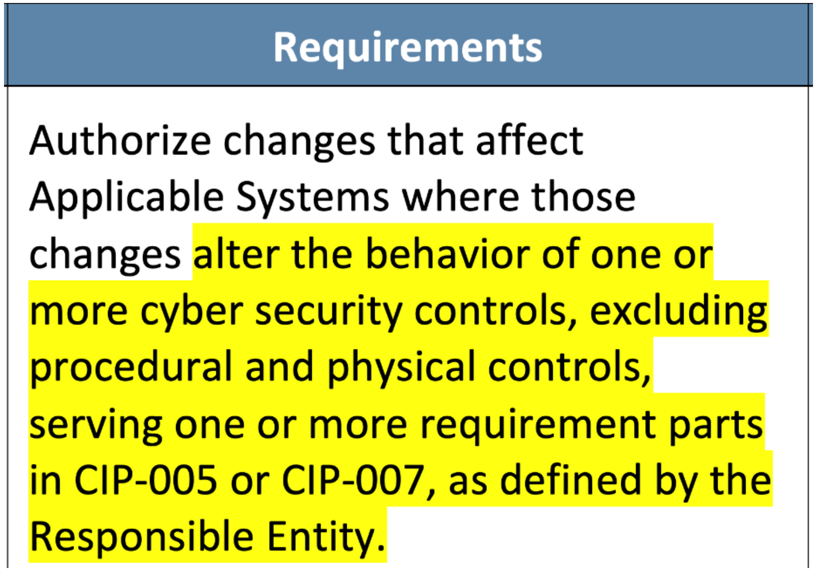
1. *As part of change…*
2. *From 1.1*
3. *Verify behavior of altered controls*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Topical: Scope of Change Management

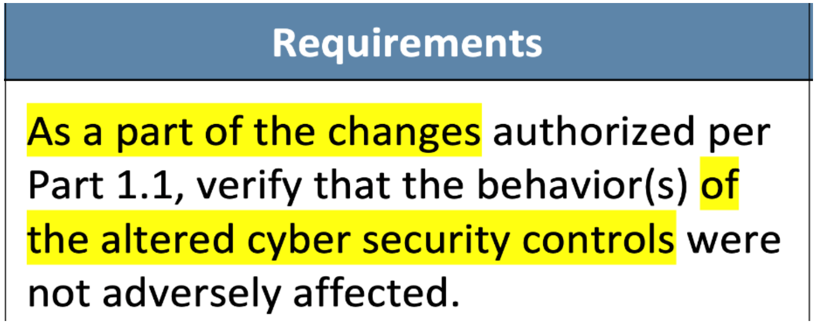
*Join at Slido.com Slido Event Code: 201602f*

## *CIP-010 R1 Part 1.1*



| Requirements |
|---|
| 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. |

## *CIP-010 R1 Part 1.4*



| Requirements |
|---|
| 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. |

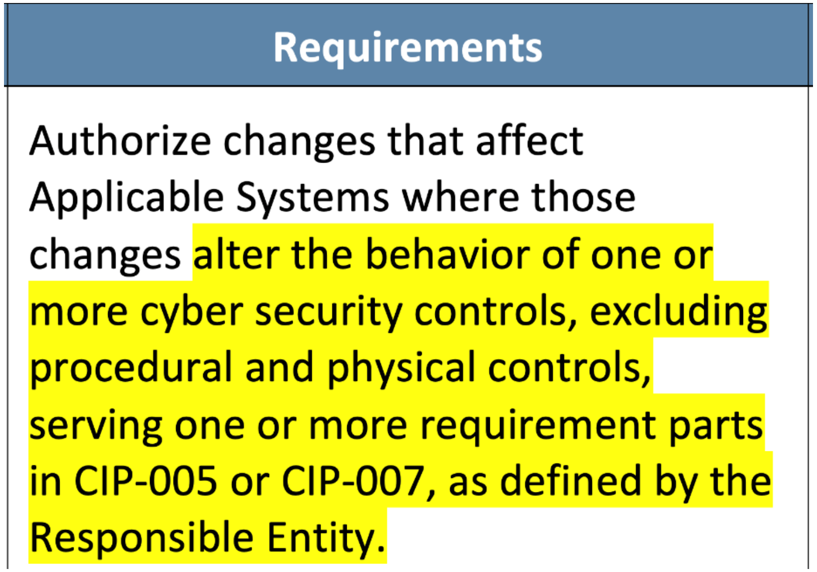
- **How does this apply to:**
  - Manual changes (one-off)
  - Automated changes & Remediation
- Examples!

# Topical: Scope of Change Management

*Join at Slido.com Slido Event Code: 201602f*

## What do you need to know to fulfil CIP-010 R1 Part 1.1?

- Where is this change applied?
- What Applicable Systems does this change affect?
- What control’s behavior does this change alter?
- What Requirement Parts does that control serve?



| Requirements |
|---|
| 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. |

# Topical: Scope of Change Management

*Join at Slido.com Slido Event Code: 201602f*

*Example 1:*

## Manual Change to modify password policy via AD

- **Where is this change applied?**
  - Active Directory servers (EACMS)
- **What Applicable Systems does this change affect?**
  - AD Servers and Applicable Systems bound to this AD Domain (likely multiple CIP Systems and types)
- **What control's behavior does this change alter?**
  - Password Policy to control allowed password behaviors (length, complexity, expiration/change interval etc.)
- **What Requirement Parts does that control serve?**
  - The responsible entity defines this as serving CIP-007 R5 Parts 5.5 & 5.6

## *Example 1 Continued:*

# Manual Change to modify password policy via AD (cont'd)

- **What does that cause us to do?**
  - Authorize a change, per CIP-010-5 R1 Part 1.1 to the AD Servers **and** bound Applicable Systems
  - Then in CIP-010-5 R1 Part 1.4 we verify that the applied password policy
    - Still serves CIP-007 R5 Parts 5.5 & 5.6 "As part of the change"
- **What this does not cause:**
  - Initiation of change process to authorize a change for each user's changed password
    - Because the defined control is the Password Policy **not** individual passwords
- **How often does this authorization need to occur?**
  - Once, (or each time) when change is to be made to the Password Policy

*Example 2:*

# Change to enable automated monthly cyber security patching

- **Where is this change applied?**
  - Patch management server (may not be a CIP Asset)
- **What Applicable Systems does this change affect?**
  - Patch management server (if CIP) and Applicable Systems managed by this server (likely multiple CIP Systems and types)
- **What control's behavior does this change alter?**
  - Control for the timing of cyber security patch installation on managed systems
- **What Requirement Parts does that control serve?**
  - The responsible entity defines this as serving CIP-007 R2 Parts 2.2 & 2.3

## *Example 2 Continued:*

# Change to enable automated monthly cyber security patching

- **What does that cause us to do?**
  - Authorize a change, per CIP-010-5 R1 Part 1.1, to the centralized patching server (if CIP) and Applicable Systems managed by this console
  - Then in CIP-010-5 R1 Part 1.4 we verify that the timing of patching
    - Still serves CIP-007 R2 Part 2.2 & 2.3 (35 calendar days) "As part of the change"
- **What this does not cause:**
  - Initiation of change process to authorize a change each month for cyber security patch installation
    - Because the defined control is the timing for patching, not each resulting patch event
- **How often does this authorization need to occur?**
  - Once, when change is made to the timing configuration of the patch server

## *Example 3:*
## Change to enable automated Remediation VLAN

- **Where is this change applied?**
  - Management Console and supporting systems (Patching, AV, etc.) (may not be a CIP Assets)
- **What Applicable Systems does this change affect?**
  - Management Console and supporting systems (if CIP) and Applicable Systems managed by this console - (likely multiple CIP Systems and types)
- **What control's behavior does this change alter?**
  - Configuration of audit and remediation actions on the console, supporting systems, and the resulting control configurations on managed systems (including managed Applicable Systems)
- **What Requirement Parts does that control serve?**
  - The responsible entity defines this as serving CIP-007 R1, R2, R3, R4, & R5

## *Example 3 Continued:*
## Change to enable automated Remediation VLAN

- **What does that cause us to do?**
  - Authorize a change, per CIP-010-5 R1 Part 1.1, to the Management Console (if CIP) and Applicable Systems managed by this console
  - Then in CIP-010 R1 Part 1.4 we verify that the audit policy and remediation actions, and resulting configurations
    - Still serves CIP-007 R1, R2, R3, R4, & R5 “As part of the change”
- **What this does not cause:**
  - Initiation of change process to authorize a change for each future remediation action
    - Because the defined control is the audit and remediation action policies, and the resulting control configurations implemented at the time change is made
- **How often does this authorization need to occur?**
  - Once, when change is to be made to enable automated Remediation VLAN

# Topical: Scope of Change Management

Join at Slido.com Slido Event Code: 201602f

## *Example 3 Continued:*

## Change to enable automated Remediation VLAN

- **What happens if another CIP VM spins up outside the change window?**
  - No Change Management action required, if that system is included in the Applicable Systems of the original authorized change.
  - If this VM spins up because of a different configuration change, then that change must be authorized per 1.1, and controls validated per 1.4
- **Security patches & AV signatures are updated each month?**
  - **Manually**: Authorize and validate another change each month like initial change, because the behaviors of identified controls serving requirement part of CIP-007 R2 & R3 are being altered to implement new items
  - **Automatically**: Nothing for CIP-010 R1 Part 1.1, if the control for automating deployment was updated as part of the original change like Example 2.

## *Example 3 Continued:*

# Change to enable automated Remediation VLAN

- **What about CIP-010 R3 Part 3.3?**
  - This Remediation VLAN may serve as the Active vulnerability assessment
    - Logs of audit results and remediation actions taken can serve as evidence
  - Any new VM Implemented with same settings at any point in future will not need additional Part 3.3 evidence.
    - Because it will be a like replacement or addition with a previously assessed configuration

# CIP-010-2 R2 Part 2.1 Change Monitoring:

- **Applicable Systems scoped to:** High impact BES Cyber Systems and their associated EACMS and PCA, and SCI supporting an Applicable System in Part 2.1
- **Part Scoped to local Cyber Asset/System configuration elements**
    - **Monitoring to detect unauthorized changes that alter behaviors serving CIP-007 requirement parts** (but not CIP-005)
- **Additionally scoped to specific controls associated with CIP-007** (2.1.1 – 2.1.7)

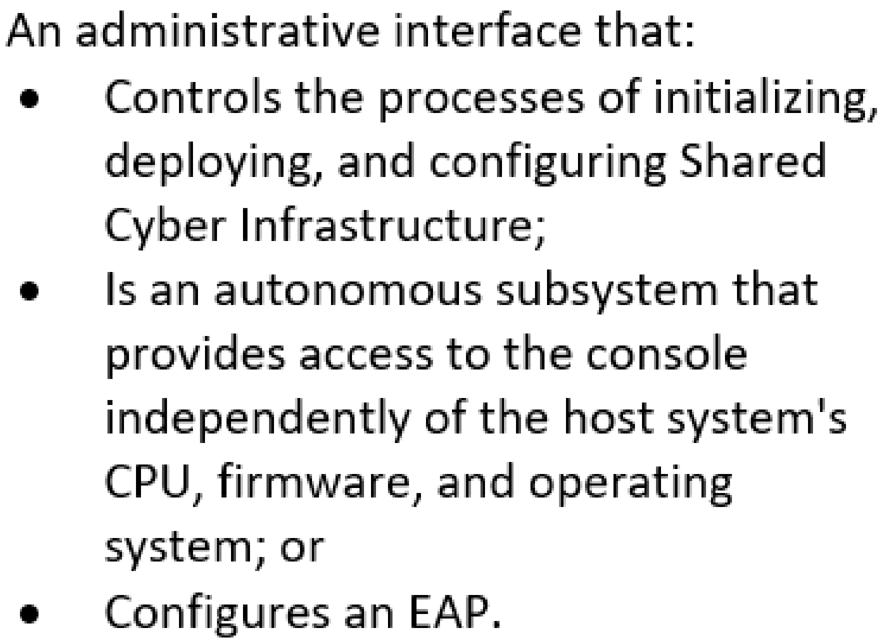
*Configurations of:*
*2.1.1 – Network ports (R1)*
*2.1.2 – VM Affinity (R1)*
*2.1.3 – Installed software (R2)*
*2.1.4 – Malicious Code (R3)*
*2.1.5 – Event Logging (R4)*
*2.1.6 – Authentication (R5)*
*2.1.7 – Account Status (R5)*

# Topical Discussions

- Management Interfaces – Access Control
- Intermediate Systems for Management Interfaces

# Management Interface

*Join at Slido.com Slido Event Code: 201602f*

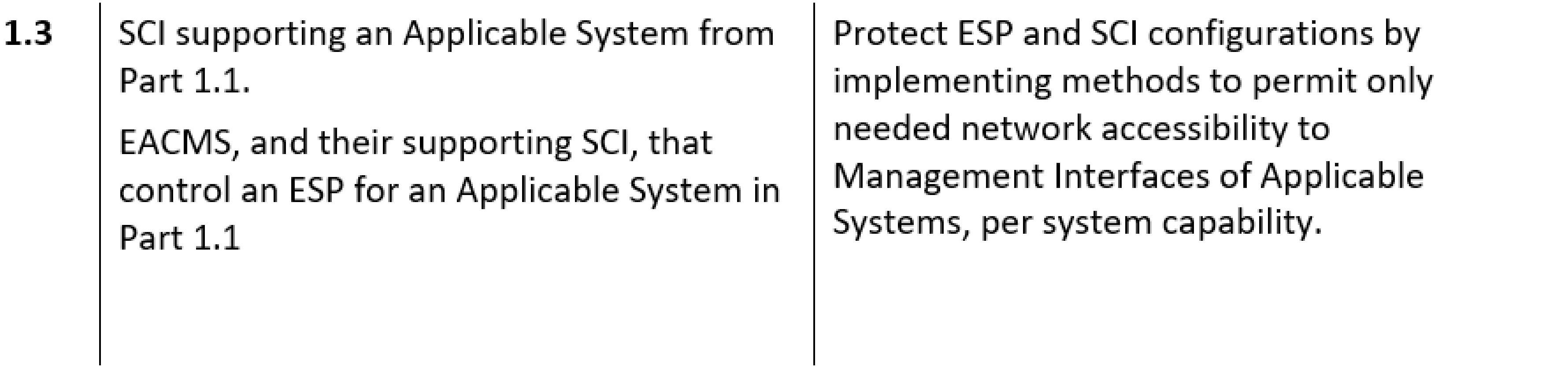


An administrative interface that:

- 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 EAP.

No change to definition from Draft 4. This definition covers user interfaces that manage SCI and ESPs including data center Lights Out server management interfaces

# Management Interface



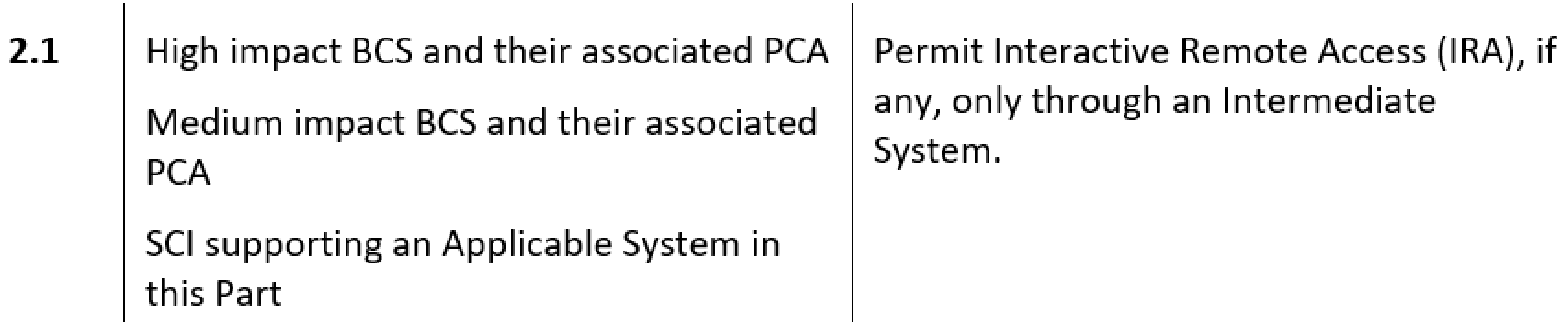
| | | |
|---|---|---|
| **1.3** | SCI supporting an Applicable System from Part 1.1.<br>EACMS, and their supporting SCI, that control an ESP for an Applicable System in Part 1.1 | Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability. |

## CIP-005-8 Requirement Part R1.3

- 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

# Management Interface

Join at Slido.com Slido Event Code: 201602f



| | | |
|---|---|---|
| **2.1** | High impact BCS and their associated PCA<br>Medium impact BCS and their associated PCA<br>SCI supporting an Applicable System in this Part | Permit Interactive Remote Access (IRA), if any, only through an Intermediate System. |

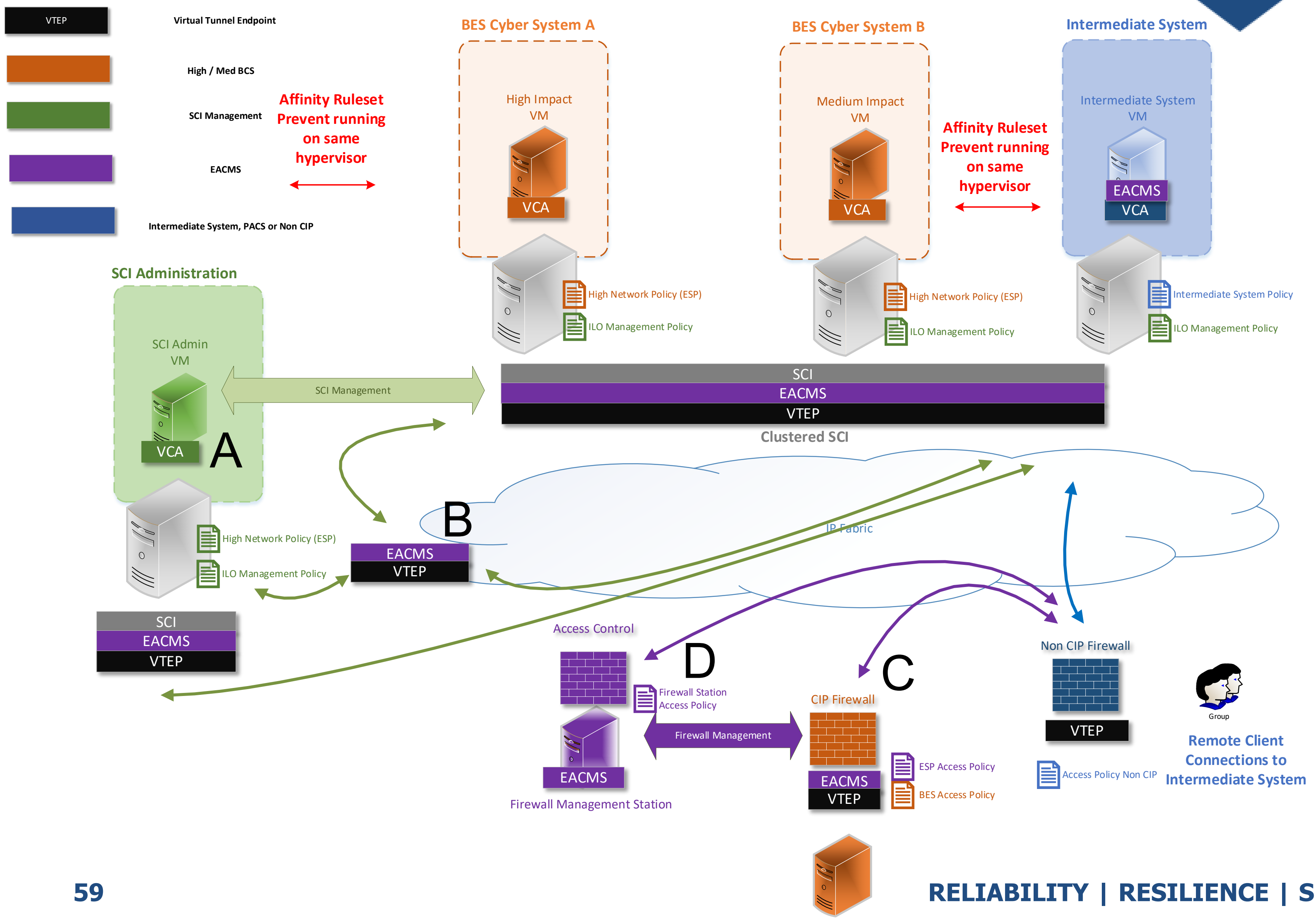
CIP-005-8 Requirement Part R2.1

- SCI Supporting an Applicable System in this part 1.1

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

# Management Interface

*Join at Slido.com Slido Event Code: 201602f*



| | |
|---|---|
| VTEP | Virtual Tunnel Endpoint |
| 🟧 | High / Med BCS |
| 🟩 | SCI Management |
| 🟪 | EACMS |
| 🟦 | Intermediate System, PACS or Non CIP |

Affinity Ruleset Prevent running on same hypervisor

BES Cyber System A
High Impact VM
VCA
High Network Policy (ESP)
ILO Management Policy

BES Cyber System B
Medium Impact VM
VCA
High Network Policy (ESP)
ILO Management Policy

Affinity Ruleset Prevent running on same hypervisor

Intermediate System
Intermediate System VM
EACMS
VCA
Intermediate System Policy
ILO Management Policy

SCI Administration
SCI Admin VM
VCA
A
High Network Policy (ESP)
ILO Management Policy
SCI
EACMS
VTEP

SCI Management

SCI
EACMS
VTEP
Clustered SCI

B
EACMS
VTEP

IP Fabric

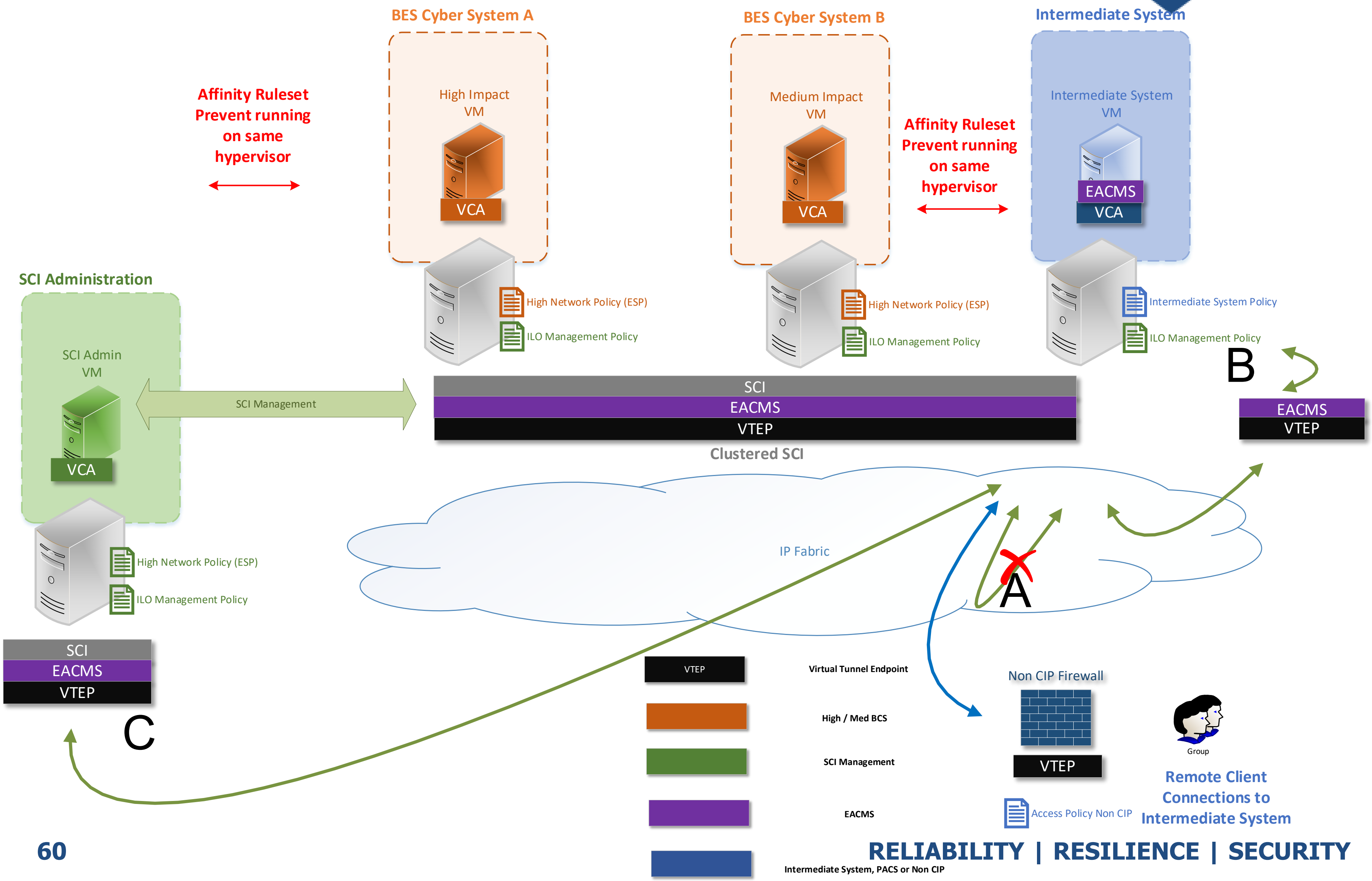
Access Control
D
Firewall Station Access Policy
Firewall Management
EACMS
Firewall Management Station

C
CIP Firewall
EACMS
VTEP
ESP Access Policy
BES Access Policy

Non CIP Firewall
VTEP
Access Policy Non CIP

Group
Remote Client Connections to Intermediate System

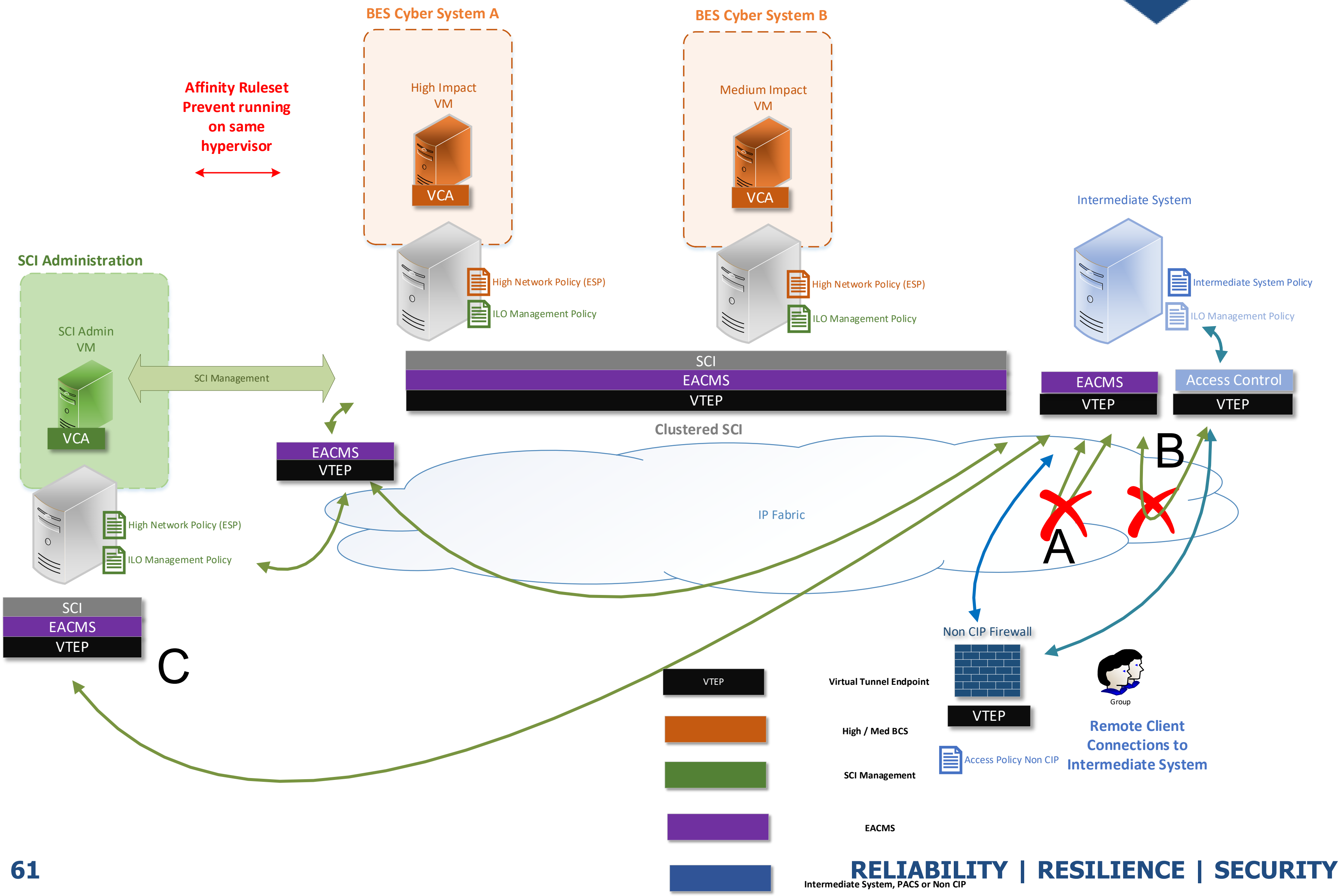
# Management Interface



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

# Management Interface

*Join at Slido.com Slido Event Code: 201602f*

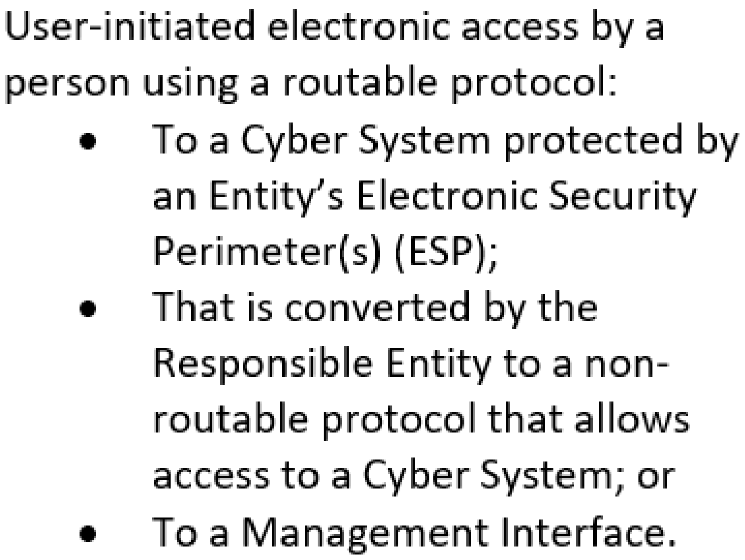


# Topical Discussions

- Serial IRA, IRA Authorization
  - Converter capabilities
  - Converted by the Responsible Entity

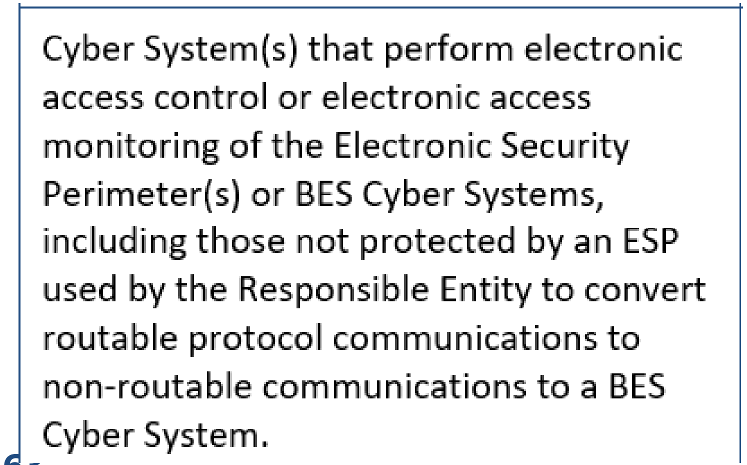
# IP to Serial Conversion - IRA

*Join at Slido.com Slido Event Code: 201602f*



User-initiated electronic access by a person using a routable protocol:

- To a Cyber System protected by an Entity's Electronic Security Perimeter(s) (ESP);
- That is converted by the Responsible Entity to a non-routable protocol that allows access to a Cyber System; or
- To a Management Interface.



Cyber System(s) that perform electronic access control or electronic access 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 communications to a BES Cyber System.

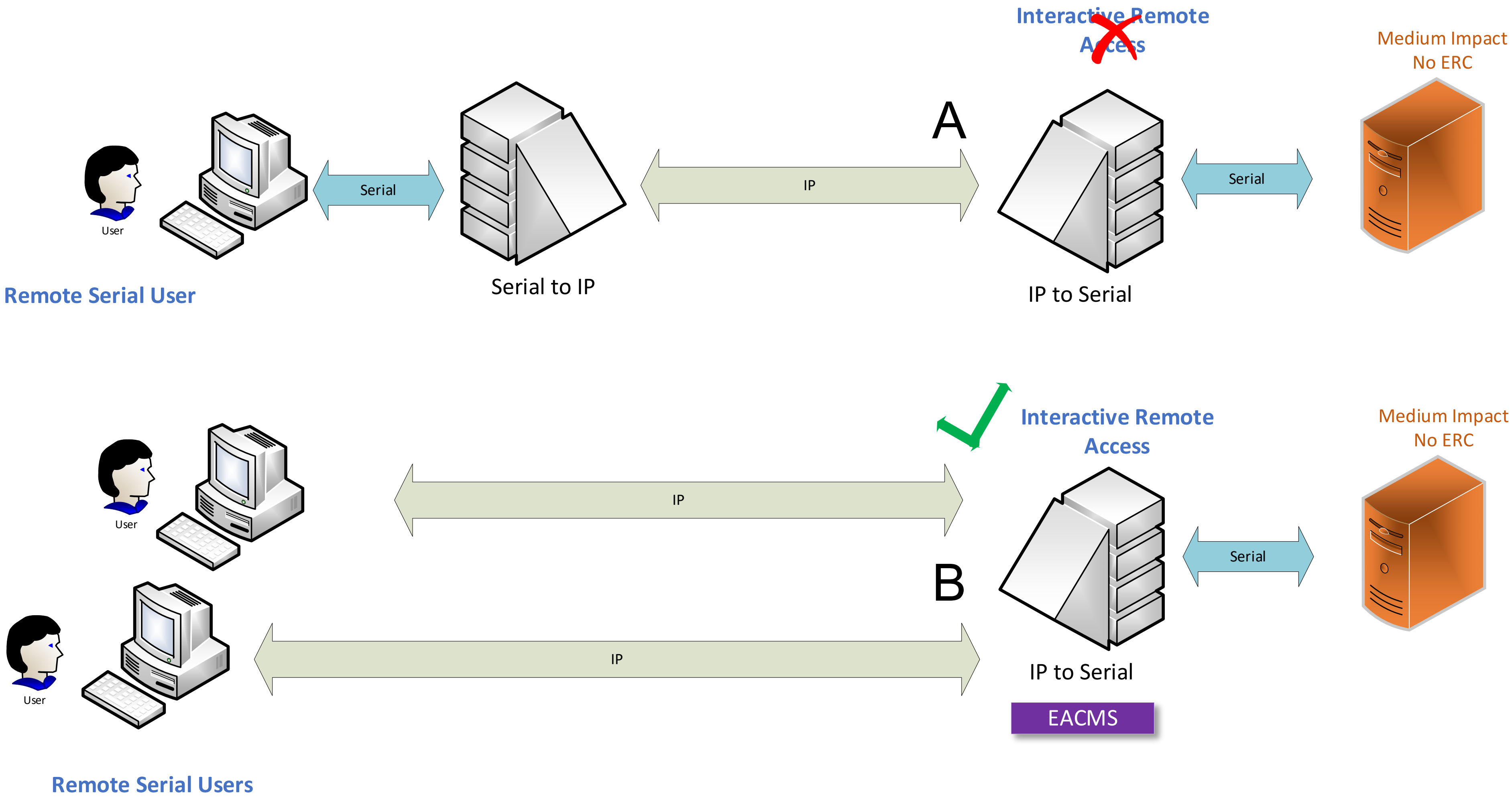
## IRA Definition (partial)

- User initiated using routable protocol
- Converted by the responsible entity to a non-routable protocol that allows access to a Cyber System
- To a Management Interface

## EACMS Definition

- User initiated using routable protocol
- Including those not protected by an ESP used by the responsible entity to convert routable protocol communications to BCS

# IP to Serial Conversion - IRA



Interactive Remote Access ✗

Medium Impact
No ERC

A

User

Serial

IP

Serial

Remote Serial User

Serial to IP

IP to Serial

✓ Interactive Remote Access

Medium Impact
No ERC

User

IP

B

Serial

User

IP

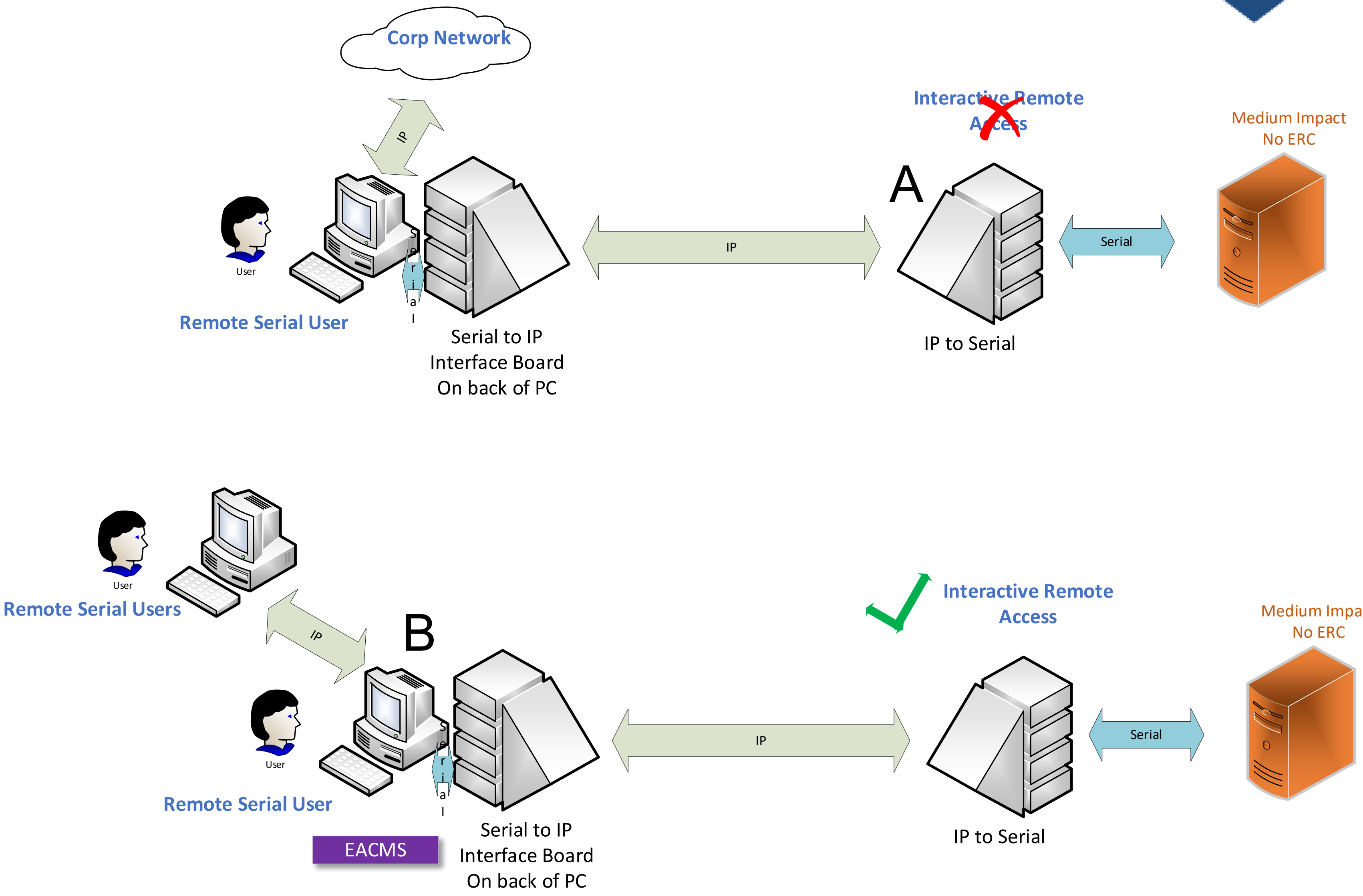
IP to Serial

EACMS

Remote Serial Users

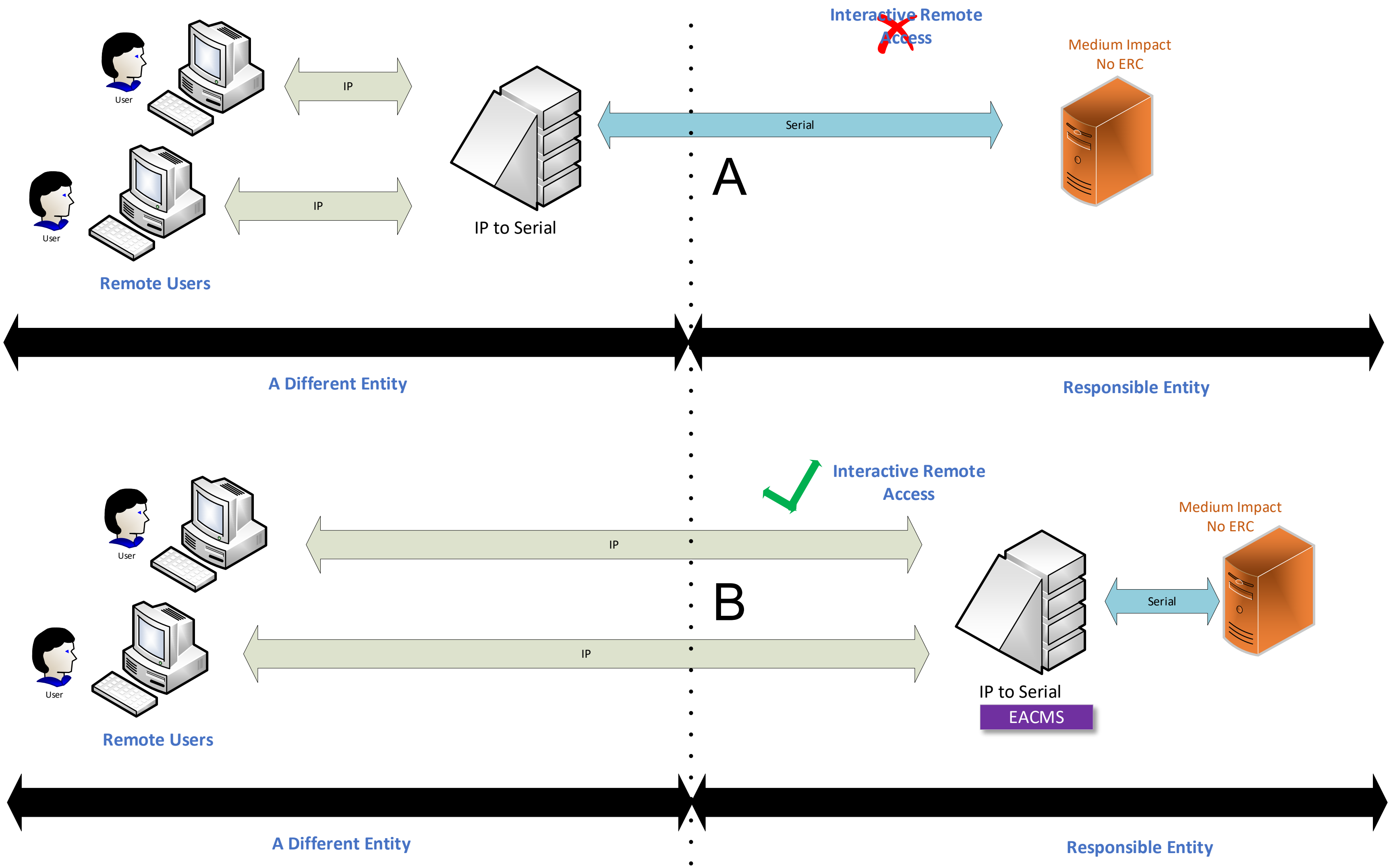
# IP to Serial Conversion - IRA

*Join at Slido.com Slido Event Code: 201602f*

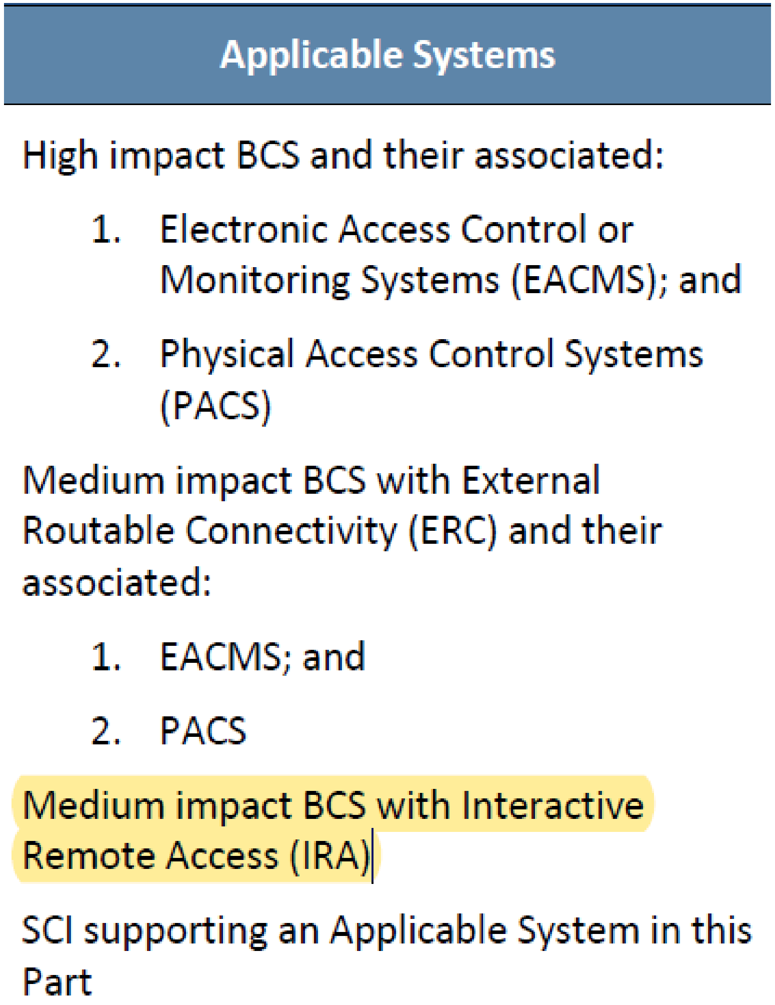


# IP to Serial Conversion - IRA

*Join at*
*Slido.com*
*Slido Event*
*Code: 201602f*



# IP to Serial Conversion - IRA



| Applicable Systems |
|---|
| High impact BCS and their associated:<br>1. Electronic Access Control or Monitoring Systems (EACMS); and<br>2. Physical Access Control Systems (PACS)<br>Medium impact BCS with External Routable Connectivity (ERC) and their associated:<br>1. EACMS; and<br>2. PACS<br>Medium impact BCS with Interactive Remote Access (IRA)<br>SCI supporting an Applicable System in this Part |

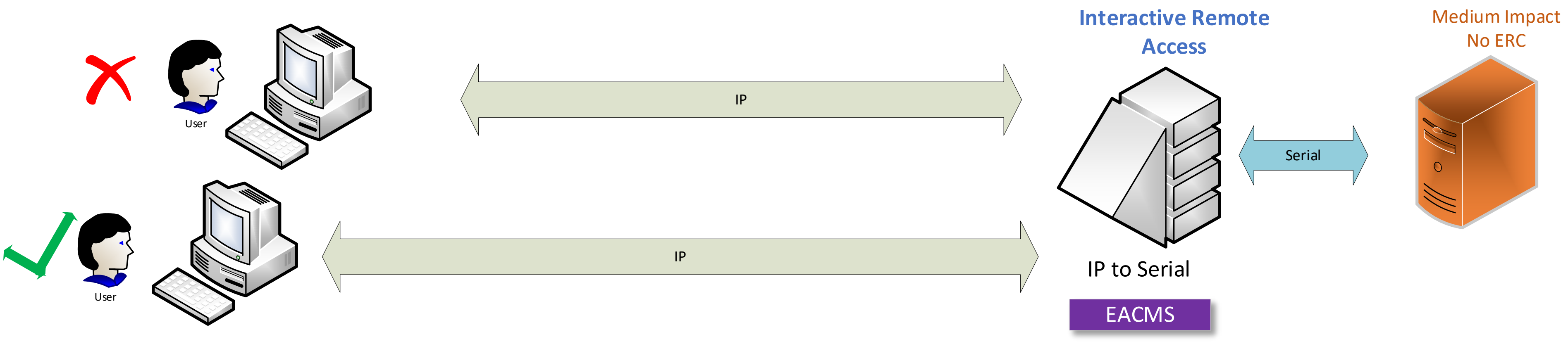
## CIP-004-8 Requirements R2-R6

Medium Impact with IRA

- covers either with ERC or without ERC

# IP to Serial Conversion - IRA

*Join at Slido.com Slido Event Code: 201602f*



Remote Serial Users

| Requirements |
|---|
| A process to initiate removal of an individual's ability for unescorted physical access (except for Medium impact BCS without ERC) and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights). |

## CIP-004-8 Requirement Part R5.1

Applicable Systems : Medium Impact with IRA

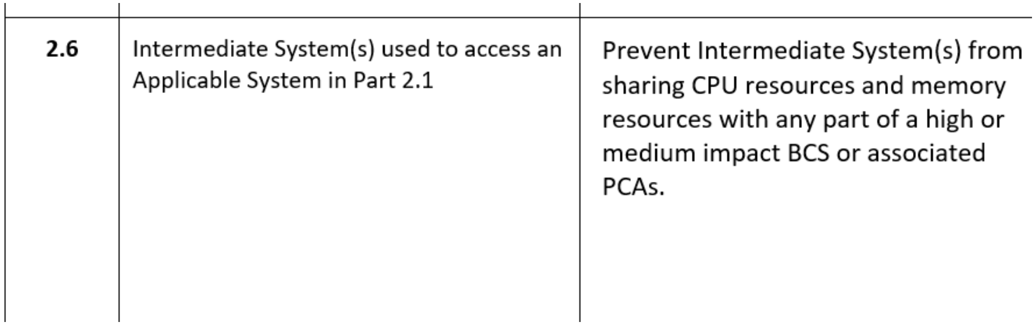
# Topical Discussions

- Affinity (CIP-007 R1 Part 1.3 & CIP-005 R2 Part 2.6)

# Intermediate Systems - Affinity

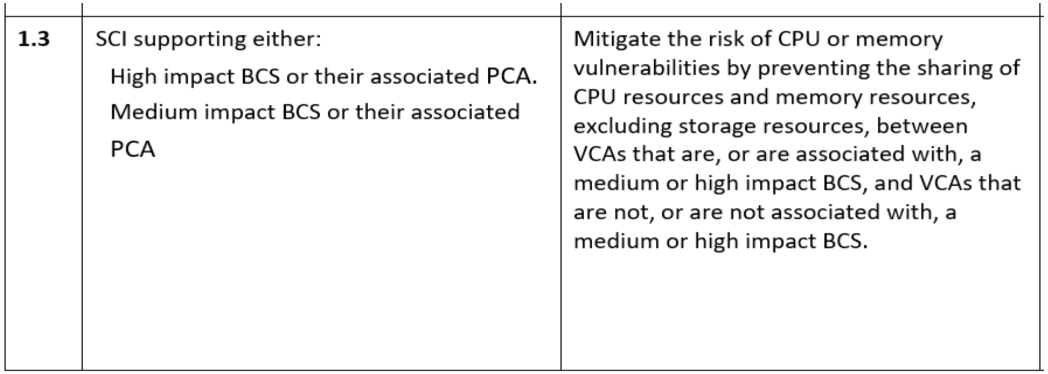
*Join at Slido.com Slido Event Code: 201602f*

## CIP-005-8 Requirement Part R2.6



| | | |
|---|---|---|
| 2.6 | Intermediate System(s) used to access an Applicable System in Part 2.1 | Prevent Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs. |

## CIP-007-7 Requirement Part R1.3



| | | |
|---|---|---|
| 1.3 | SCI supporting either:<br>High impact BCS or their associated PCA.<br>Medium impact BCS or their associated PCA | 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. |

## Affinity

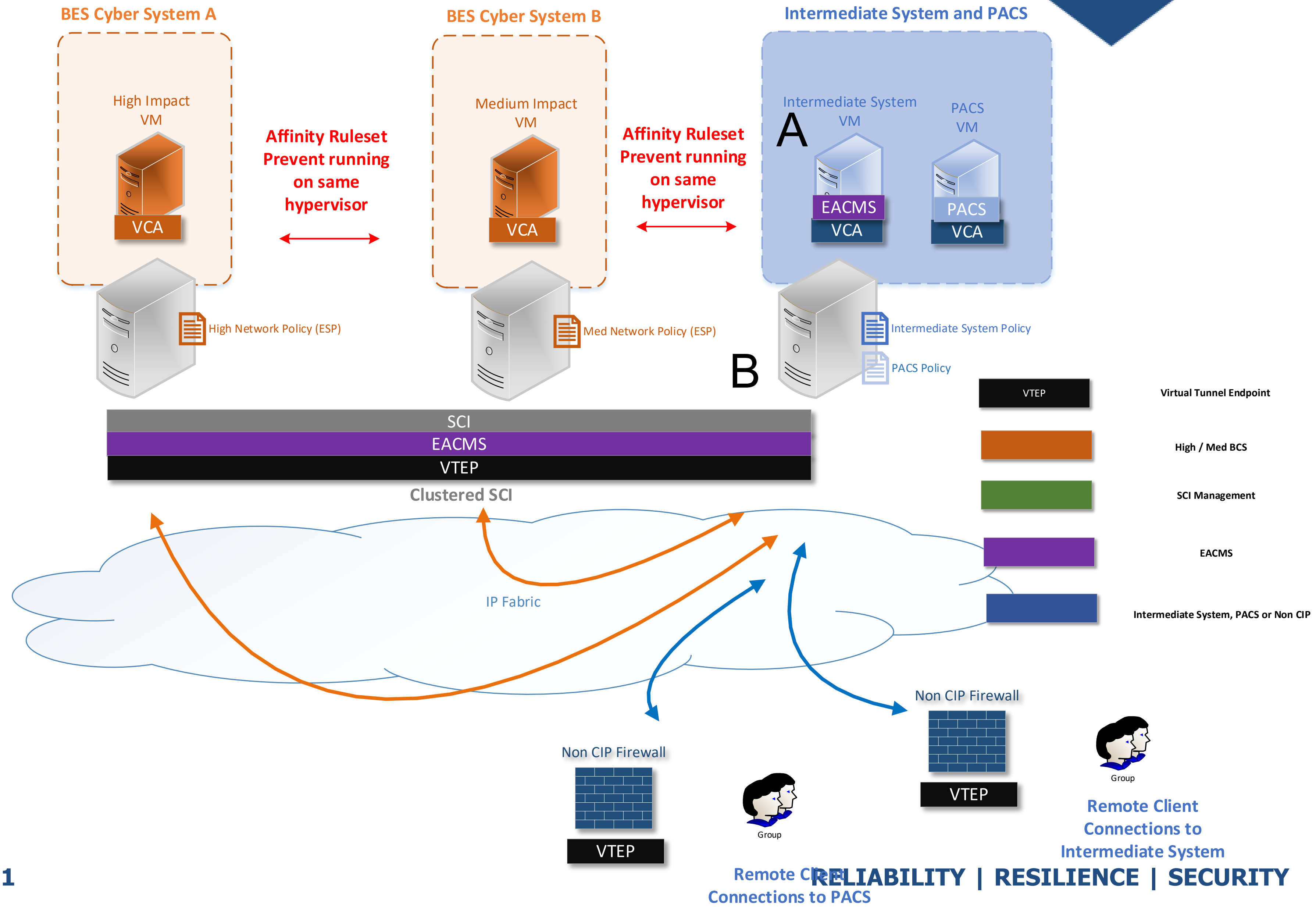
Keep CPU and Memory separate for High impact and Medium impact BCS VCAs

Otherwise

Any VCAs that share CPU or Memory become PCAs of the High / Medium impact BCS

# Intermediate Systems - Affinity

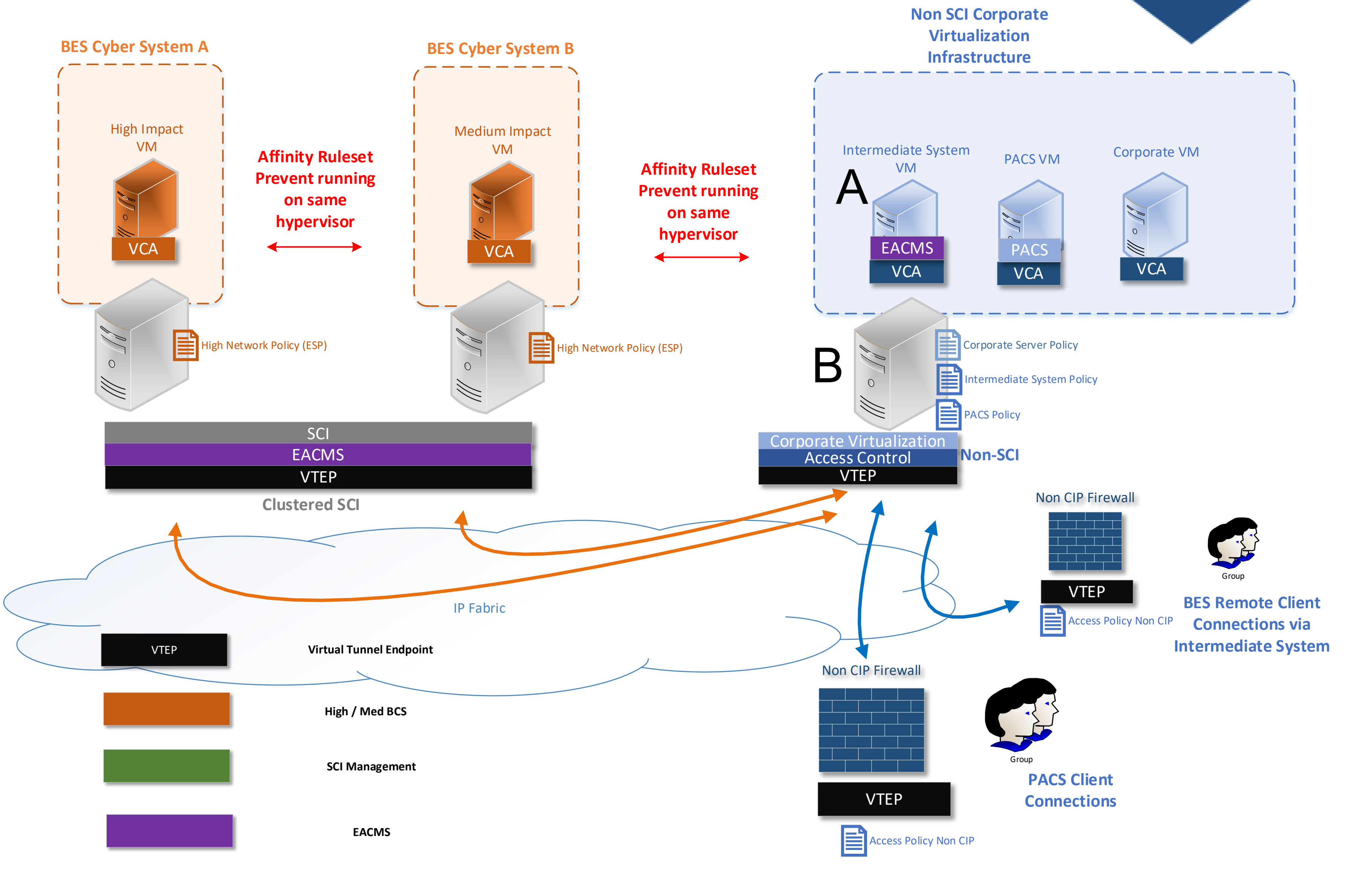
*Join at Slido.com Slido Event Code: 201602f*


BES Cyber System A
High Impact VM
VCA
High Network Policy (ESP)
Affinity Ruleset Prevent running on same hypervisor
BES Cyber System B
Medium Impact VM
VCA
Med Network Policy (ESP)
Affinity Ruleset Prevent running on same hypervisor
Intermediate System and PACS
Intermediate System VM
A
EACMS
VCA
PACS VM
PACS
VCA
Intermediate System Policy
PACS Policy
B
SCI
EACMS
VTEP
Clustered SCI
IP Fabric
Non CIP Firewall
VTEP
Group
Remote Client Connections to PACS
Non CIP Firewall
VTEP
Group
Remote Client Connections to Intermediate System
VTEP
Virtual Tunnel Endpoint
High / Med BCS
SCI Management
EACMS
Intermediate System, PACS or Non CIP

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Intermediate Systems - Affinity

*Join at Slido.com Slido Event Code: 201602f*



| | |
|---|---|
| VTEP | Virtual Tunnel Endpoint |
| 🟧 | High / Med BCS |
| 🟩 | SCI Management |
| 🟪 | EACMS |
| 🟦 | Intermediate System, PACS or Non CIP |

# Implementation Plan

# Implementation Plan

*Join at Slido.com Slido Event Code: 201602f*

- 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.

# Implementation Plan

*Join at Slido.com Slido Event Code: 201602f*

- Revised CIP Standards and Definitions Effective Date
  - Where approval by an applicable governmental authority is required, the Revised CIP Standards and Definitions shall become effective on the later of: (1) April 1, 2026; or (2) the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority.
- Other Minor non-substantive changes

# Resources Continued

*Join at Slido.com Slido Event Code: 201602f*

- 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

*Join at*
*Slido.com*
*Slido Event*
*Code: 201602f*

# Questions and Answers