NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Virtualization Workshop

Project 2016-02 |CIP-005, CIP-007, CIP-010

Standards Drafting Team
September 30, 2020

RELIABILITY | RESILIENCE | SECURITY

NERC Antitrust

slido.com
#2016-02

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. It is the responsibility of every NERC participant and employee who may in any way affect NERC’s compliance with the antitrust laws to carry out this commitment.

NERC Public Disclaimer

Participants are reminded that this meeting is public. Notice of the meeting was widely distributed. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Standard Drafting Team Work Product

slido.com
#2016-02

The content of this workshop represents the views of the Project 2016-02 standard drafting team regarding proposed revisions to NERC’s Reliability Standards. The purpose of this webinar is not to provide compliance advice for existing Reliability Standards. Questions regarding an individual entity’s compliance with existing Reliability Standards may be directed to ERO Enterprise compliance staff.

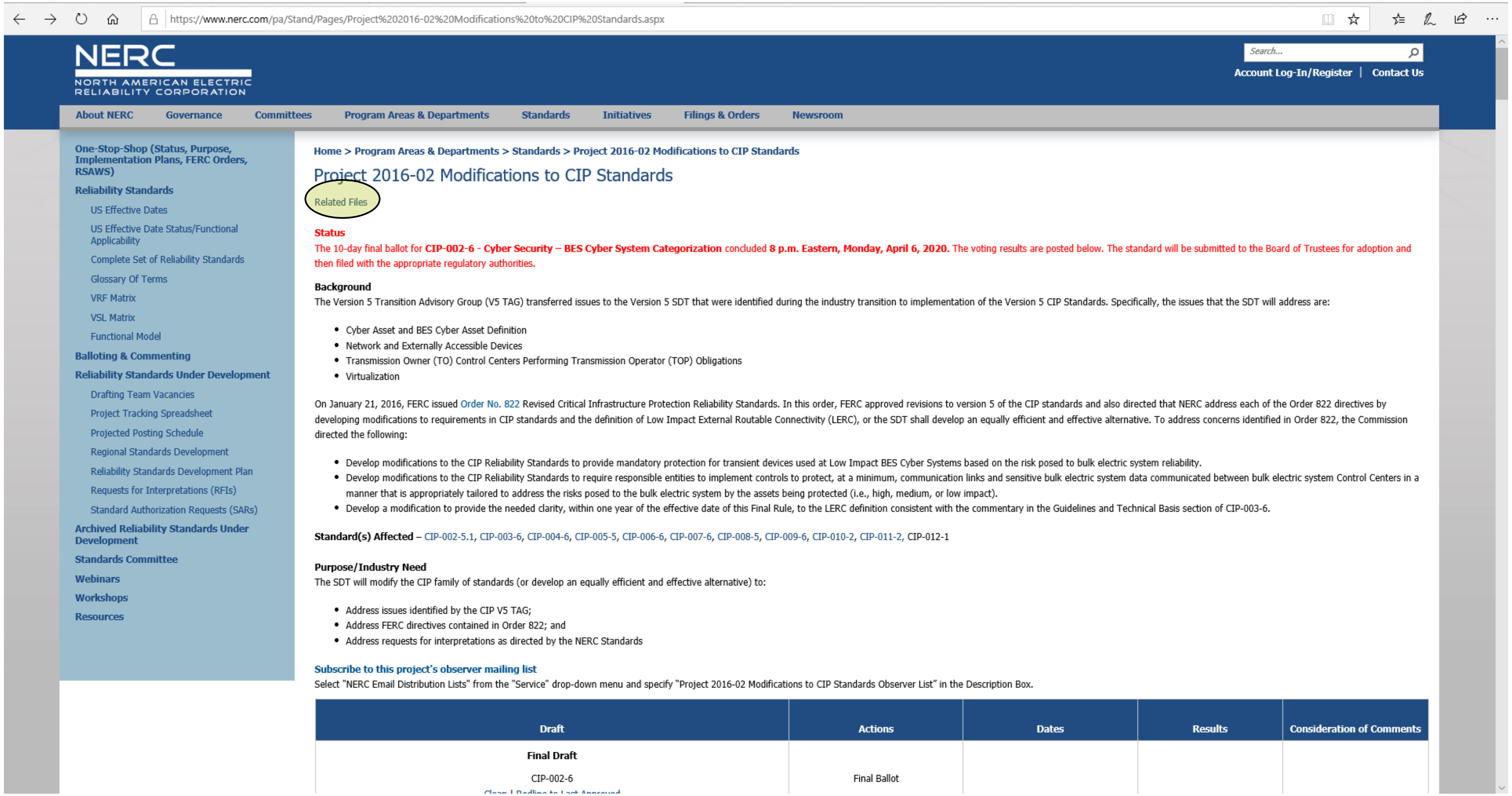
Agenda

slido.com
#2016-02

- Workshop Objective (12:00 – 12:10 p.m. Eastern)
- How to Participate (12:10 – 12:25 p.m.)
- Virtualization Definitions and Example Infrastructure
  - Establishing Infrastructure (12:25 – 12:50 p.m.)
- Walk-thru Standards
  - CIP-005 (1:00 – 2:30 p.m.)
  - CIP-007 (2:40 – 3:15 p.m.)
  - CIP-010 (3:25 – 4:20 p.m.)
- Q&A (4:20 – 5:00 p.m.)

Workshop Objectives

slido.com
#2016-02


https://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Search...
Account Log-In/Register | Contact Us
About NERC
Governance
Committees
Program Areas & Departments
Standards
Initiatives
Filings & Orders
Newsroom

- One-Stop-Shop (Status, Purpose, Implementation Plans, FERC Orders, RSAWS)
- Reliability Standards
  - US Effective Dates
  - US Effective Date Status/Functional Applicability
  - Complete Set of Reliability Standards
  - Glossary Of Terms
  - VRF Matrix
  - VSL Matrix
  - Functional Model
- Balloting & Commenting
- Reliability Standards Under Development
  - Drafting Team Vacancies
  - Project Tracking Spreadsheet
  - Projected Posting Schedule
  - Regional Standards Development
  - Reliability Standards Development Plan
  - Requests for Interpretations (RFIs)
  - Standard Authorization Requests (SARs)
- Archived Reliability Standards Under Development
- Standards Committee
- Webinars
- Workshops
- Resources

Home > Program Areas & Departments > Standards > Project 2016-02 Modifications to CIP Standards

Project 2016-02 Modifications to CIP Standards

Related Files

Status

The 10-day final ballot for **CIP-002-6 - Cyber Security – BES Cyber System Categorization** concluded **8 p.m. Eastern, Monday, April 6, 2020.** The voting results are posted below. The standard will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Background

The Version 5 Transition Advisory Group (V5 TAG) transferred issues to the Version 5 SDT that were identified during the industry transition to implementation of the Version 5 CIP Standards. Specifically, the issues that the SDT will address are:

- Cyber Asset and BES Cyber Asset Definition
- Network and Externally Accessible Devices
- Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations
- Virtualization

On January 21, 2016, FERC issued Order No. 822 Revised Critical Infrastructure Protection Reliability Standards. In this order, FERC approved revisions to version 5 of the CIP standards and also directed that NERC address each of the Order 822 directives by developing modifications to requirements in CIP standards and the definition of Low Impact External Routable Connectivity (LERC), or the SDT shall develop an equally efficient and effective alternative. To address concerns identified in Order 822, the Commission directed the following:

- Develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability.
- Develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact).
- Develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule, to the LERC definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.

Standard(s) Affected – CIP-002-5.1, CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, CIP-011-2, CIP-012-1

Purpose/Industry Need

The SDT will modify the CIP family of standards (or develop an equally efficient and effective alternative) to:

- Address issues identified by the CIP V5 TAG;
- Address FERC directives contained in Order 822; and
- Address requests for interpretations as directed by the NERC Standards

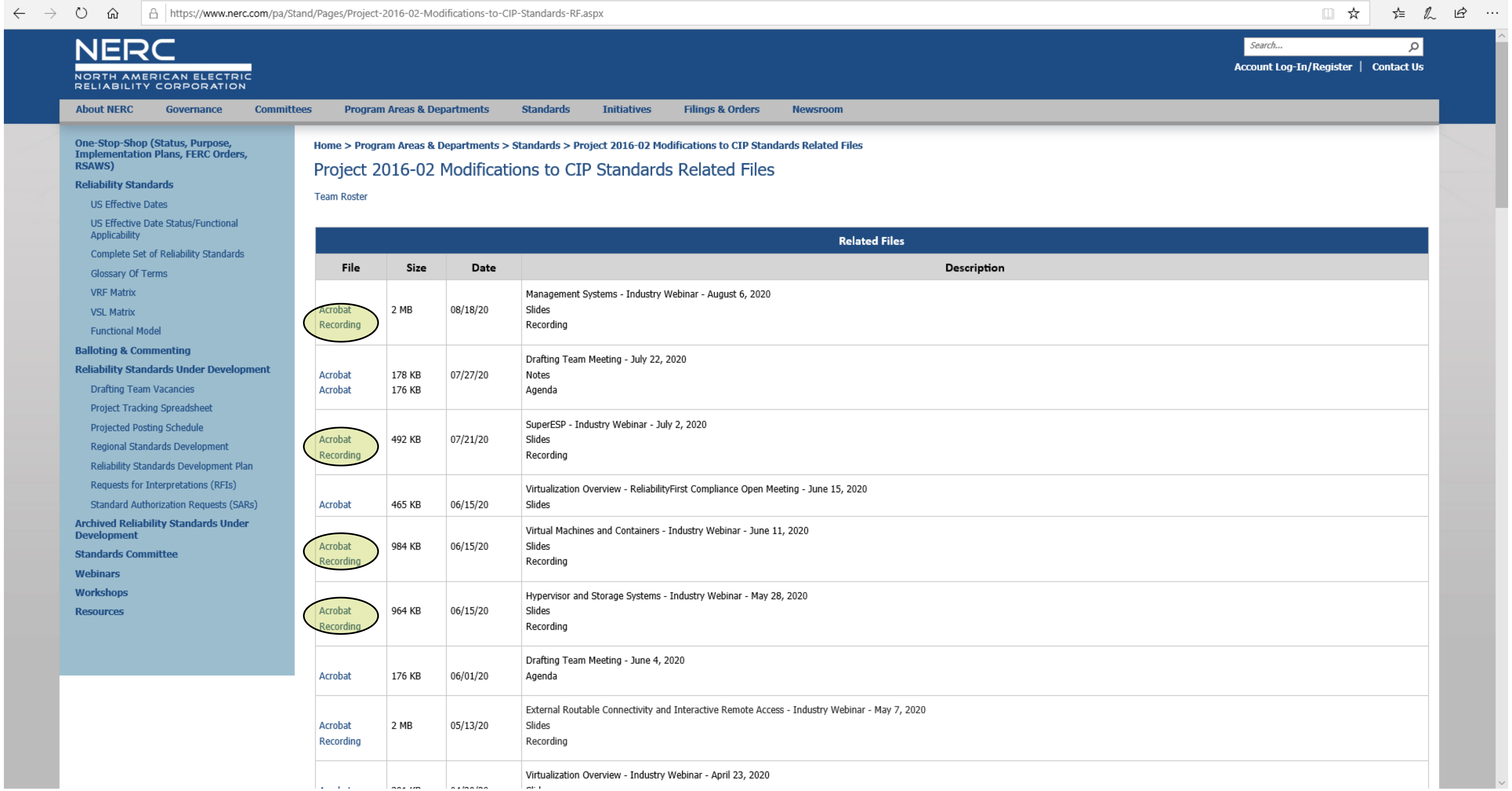
Subscribe to this project's observer mailing list

Select "NERC Email Distribution Lists" from the "Service" drop-down menu and specify "Project 2016-02 Modifications to CIP Standards Observer List" in the Description Box.

Draft	Actions	Dates	Results	Consideration of Comments
Final Draft CIP-002-6 Clean | Redline to Last Approved	Final Ballot			

Workshop Objectives

slido.com
#2016-02



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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Search...
Account Log-In/Register | Contact Us
About NERC
Governance
Committees
Program Areas & Departments
Standards
Initiatives
Filings & Orders
Newsroom
One-Stop-Shop (Status, Purpose, Implementation Plans, FERC Orders, RSAWS)
Reliability Standards
US Effective Dates
US Effective Date Status/Functional Applicability
Complete Set of Reliability Standards
Glossary Of Terms
VRF Matrix
VSL Matrix
Functional Model
Balloting & Commenting
Reliability Standards Under Development
Drafting Team Vacancies
Project Tracking Spreadsheet
Projected Posting Schedule
Regional Standards Development
Reliability Standards Development Plan
Requests for Interpretations (RFIs)
Standard Authorization Requests (SARs)
Archived Reliability Standards Under Development
Standards Committee
Webinars
Workshops
Resources

Home > Program Areas & Departments > Standards > Project 2016-02 Modifications to CIP Standards Related Files

Project 2016-02 Modifications to CIP Standards Related Files

Team Roster

Related Files

File	Size	Date	Description
Acrobat Recording	2 MB	08/18/20	Management Systems - Industry Webinar - August 6, 2020 Slides Recording
Acrobat Acrobat	178 KB 176 KB	07/27/20	Drafting Team Meeting - July 22, 2020 Notes Agenda
Acrobat Recording	492 KB	07/21/20	SuperESP - Industry Webinar - July 2, 2020 Slides Recording
Acrobat	465 KB	06/15/20	Virtualization Overview - ReliabilityFirst Compliance Open Meeting - June 15, 2020 Slides
Acrobat Recording	984 KB	06/15/20	Virtual Machines and Containers - Industry Webinar - June 11, 2020 Slides Recording
Acrobat Recording	964 KB	06/15/20	Hypervisor and Storage Systems - Industry Webinar - May 28, 2020 Slides Recording
Acrobat	176 KB	06/01/20	Drafting Team Meeting - June 4, 2020 Agenda
Acrobat Recording	2 MB	05/13/20	External Routable Connectivity and Interactive Remote Access - Industry Webinar - May 7, 2020 Slides Recording
			Virtualization Overview - Industry Webinar - April 23, 2020

Workshop Objectives

slido.com
#2016-02

FEEDBACK

Workshop Objectives

slido.com
#2016-02

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Virtualization and Future Technologies

Project 2016-02 Standards Drafting Team:
What's in it for me?

April 2020

RELIABILITY | RESILIENCE | SECURITY

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

Virtualization and Future Technologies

Project 2016-02 Standards Drafting Team:
The Case for Change

April 2019

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Virtualization Overview

Project 2016-02 – CIP Modifications

CIP SDT Members
March, 2020

RELIABILITY | ACCOUNTABILITY

Reminder

These changes to CIP standards are to ***ENABLE***
new methods/models

NOT

REQUIRE *Them*

Previous Approaches

slido.com
#2016-02

- Add Virtual to Cyber Asset definition
- Add a new CIP standard for virtualization
- Move to System level with objective requirements

- **Current Approach:** Parallel approach within current standards through additional definitions and focused requirement changes

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Providing Feedback

Ask anonymously at anytime!
Vote other’s questions up/down
Answer Polls and Surveys

Join at
slido.com
#2016-02

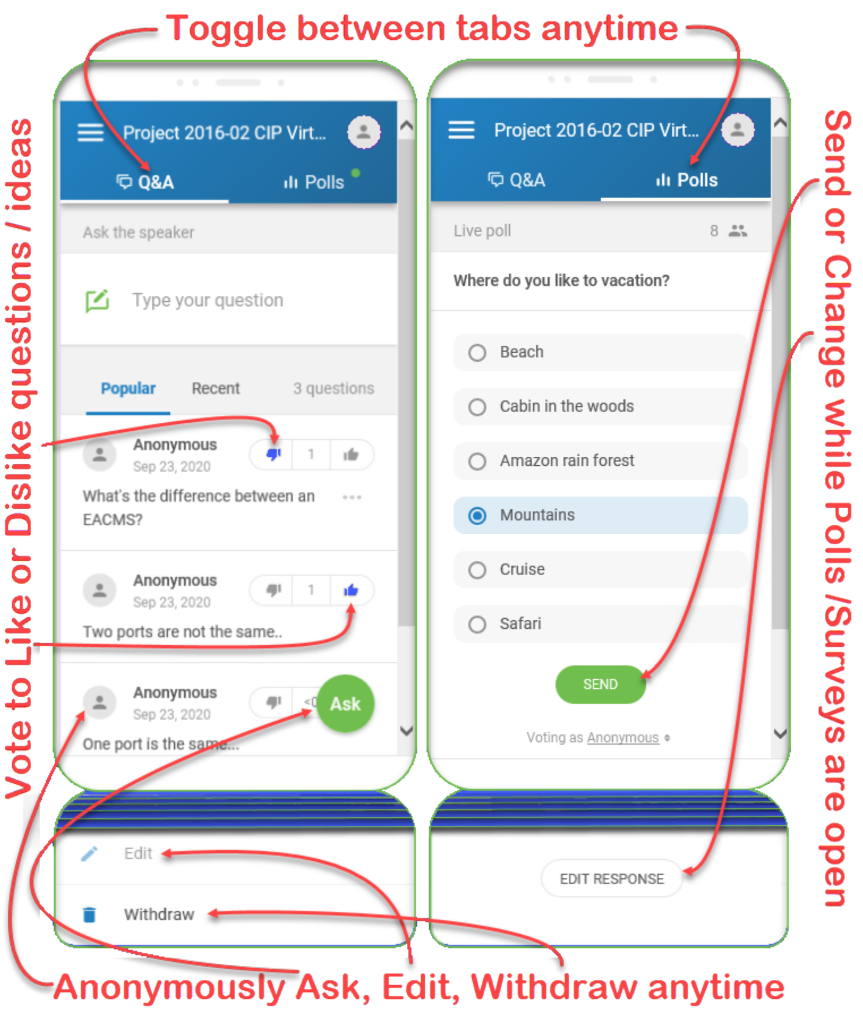
RELIABILITY | RESILIENCE | SECURITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Slido Features and Navigation

slido.com
#2016-02

Use the Mobile App or a Browser



Toggle between tabs anytime

Vote to Like or Dislike questions / ideas

Send or Change while Polls /Surveys are open

Anonymously Ask, Edit, Withdraw anytime

Project 2016-02 CIP Virt...
Q&A | Polls

Ask the speaker

Type your question

Popular | Recent | 3 questions

Anonymous
Sep 23, 2020
1
What's the difference between an EACMS?

Anonymous
Sep 23, 2020
1
Two ports are not the same..

Anonymous
Sep 23, 2020
One port is the same...

Ask

Edit
Withdraw

Project 2016-02 CIP Virt...
Q&A | Polls

Live poll 8

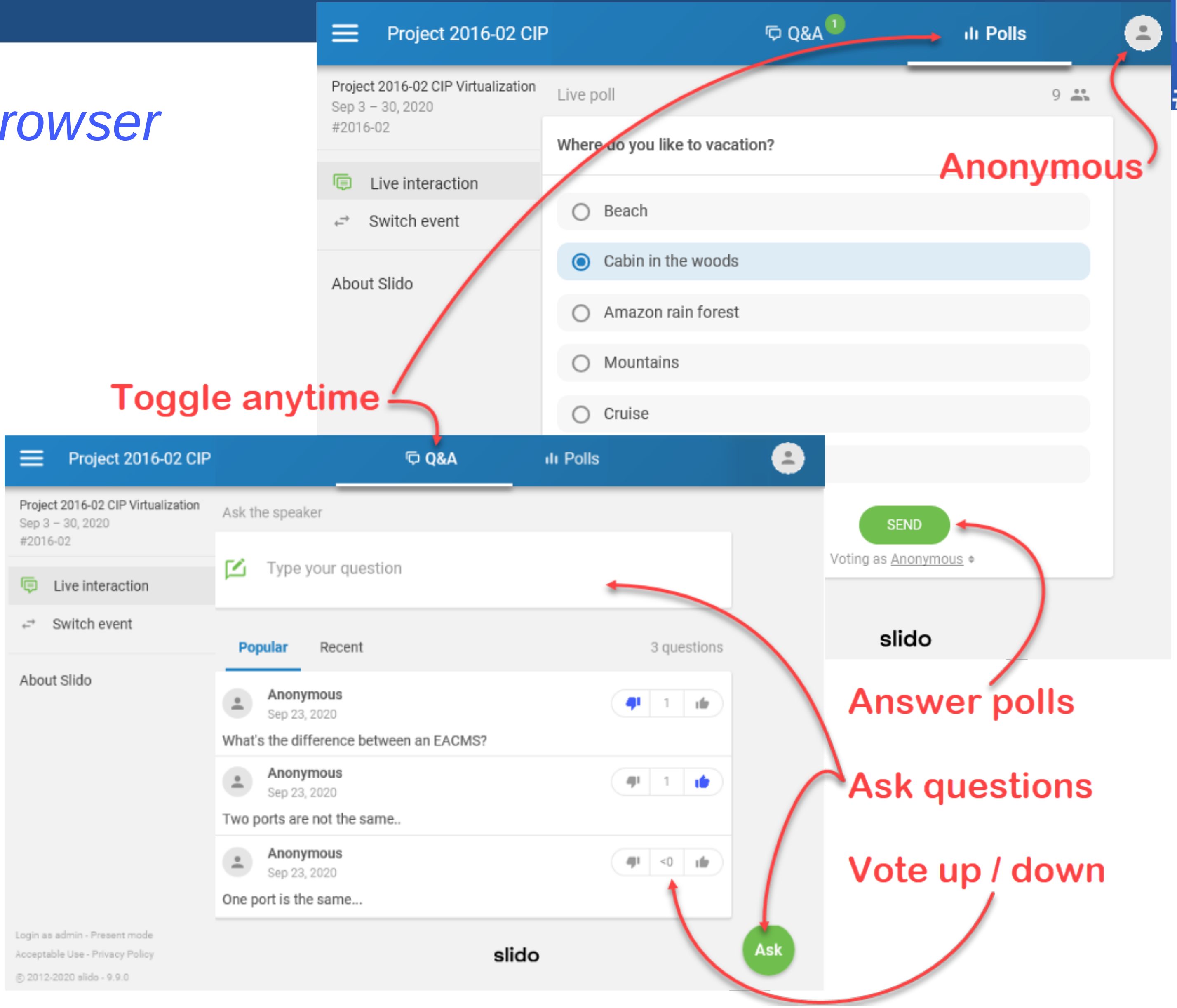
Where do you like to vacation?

○ Beach
○ Cabin in the woods
○ Amazon rain forest
● Mountains
○ Cruise
○ Safari

SEND

Voting as Anonymous

EDIT RESPONSE



Anonymous

Toggle anytime

Answer polls

Ask questions

Vote up / down

Project 2016-02 CIP
Q&A 1 | Polls

Project 2016-02 CIP Virtualization
Sep 3 – 30, 2020
#2016-02

Live interaction
Switch event
About Slido

Live poll 9

Where do you like to vacation?

○ Beach
● Cabin in the woods
○ Amazon rain forest
○ Mountains
○ Cruise

SEND

Voting as Anonymous

slido

Project 2016-02 CIP
Q&A | Polls

Project 2016-02 CIP Virtualization
Sep 3 – 30, 2020
#2016-02

Live interaction
Switch event
About Slido

Ask the speaker

Type your question

Popular | Recent | 3 questions

Anonymous
Sep 23, 2020
1
What's the difference between an EACMS?

Anonymous
Sep 23, 2020
1
Two ports are not the same..

Anonymous
Sep 23, 2020
0
One port is the same...

Login as admin · Present mode
Acceptable Use · Privacy Policy
© 2012-2020 slido · 9.9.0

slido

Ask

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Initial Survey

Join at
slido.com
#2016-02

RELIABILITY | RESILIENCE | SECURITY

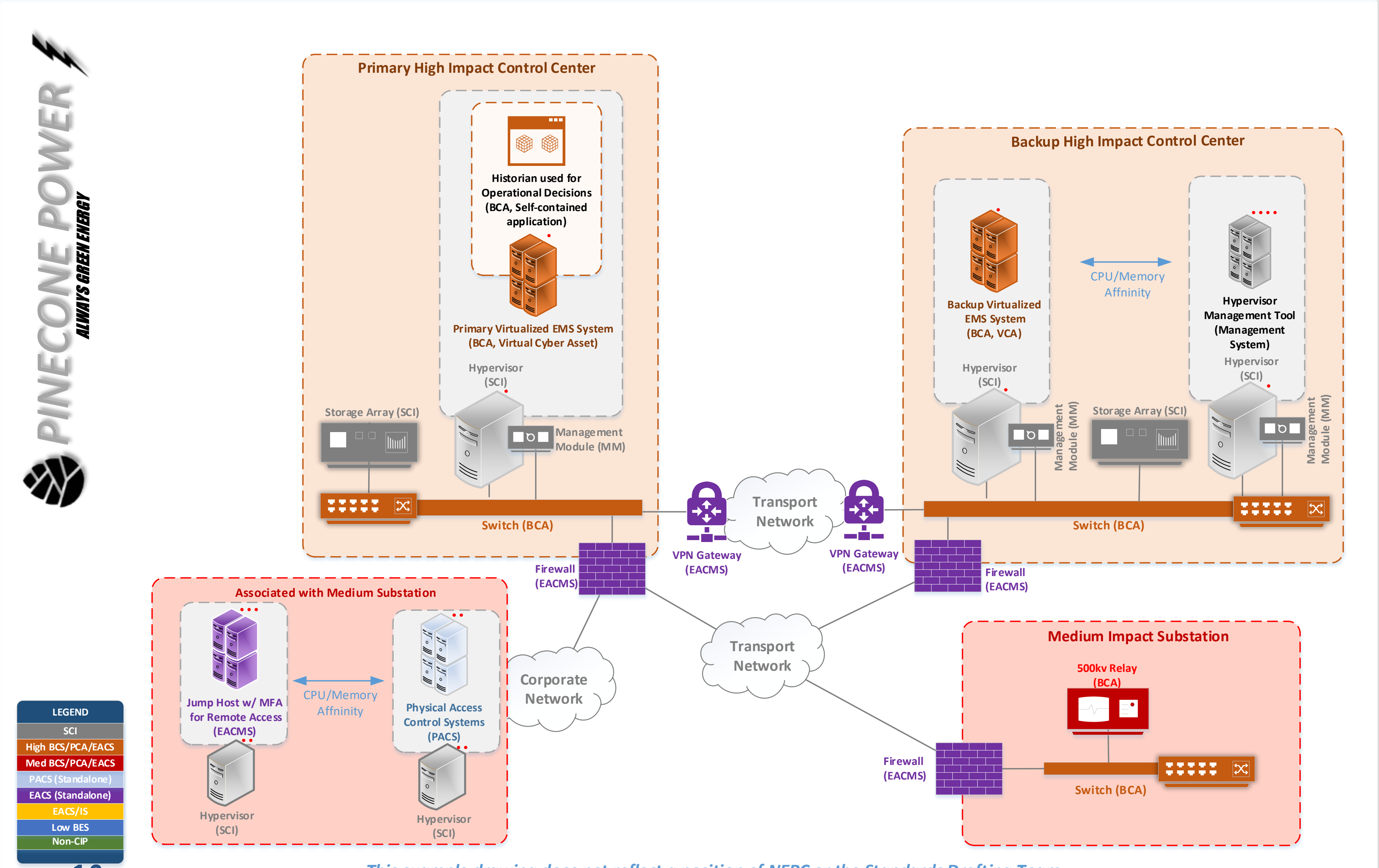
Virtualization Walkthrough Format

- Virtualization Concepts and Mechanics with Compliance
  - Establish a Example Infrastructure
    - Handout – Links sent to attendees via email
  - Walking the Pinecone Power example infrastructure through CIP-005, CIP-007, and CIP-010

Topology Example

slido.com
#2016-02

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

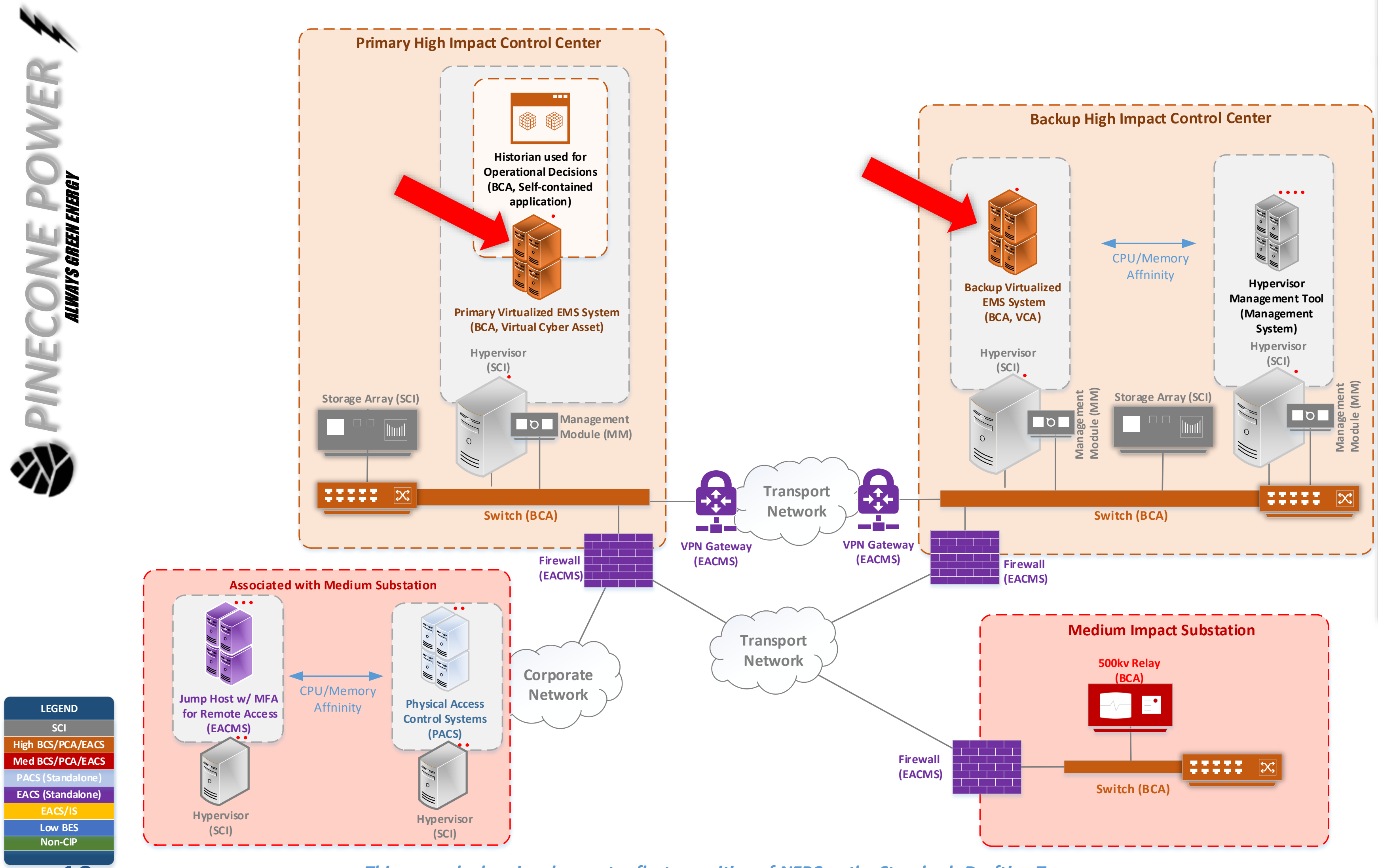
Asset List

- Asset List
  - Control Center (High)
    - Containerized Historian used for Operational Decisions
    - Geographically Distributed Virtual EMS System
    - Geographically Distributed Hypervisor Cluster, Including its Management System
    - Lights Out Management Module
    - Geographically Distributed Storage Array
    - Hypervisor Management Tool
  - Substation (Medium)
    - 500kv Relay
  - Corporate Network
    - Jumphost w/ MFA for Remote Access associated with Substation
    - Hypervisors associated with Substation
    - Centralized PACS System associated with Medium Impact BCS

Geographically Distributed Virtual EMS System

slido.com #2016-02

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

BES Cyber Asset

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

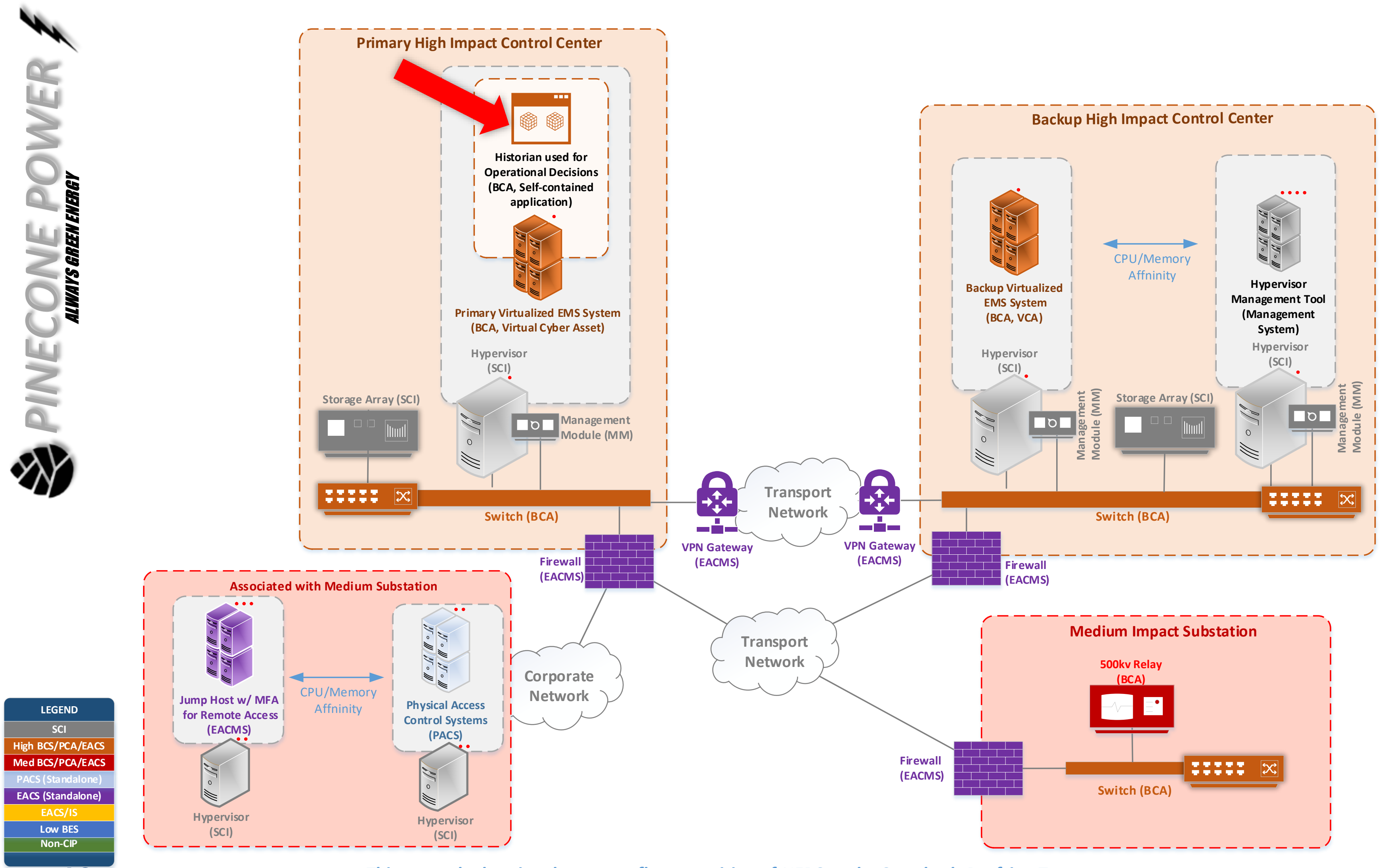
Virtual Cyber Asset

A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure.

Containerized Historian used for Operational Decisions

slido.com
#2016-02

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

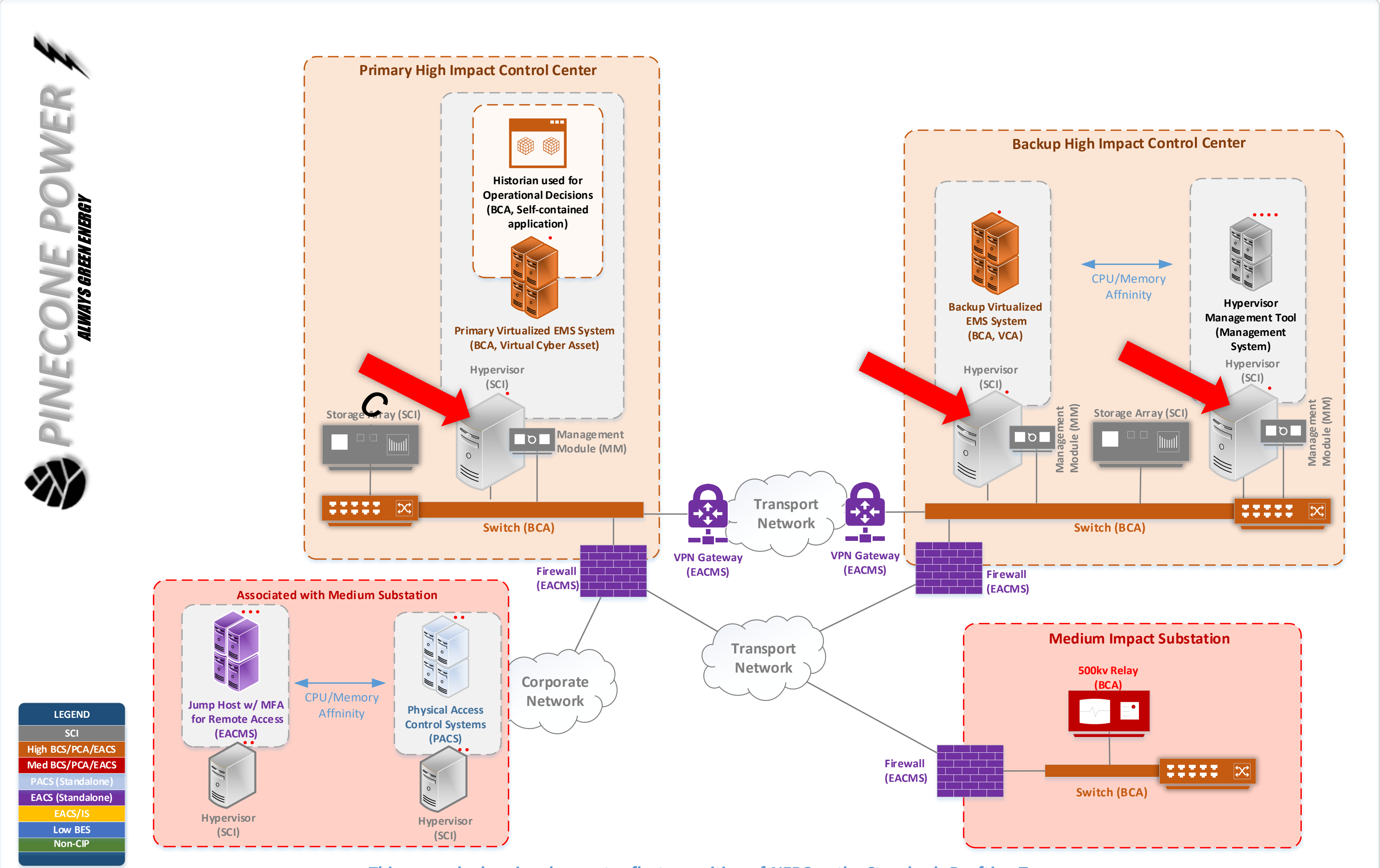
Self-Contained Application

Immutable software binaries containing operating system dependencies and application software packaged to execute in an isolated environment.

SCI Hypervisors Geographically Distributed Cluster

slido.com
#2016-02

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

Shared Cyber Infrastructure

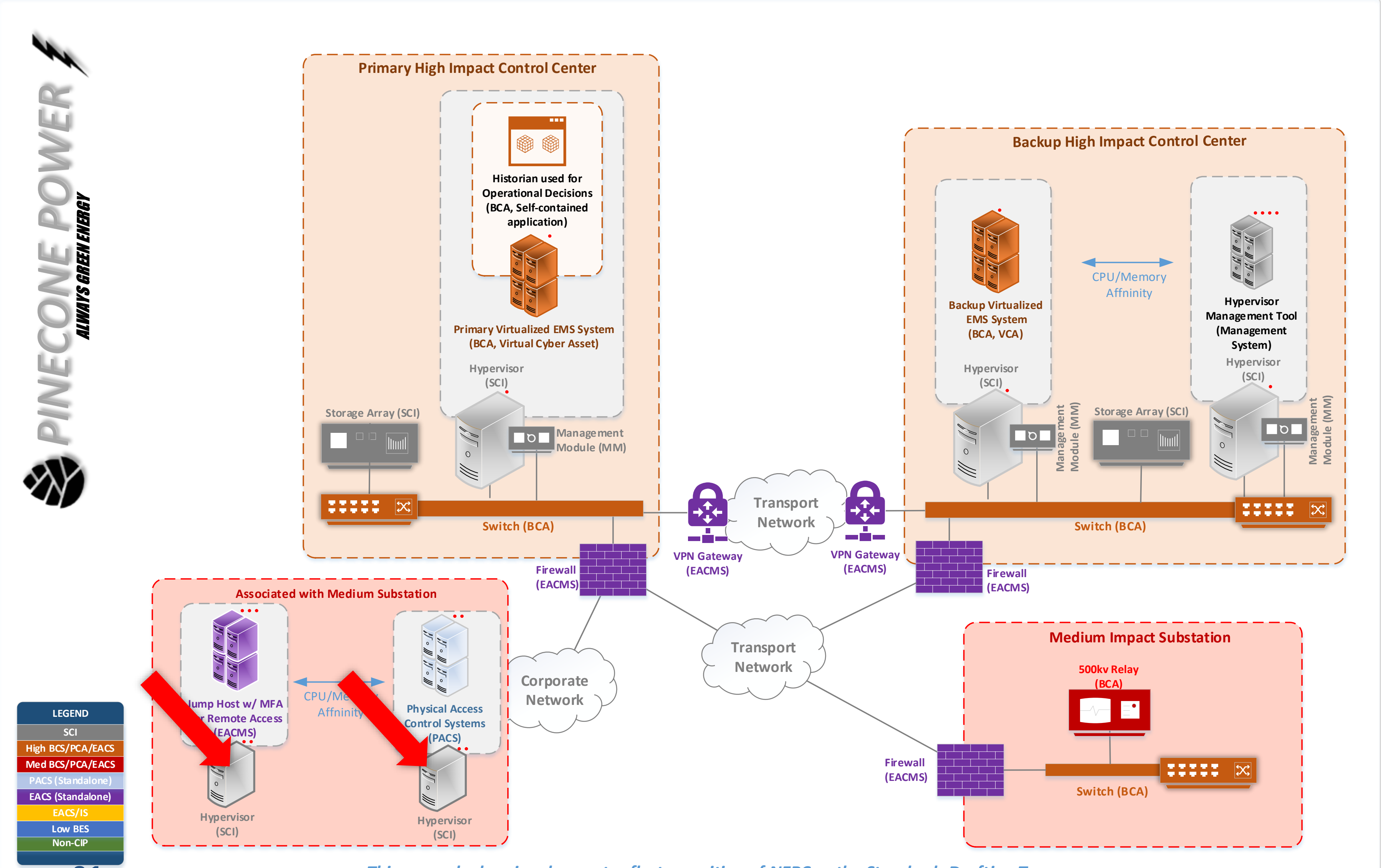
One or more programmable electronic devices (excluding Management Modules) and their software that share their computer or storage resources with one or more Virtual Cyber Assets or other Cyber Assets; including Management Systems used to initialize, deploy, or configure the SCI.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SCI for medium PACS, EACS

slido.com
#2016-02

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

Shared Cyber Infrastructure

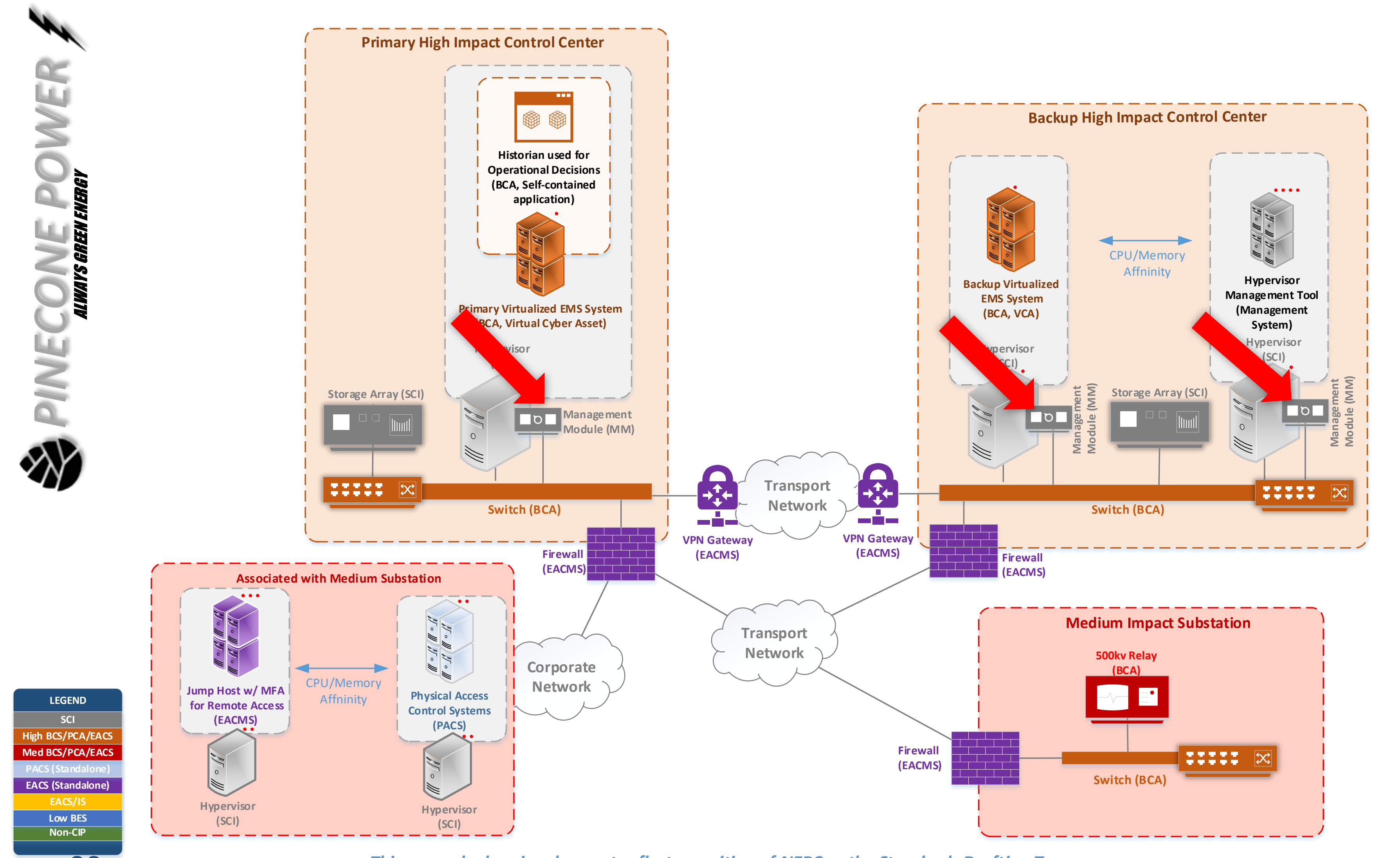
One or more programmable electronic devices (excluding Management Modules) and their software that share their computer or storage resources with one or more Virtual Cyber Assets or other Cyber Assets; including Management Systems used to initialize, deploy, or configure the SCI.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lights Out Management Module

slido.com
#2016-02

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



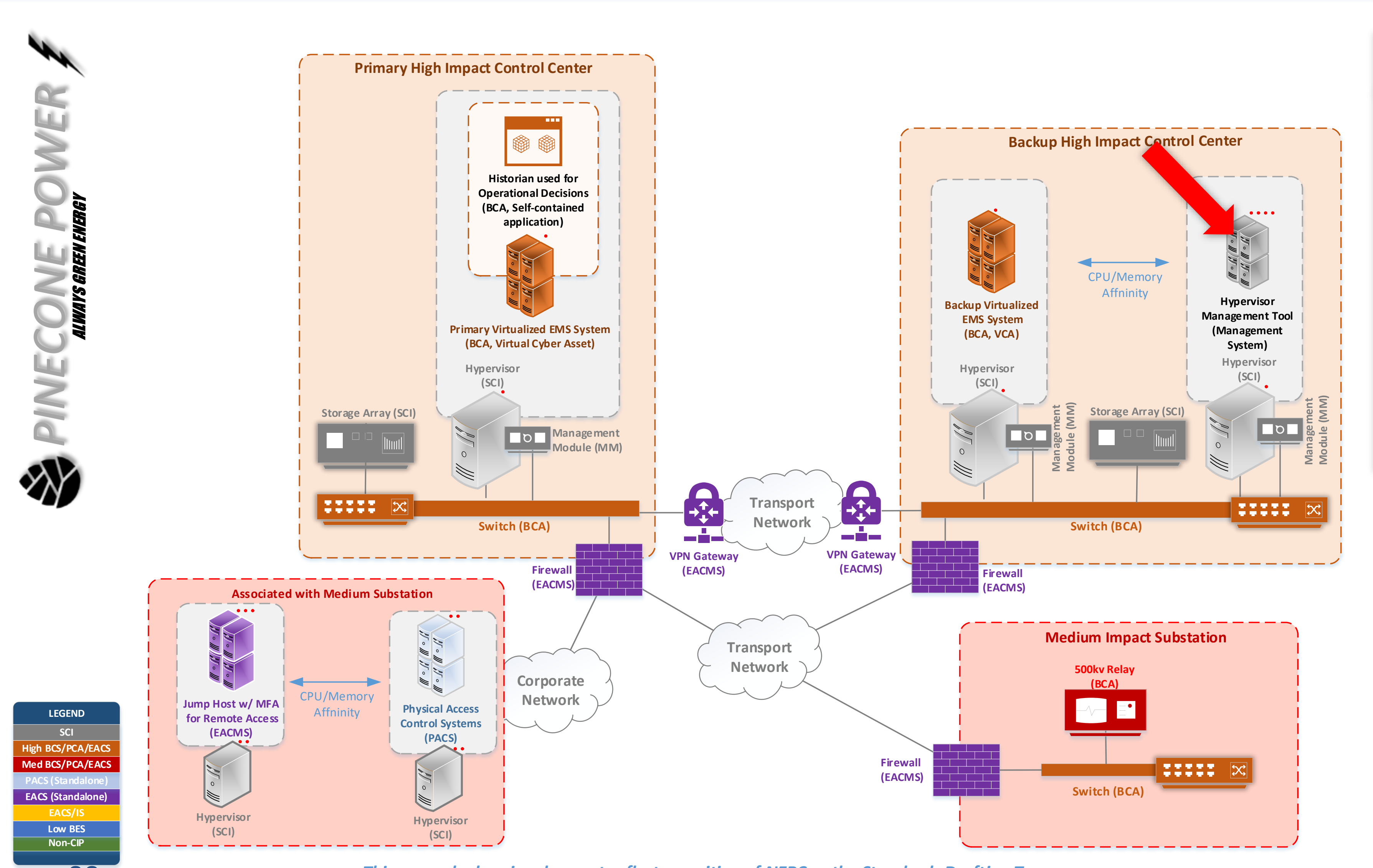
This example drawing does not reflect a position of NERC or the Standards Drafting Team

Management Module

An autonomous subsystem of a Cyber Asset or SCI that provides management and monitoring capabilities independently of the host system's CPU, firmware (BIOS or UEFI), and operating system.

Hypervisor Management Tool

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

Shared Cyber Infrastructure

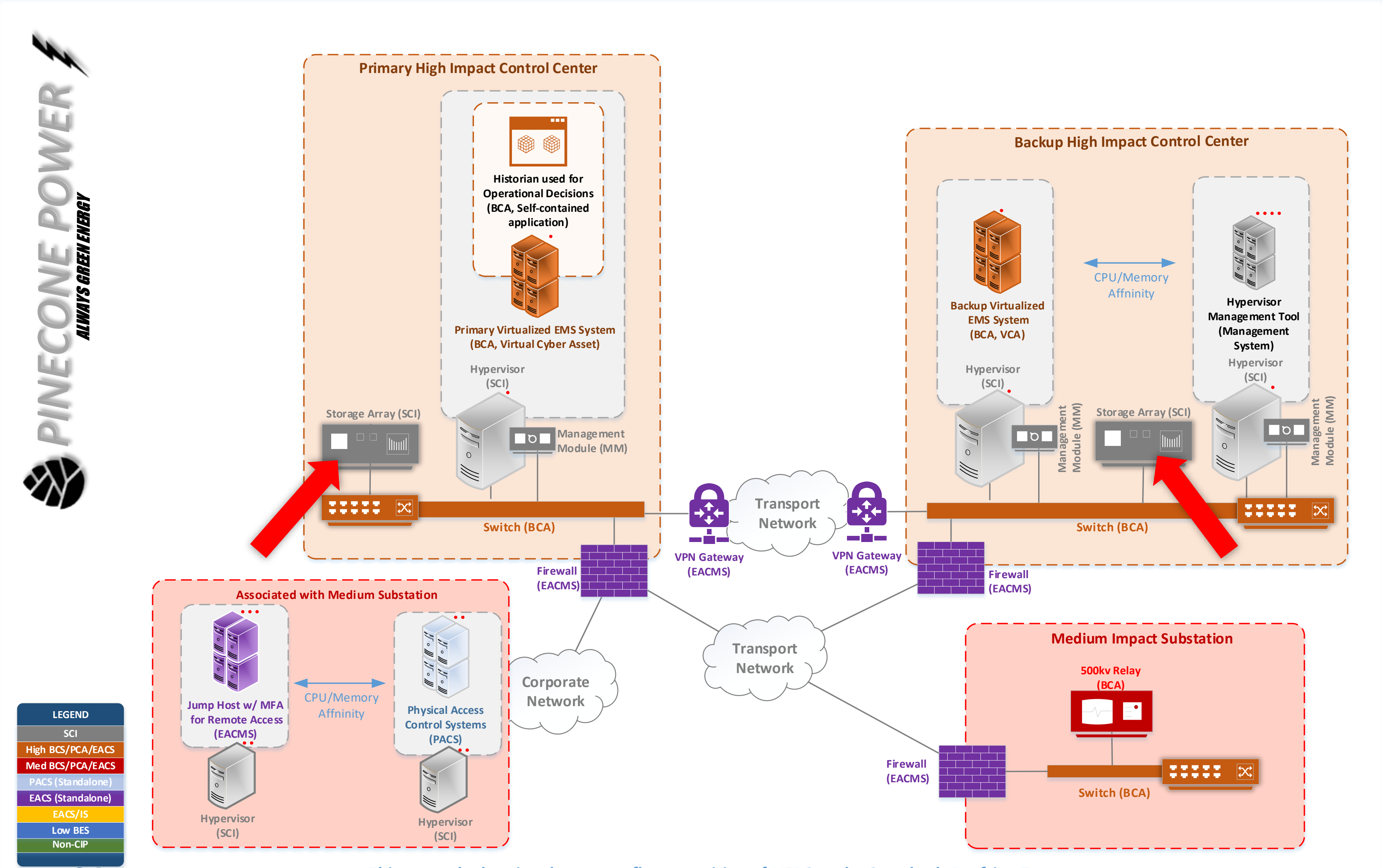
One or more programmable electronic devices (excluding Management Modules) and their software that share their computer or storage resources with one or more Virtual Cyber Assets or other Cyber Assets; including Management Systems used to initialize, deploy, or configure the SCI.

Management Systems

Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of Virtual Cyber Assets or Cyber Assets, through control of the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.

Geographically Distributed Storage Array

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



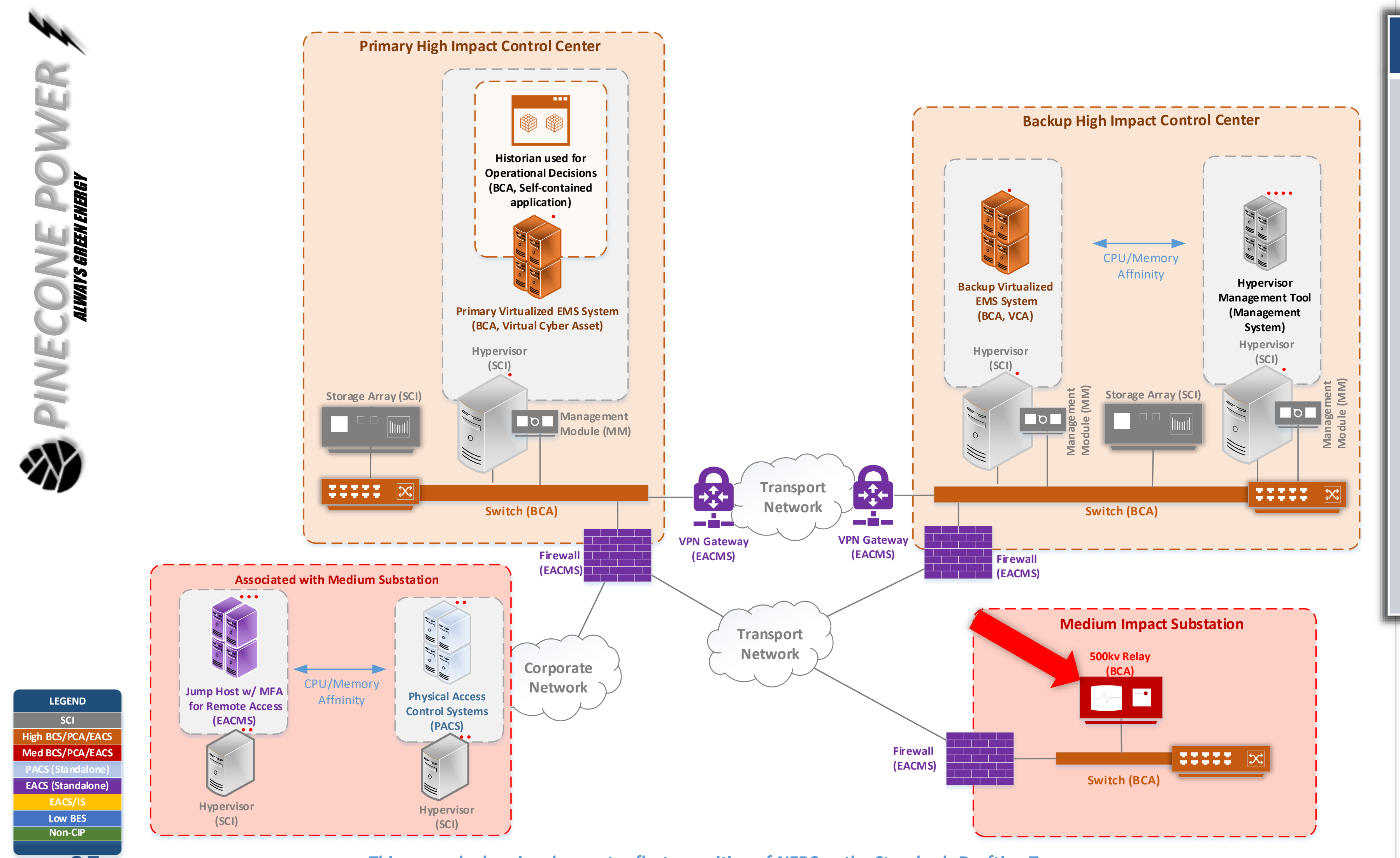
This example drawing does not reflect a position of NERC or the Standards Drafting Team

Shared Cyber Infrastructure

One or more programmable electronic devices (excluding Management Modules) and their software that share their computer or storage resources with one or more Virtual Cyber Assets or other Cyber Assets; including Management Systems used to initialize, deploy, or configure the SCI.

500KV Relay

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

BES Cyber Asset

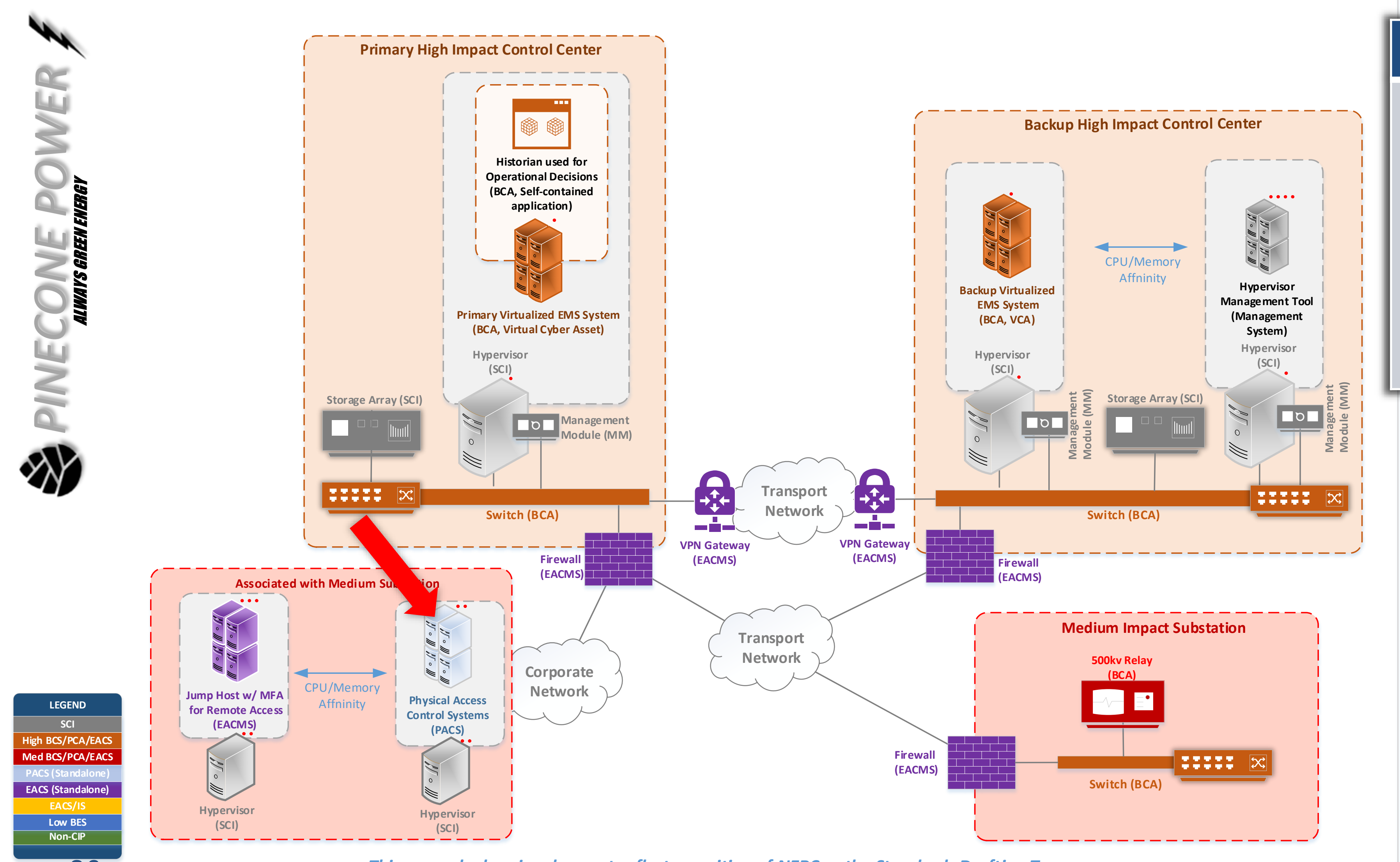
A Cyber Asset or Virtual Cyber Asset; excluding Shared Cyber Infrastructure , that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded,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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Centralized PACS System associated with Medium BCS

slido.com
#2016-02

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

Physical Access Control Systems

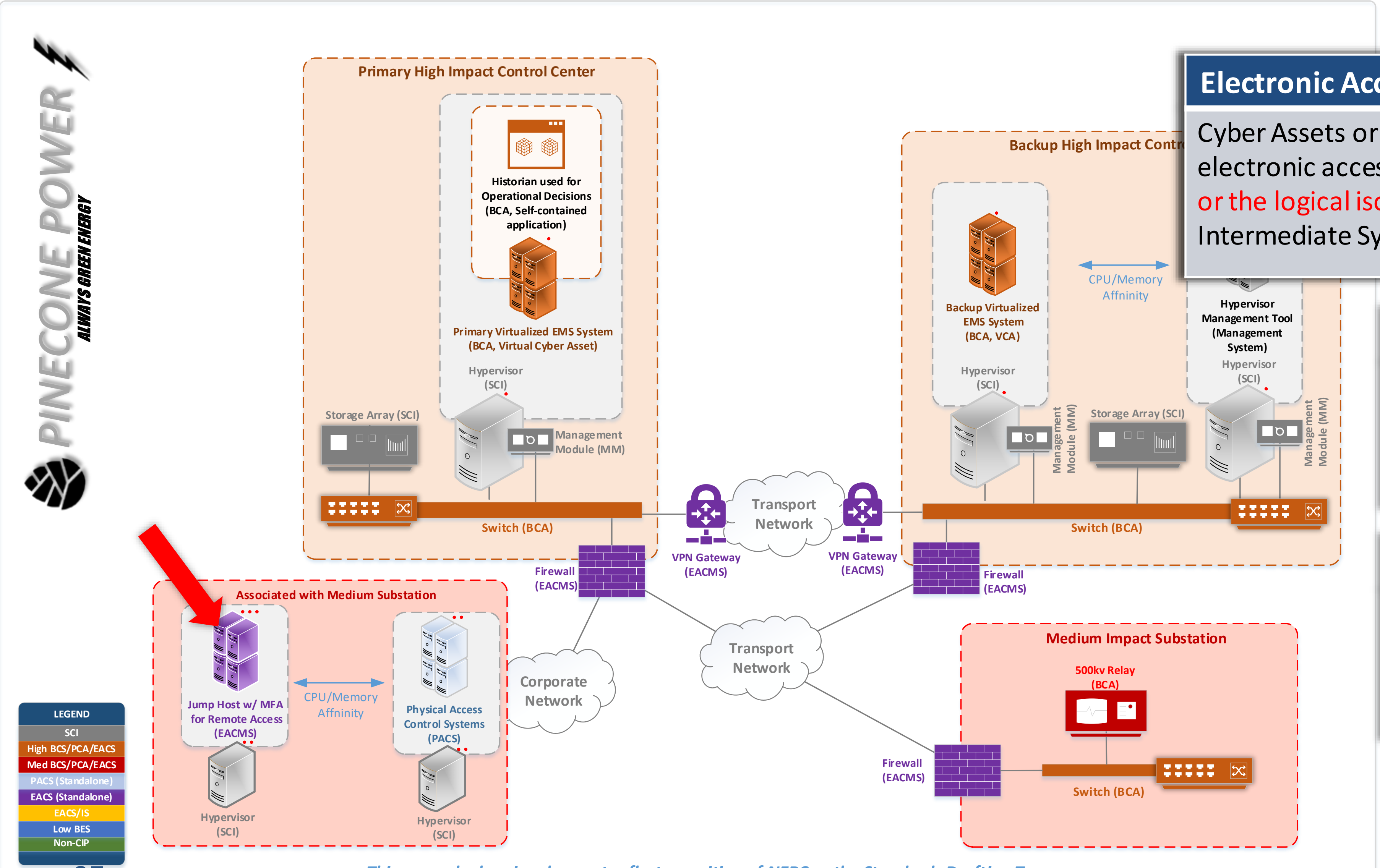
Cyber Assets or Virtual Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Virtual Cyber Asset

A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure.

Jumphost w/ MFA for Remote Access associated with Medium BCS

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

Electronic Access Control or Monitoring Systems

Cyber Assets or Virtual Cyber Assets that perform electronic access control or electronic access monitoring or the logical isolation of BES Cyber Systems. This includes Intermediate Systems.

Intermediate System

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

Interactive Remote Access

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

Asset List

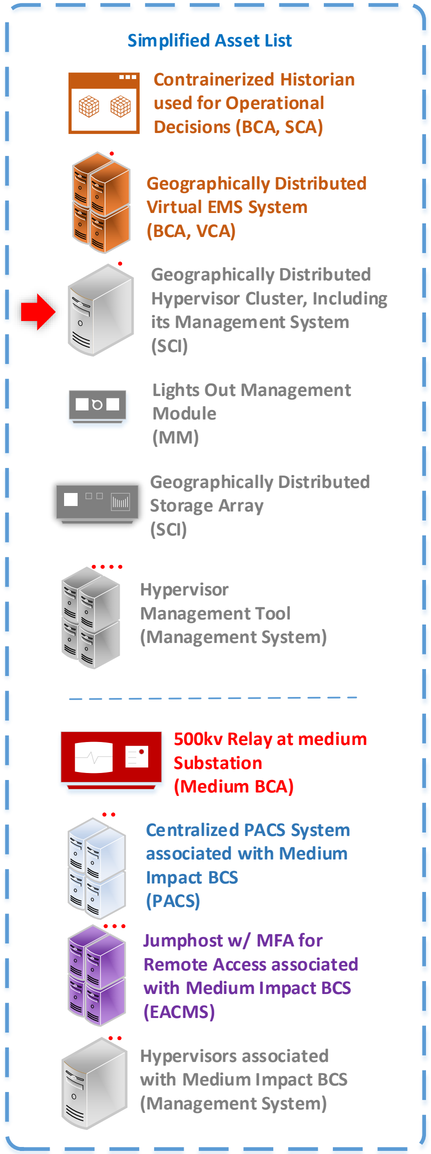
slido.com #2016-02

- Asset List
  - Control Center (containing High Assets)
    - Containerized Historian used for Operational Decisions (BCA, VCA)
    - Geographically Distributed Virtual EMS System (BCA, VCA)
    - Geographically Distributed Hypervisor Cluster, Including its Management System (Shared Cyber Infrastructure)
    - Lights Out Management Module (Management Module)
    - Geographically Distributed Storage Array (Shared Cyber Infrastructure)
    - Hypervisor Management Tool (Management System)
  - Medium Substation (containing Medium Assets)
    - 500kv Relay (BES Cyber Asset)
    - Centralized PACS System associated with Medium Impact BCS (PACS)
    - Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
    - Hypervisors associated with Medium Impact BCS (Shared Cyber Infrastructure)

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Mapping Asset List to Visual Aid

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

- Asset List
  - Control Center (containing High Assets)
    - Containerized Historian used for Operational Decisions (BCA, VCA)
    - Geographically Distributed Virtual EMS System (BCA, VCA)
    - Geographically Distributed Hypervisor Cluster, Including its Management System (Shared Cyber Infrastructure)
    - Lights Out Management Module (Management Module)
    - Geographically Distributed Storage Array (Shared Cyber Infrastructure)
    - Hypervisor Management Tool (Management System)
  - Medium Substation (containing Medium Assets)
    - 500kv Relay (BES Cyber Asset)
    - Centralized PACS System associated with Medium Impact BCS (PACS)
    - Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
    - Hypervisor associated with Medium Impact BCS (Management System)

Q&A Response

Join at

slido.com

#2016-02

RELIABILITY | RESILIENCE | SECURITY

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Break

We will return at X:XX p.m. Eastern

Join at
slido.com
#2016-02

RELIABILITY | RESILIENCE | SECURITY

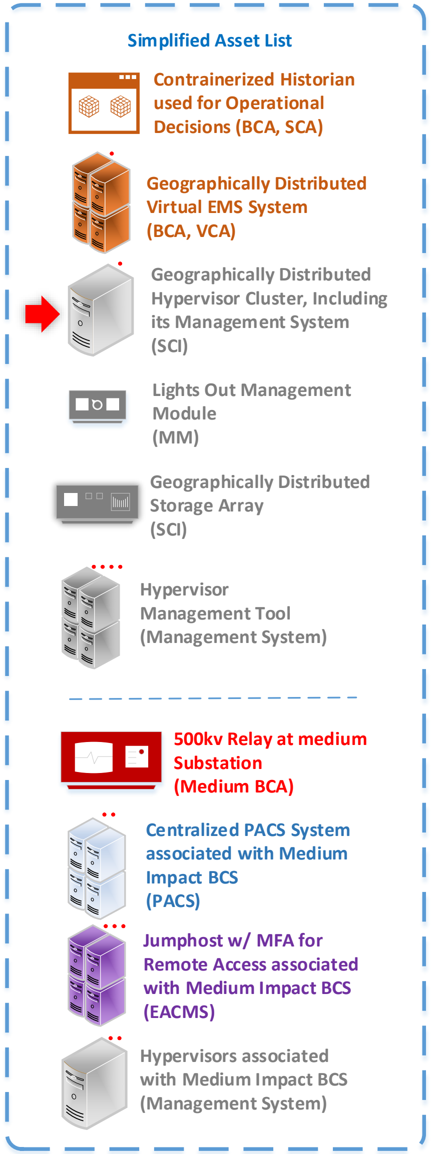
Q&A Response

Join at

slido.com

#2016-02

Mapping Asset List to Visual Aid



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

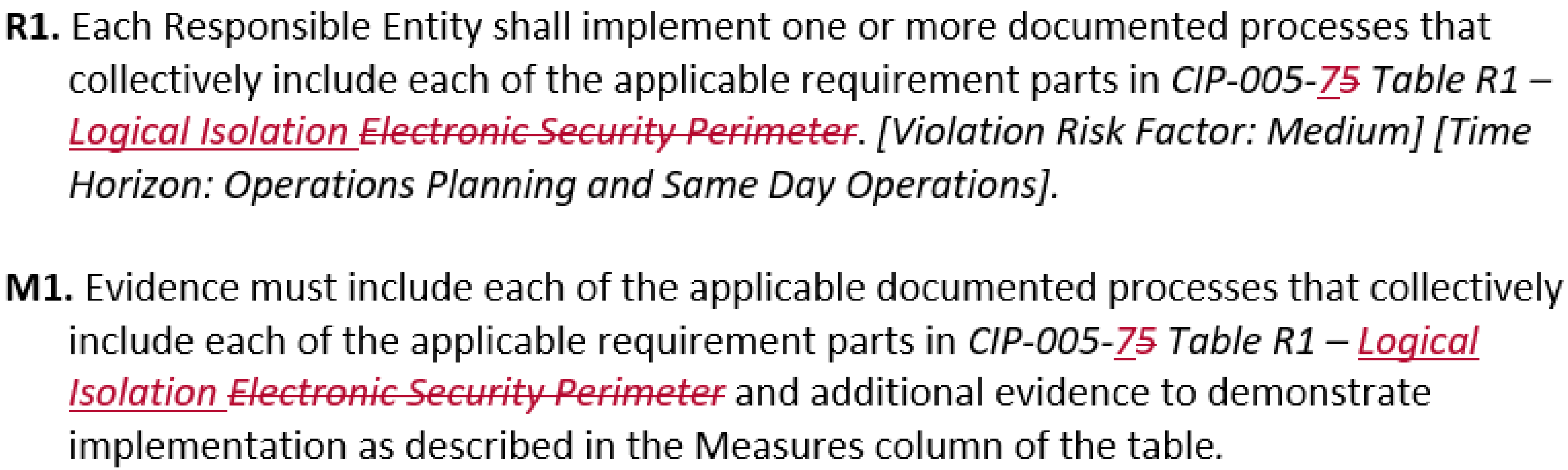
Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

- Asset List
  - Control Center (containing High Assets)
    - Containerized Historian used for Operational Decisions (BCA, VCA)
    - Geographically Distributed Virtual EMS System (BCA, VCA)
    - Geographically Distributed Hypervisor Cluster, Including its Management System (Shared Cyber Infrastructure)
    - Lights Out Management Module (Management Module)
    - Geographically Distributed Storage Array (Shared Cyber Infrastructure)
    - Hypervisor Management Tool (Management System)
  - Medium Substation (containing Medium Assets)
    - 500kv Relay (BES Cyber Asset)
    - Centralized PACS System associated with Medium Impact BCS (PACS)
    - Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
    - Hypervisor associated with Medium Impact BCS (Shared Cyber Infrastructure)

Proposed CIP-005 Requirement R1

slido.com
#2016-02

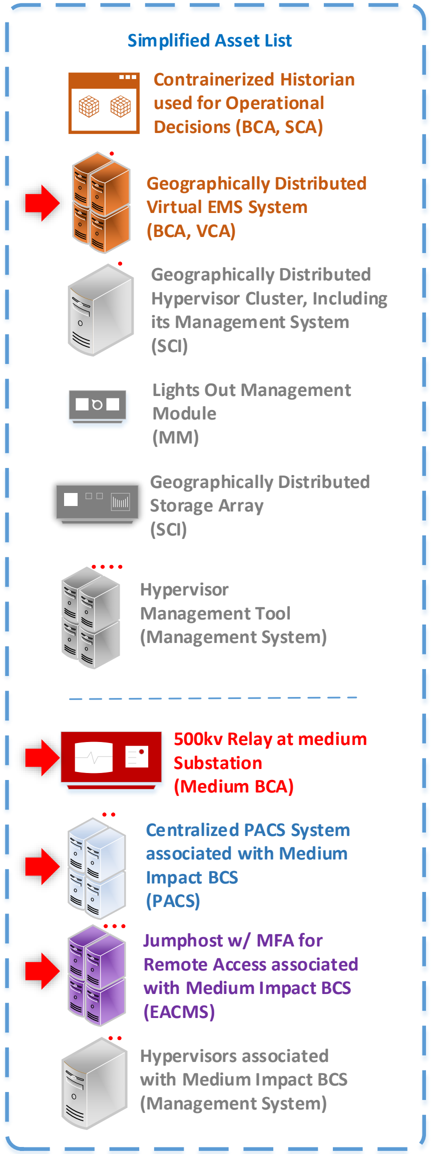


R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7~~5~~ Table R1 – Logical Isolation ~~Electronic Security Perimeter~~. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7~~5~~ Table R1 – Logical Isolation ~~Electronic Security Perimeter~~* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Proposed CIP-005 R1 Part 1.1

slido.com
#2016-02



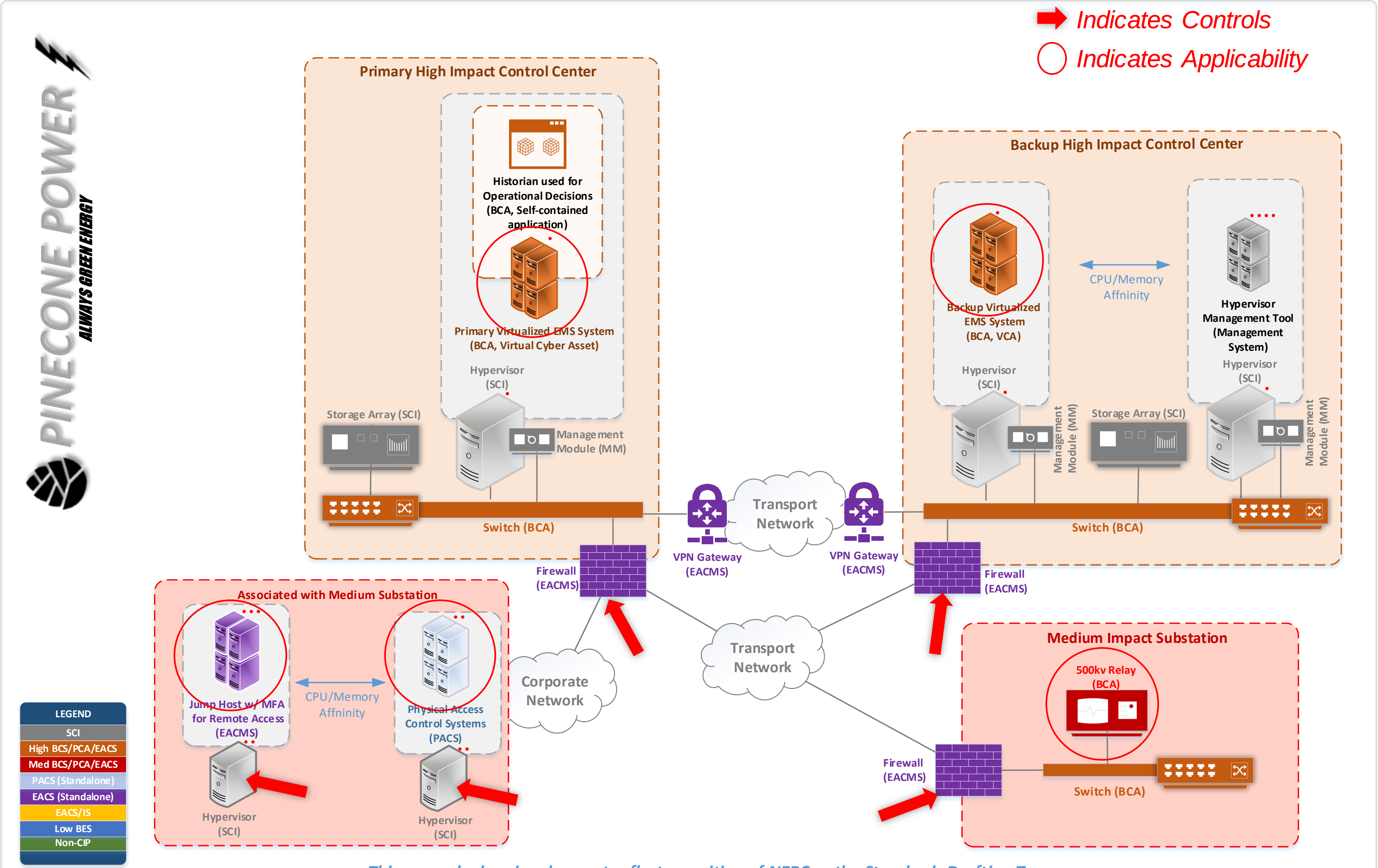
Simplified Asset List

- Contrainerized Historian used for Operational Decisions (BCA, SCA)
- Geographically Distributed Virtual EMS System (BCA, VCA)
- Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)
- Lights Out Management Module (MM)
- Geographically Distributed Storage Array (SCI)
- Hypervisor Management Tool (Management System)
- 500kv Relay at medium Substation (Medium BCA)
- Centralized PACS System associated with Medium Impact BCS (PACS)
- Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
- Hypervisors associated with Medium Impact BCS (Management System)

1.1	High Impact BES Cyber Systems connected to a network via routable protocol and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI Medium Impact BES Cyber Systems connected to a network via routable protocol and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI	~~All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.~~ Permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	~~An e~~Examples of evidence may include, but is not limited to, documentation that includes the configuration of systems that enforce electronic access control and logical isolation and document business need such as: • Network infrastructure configuration or policies (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • SCI configuration or policies (hypervisor, fabric, back-plane, or SAN configuration) ~~a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.~~

CIP-005 R1 Part 1.1 - Perimeter Model

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R1 Part 1.1

Permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Implemented Controls – Option 1

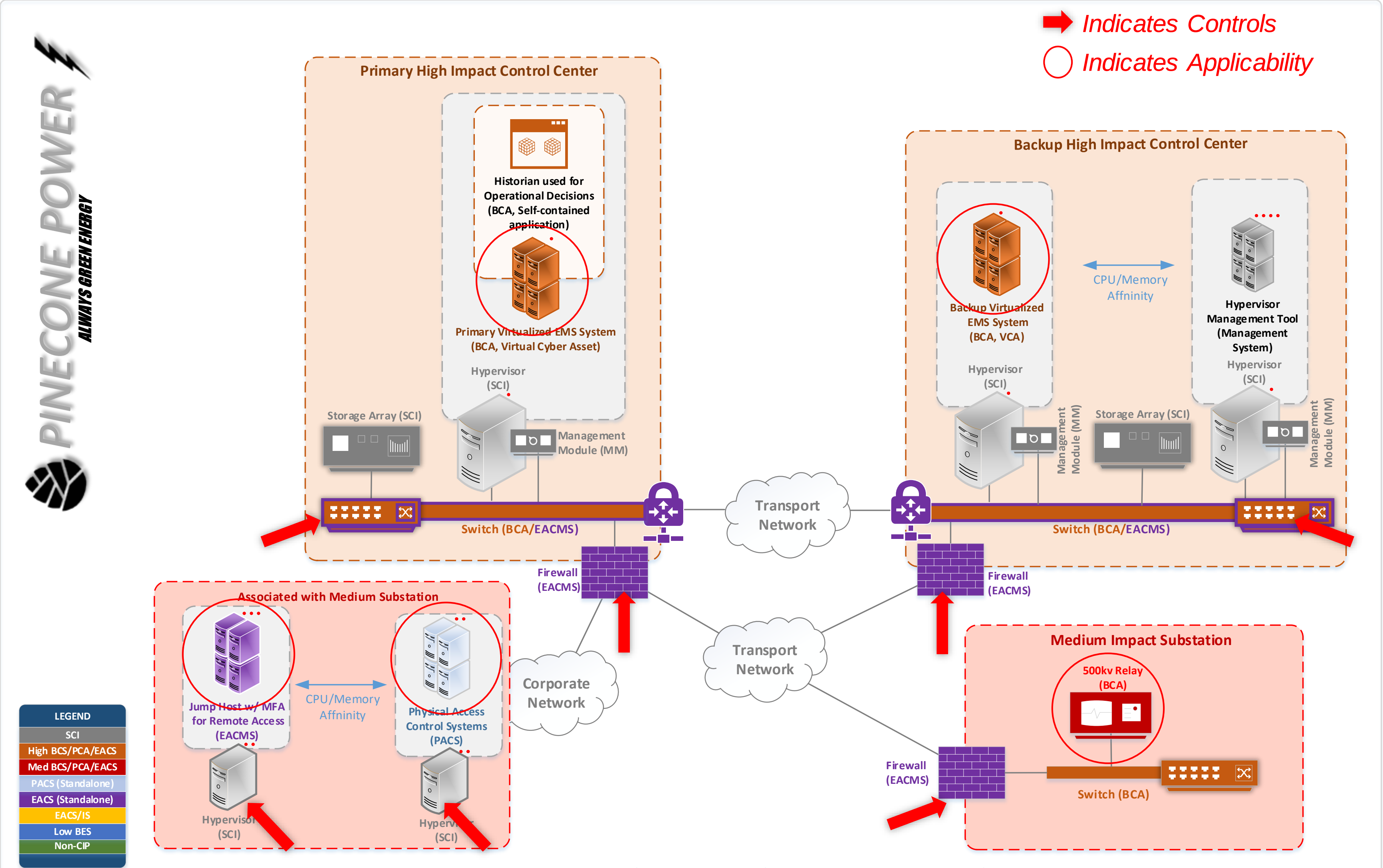
1.1 at Firewalls; implemented on Hypervisor for PACS/EACMS

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-005 R1 Part 1.1 – VLAN Model

slido.com
#2016-02

Workshop Sample Infrastructure – VLAN Model (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R1 Part 1.1

Permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

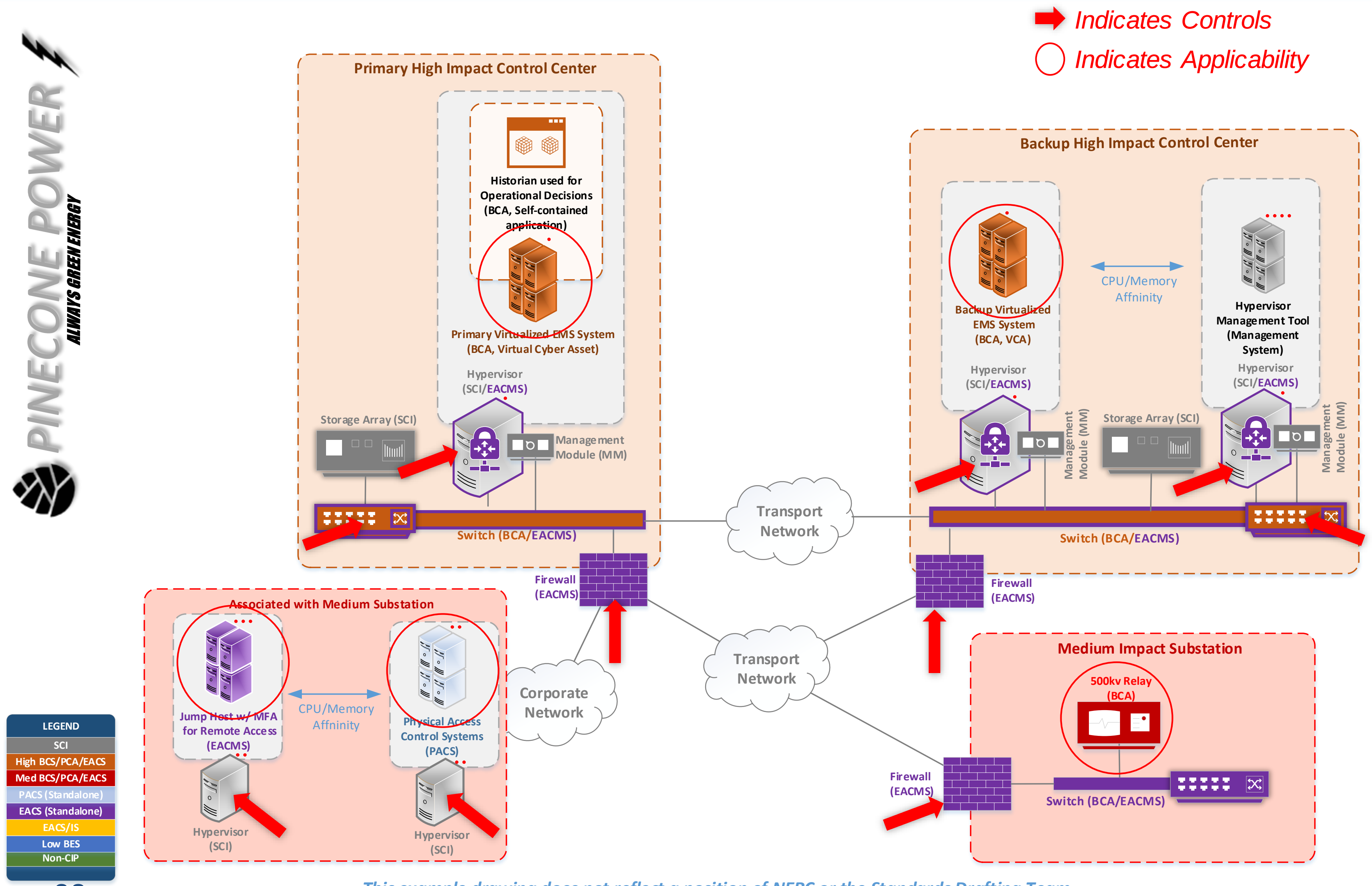
Implemented Controls – Option 2

1.1 implemented at Firewalls and switches;
1.1 implemented on Hypervisor for PACS/EACMS

CIP-005 R1 Part 1.1 – Zero Trust Model

slido.com
#2016-02

Workshop Sample Infrastructure – Zero Trust Model (CIP-002 Evaluation Already Completed)



➡ *Indicates Controls*

○ *Indicates Applicability*

PINECONE POWER
ALWAYS GREEN ENERGY

Primary High Impact Control Center

Historian used for Operational Decisions (BCA, Self-contained application)

Primary Virtualized EMS System (BCA, Virtual Cyber Asset)

Hypervisor (SCI/EACMS)

Storage Array (SCI)

Management Module (MM)

Switch (BCA/EACMS)

Firewall (EACMS)

Transport Network

Backup High Impact Control Center

Backup Virtualized EMS System (BCA, VCA)

CPU/Memory Affinity

Hypervisor Management Tool (Management System)

Hypervisor (SCI/EACMS)

Hypervisor (SCI/EACMS)

Management Module (MM)

Storage Array (SCI)

Management Module (MM)

Switch (BCA/EACMS)

Firewall (EACMS)

Associated with Medium Substation

Jump Host w/ MFA for Remote Access (EACMS)

CPU/Memory Affinity

Physical Access Control Systems (PACS)

Hypervisor (SCI)

Hypervisor (SCI)

Corporate Network

Transport Network

Medium Impact Substation

500kv Relay (BCA)

Firewall (EACMS)

Switch (BCA/EACMS)

LEGEND
SCI
High BCS/PCA/EACS
Med BCS/PCA/EACS
PACS (Standalone)
EACS (Standalone)
EACS/IS
Low BES
Non-CIP

This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R1 Part 1.1

Permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Implemented Controls – Option 2

1.1 Implemented by policy at Firewalls, Switches, and Hypervisors;
1.1 implemented on Hypervisor for PACS/EACMS

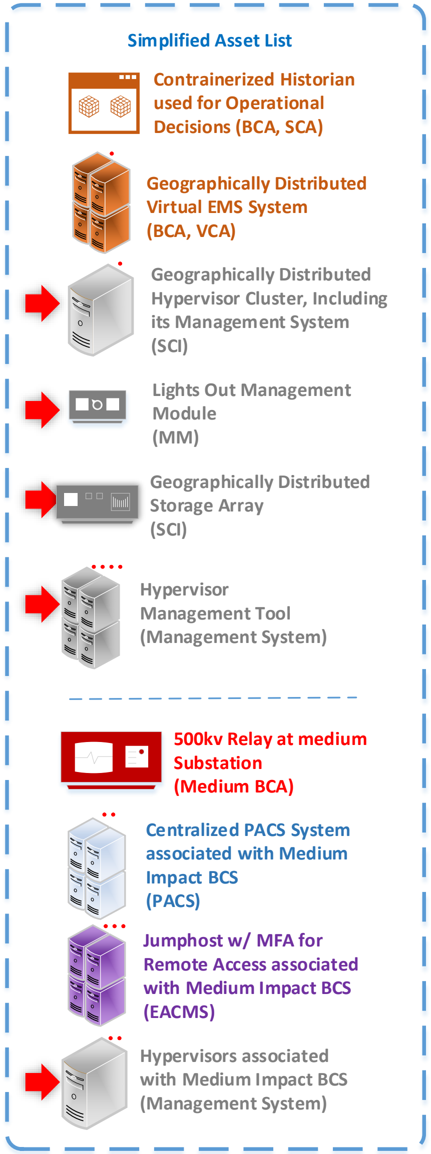
Q&A Response

Join at
slido.com
#2016-02

RELIABILITY | RESILIENCE | SECURITY

Proposed CIP-005 R1 Part 1.2

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

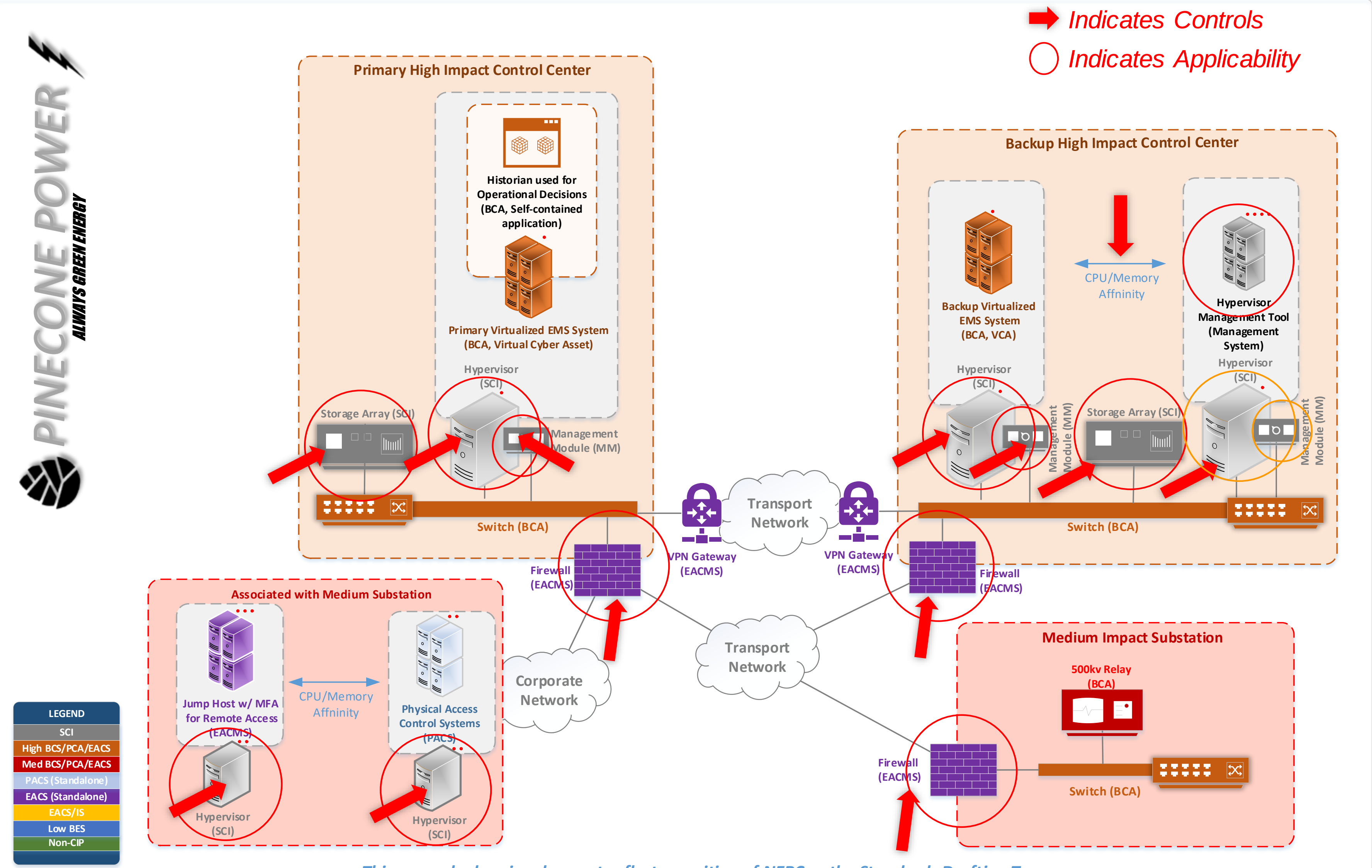
CIP-005-7 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. EACMS that perform logical isolation for a High impact BES Cyber System. EACMS that perform logical isolation for a Medium impact BES Cyber System.	**1.2.1.** Management Systems may only share CPU and memory with other Management Systems and its associated SCI, per system capability. **1.2.2.** Have one or more methods for permitting only needed and controlled communications to and from its Management Interfaces and Management Systems, logically isolating all other communications. **1.2.3.** Deny communications from BES Cyber Systems and their associated PCAs to the Management Interfaces and Management Systems, per system capability.	Examples of evidence may include, but is not limited to, documentation that includes the configuration of systems that enforce access control and logical isolation such as: • Logically isolated out-of-band network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment) • Physically isolated out-of-band network for dedicated Management Interfaces, Management Modules, or Management Systems • SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-005 R1 Part 1.2 – Perimeter Model

slido.com #2016-02

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R1 Part 1.2

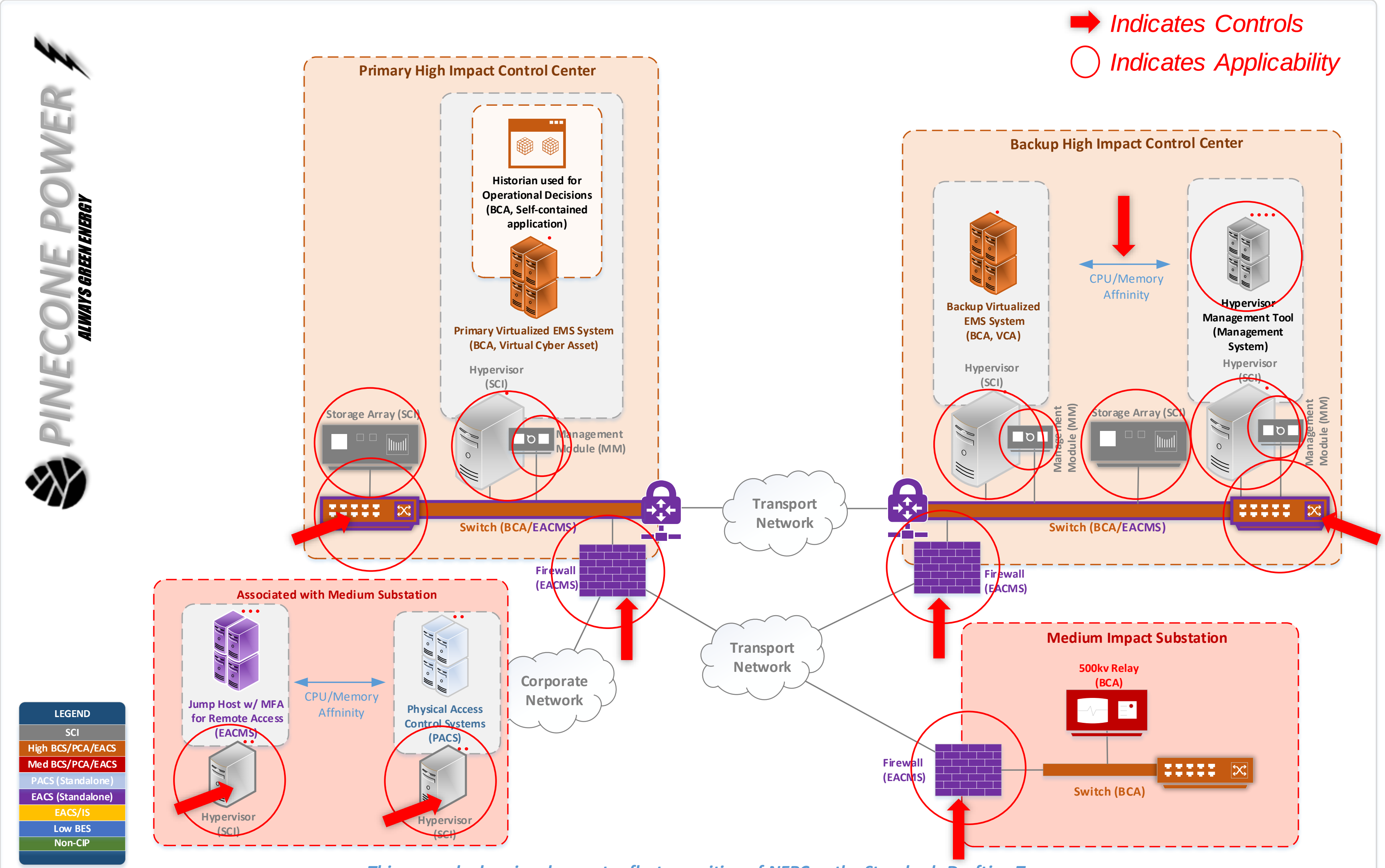
1.2.1. Management Systems may only share CPU and memory with other Management Systems and its associated SCI, per system capability.
1.2.2. Have one or more methods for permitting only needed and controlled communications to and from its Management Interfaces and Management Systems, logically isolating all other communications.
1.2.3. Deny communications from BES Cyber Systems and their associated PCAs to the Management Interfaces and Management Systems, per system capability.

Option 1

1.2.1 CPU/Memory Affinity Rule at Hypervisor
1.2.2 ACL implemented at each device
1.2.3 ACL implemented at each device

CIP-005 R1 Part 1.2 – VLAN Model

Workshop Sample Infrastructure – VLAN Model (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R1 Part 1.2

1.2.1. Management Systems may only share CPU and memory with other Management Systems and its associated SCI, per system capability.

1.2.2. Have one or more methods for permitting only needed and controlled communications to and from its Management Interfaces and Management Systems, logically isolating all other communications.

1.2.3. Deny communications from BES Cyber Systems and their associated PCAs to the Management Interfaces and Management Systems, per system capability.

Option 2

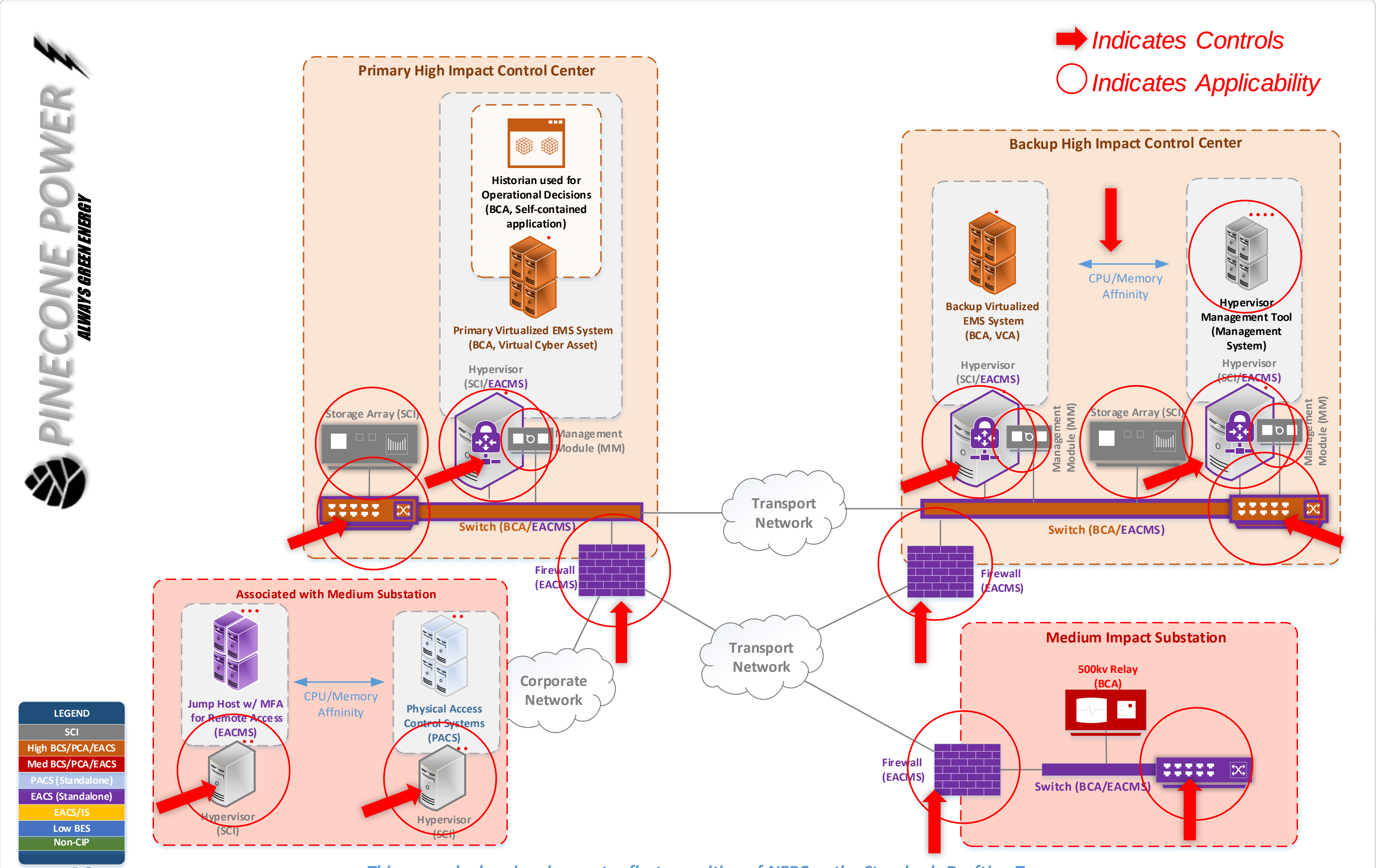
1.2.1 CPU/Memory Affinity Rule at Hypervisor

1.2.2 VLANs Implemented at the Switch; ACL on the Corporate Hypervisor

1.2.3 VLANs Implemented at the Switch

CIP-005 R1 Part 1.2 – Zero Trust Model

Workshop Sample Infrastructure – Zero Trust Model (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R1 Part 1.2

1.2.1. Management Systems may only share CPU and memory with other Management Systems and its associated SCI, per system capability.
1.2.2. Have one or more methods for permitting only needed and controlled communications to and from its Management Interfaces and Management Systems, logically isolating all other communications.
1.2.3. Deny communications from BES Cyber Systems and their associated PCAs to the Management Interfaces and Management Systems, per system capability.

Option 2

1.2.1 CPU/Memory Affinity Rule at Hypervisor
1.2.2 VLANs Implemented at the Switch; ACL on the Corporate Hypervisor
1.2.3 VLANs Implemented at the Switch

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

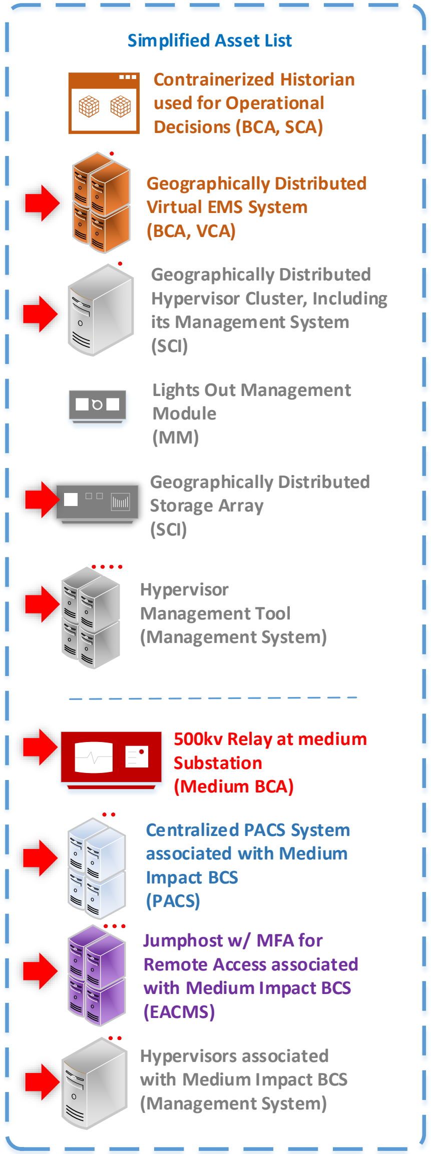
Q&A Response

Join at
slido.com
#2016-02

RELIABILITY | RESILIENCE | SECURITY

Proposed CIP-005 R1 Part 1.3

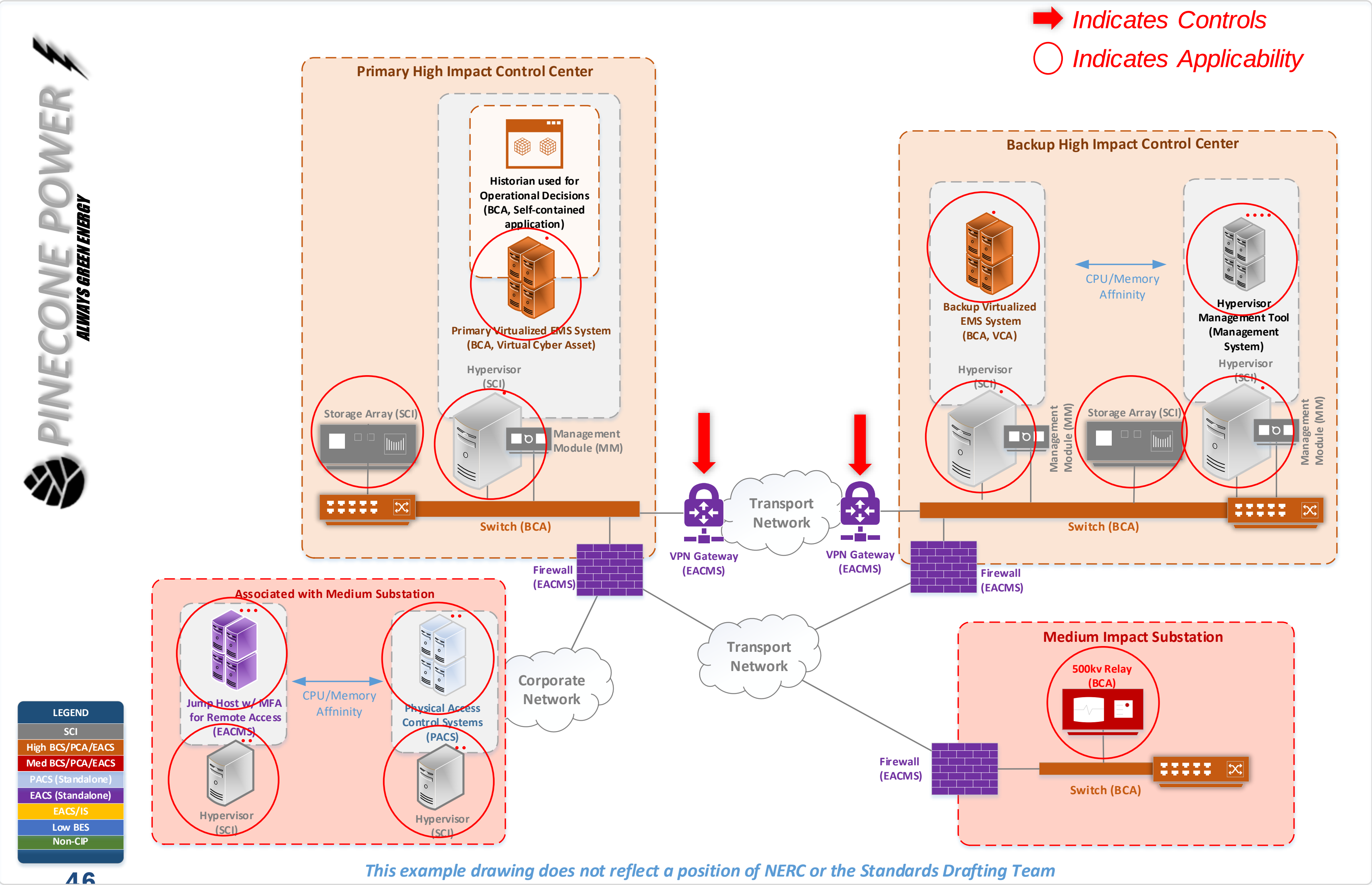
slido.com
#2016-02


Simplified Asset List
Contrainerized Historian used for Operational Decisions (BCA, SCA)
Geographically Distributed Virtual EMS System (BCA, VCA)
Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)
Lights Out Management Module (MM)
Geographically Distributed Storage Array (SCI)
Hypervisor Management Tool (Management System)
500kv Relay at medium Substation (Medium BCA)
Centralized PACS System associated with Medium Impact BCS (PACS)
Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
Hypervisors associated with Medium Impact BCS (Management System)

Part	Applicable Systems	Requirements	Measures
1.~~3~~3	High Impact BES Cyber Systems and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI Medium Impact BES Cyber Systems connected to a network via routable protocol and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI SCI connected to a network via routable protocol hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	Protect the confidentiality and integrity of the data traversing communication ~~networks~~links~~ and data communication ~~t~~links used to enable the communication~~hat -span multiple ~~between~~geographical locations, where methods from Part 1.1 or Part 1.2.2 -are not applied~~ the components of a BES Cyber System located at multiple geographic locations~~, excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	Evidence may include, but is not limited to, architecture documents detailing the methods used to ~~mitigate the risk of unauthorized disclosure~~protect the confidentiality and integrity of the data. ~~Examples include physical protection and the points where encryption initiates and terminates~~(e.g., encryption)~~.~~

CIP-005 R1 Part 1.3 – Perimeter Model

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R1 Part 1.3

Protect the confidentiality and integrity of the data traversing communication links that span multiple geographical locations, where methods from Part 1.1 or Part 1.2.2 are not applied, excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

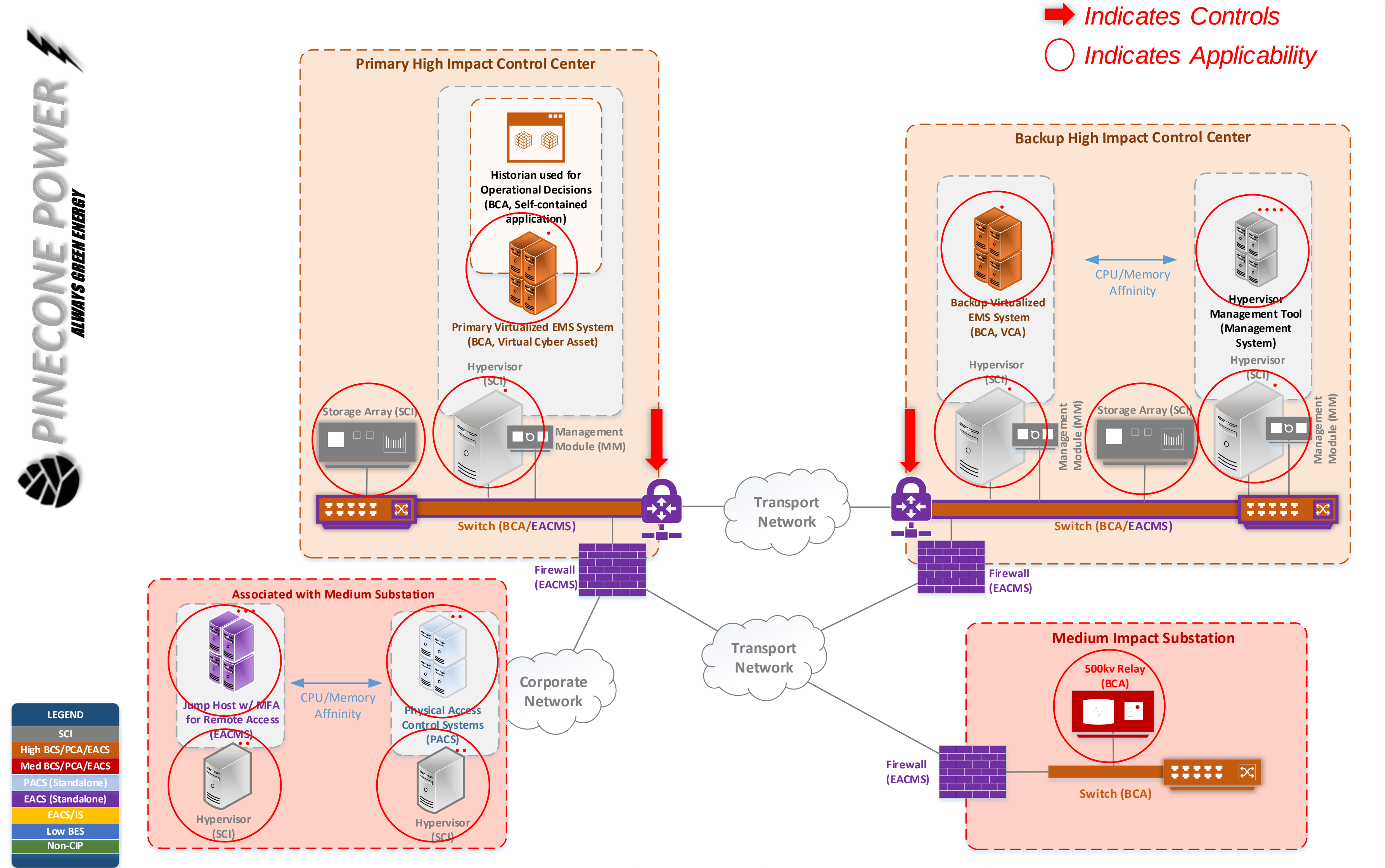
Implemented Protection

- **Part 1.1 and 1.2.2 Firewalls controlling communications; Hypervisor Controlling on behalf of EACMS and PACS**
- **Encryption via VPN gateway protecting integrity and confidentiality between Primary and Backup**

CIP-005 R1 Part 1.3 – VLAN Model

slido.com
#2016-02

Workshop Sample Infrastructure – VLAN Model (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R1 Part 1.3

Protect the confidentiality and integrity of the data traversing communication links that span multiple geographical locations, where methods from Part 1.1 or Part 1.2.2 are not applied, excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Implemented Protection

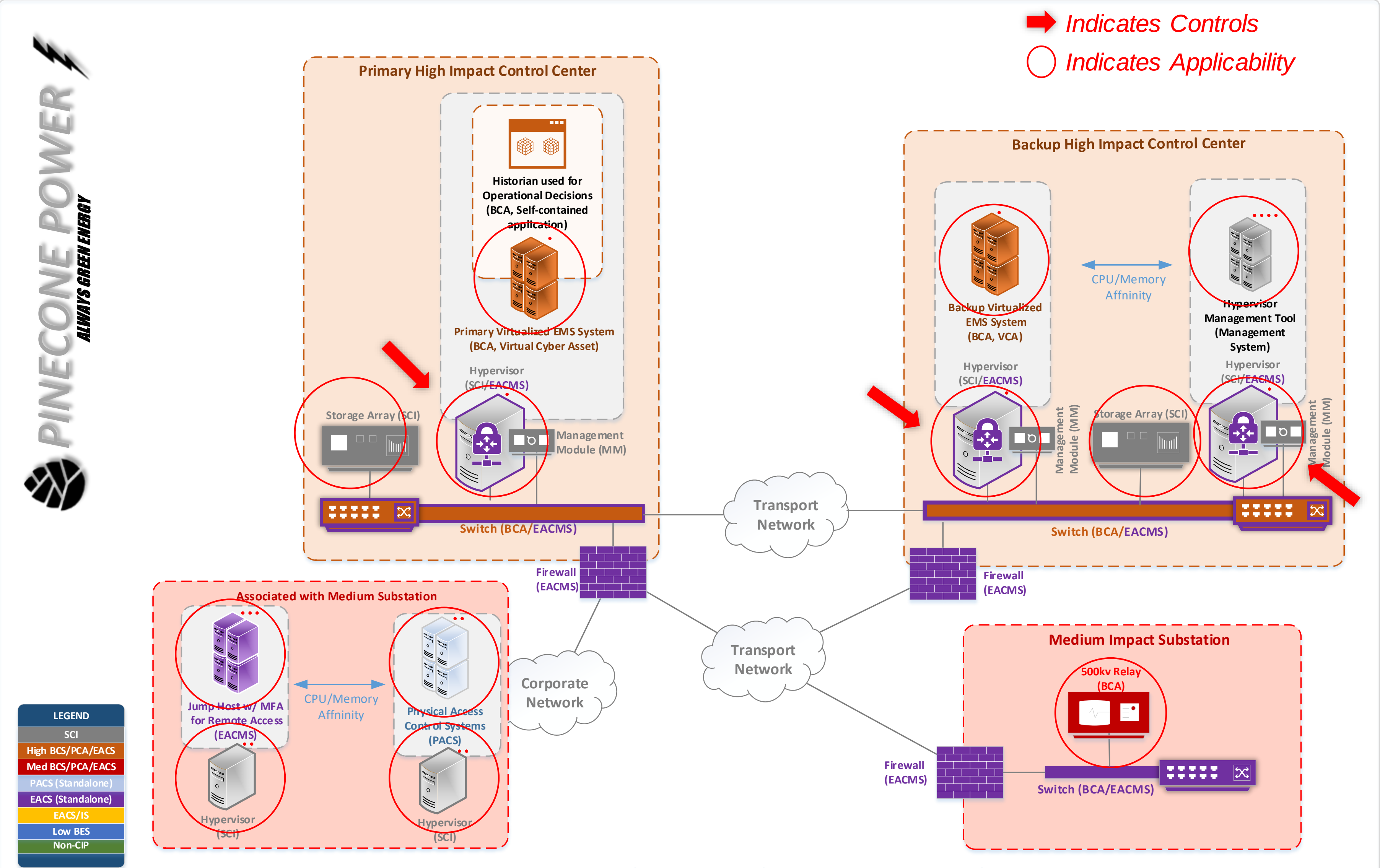
- **Part 1.1 and 1.2.2 Firewalls controlling communications; Hypervisor Controlling on behalf of EACMS and PACS**
- **Encryption via VPN gateway protecting integrity and confidentiality between Primary and Backup**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-005 R1 Part 1.3 – Zero Trust Model

slido.com
#2016-02

Workshop Sample Infrastructure – Zero Trust Model (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R1 Part 1.3

Protect the confidentiality and integrity of the data traversing communication links that span multiple geographical locations, where methods from Part 1.1 or Part 1.2.2 are not applied, excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Implemented Protection

- **Part 1.1 and 1.2.2 Firewalls controlling communications; Hypervisor Controlling on behalf of EACMS and PACS**
- **Encryption via VPN gateway protecting integrity and confidentiality between Primary and Backup**

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

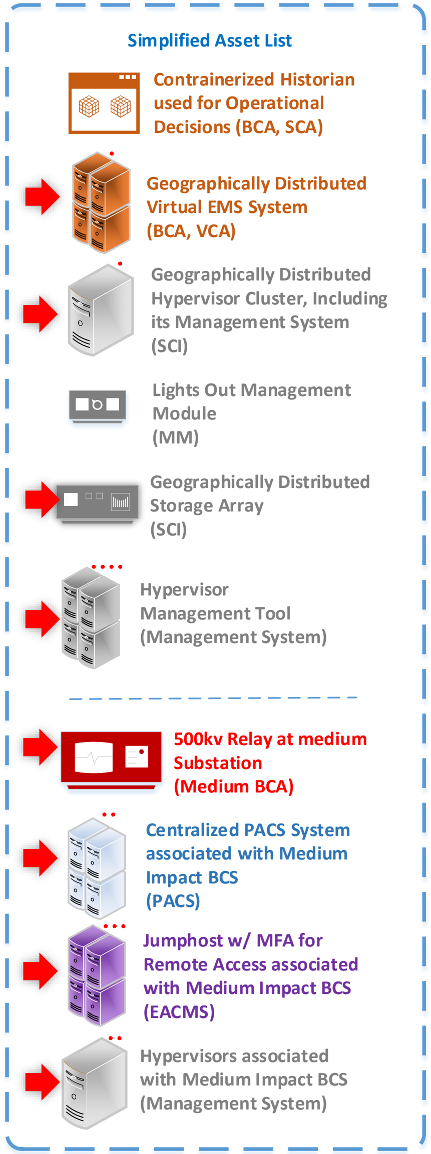
Q&A Response

Join at
slido.com
#2016-02

RELIABILITY | RESILIENCE | SECURITY

Proposed CIP-005 R1 Part 1.4

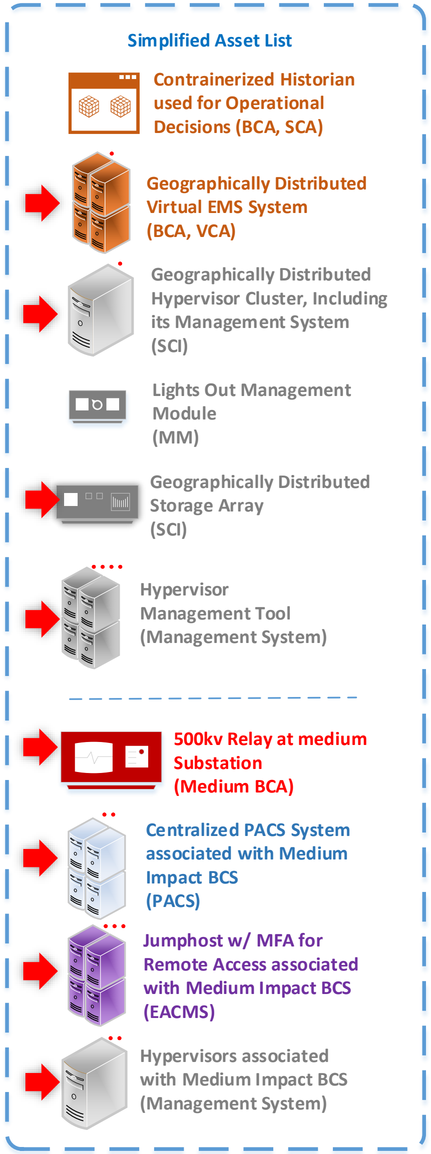
slido.com
#2016-02


Simplified Asset List
Contrainerized Historian used for Operational Decisions (BCA, SCA)
Geographically Distributed Virtual EMS System (BCA, VCA)
Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)
Lights Out Management Module (MM)
Geographically Distributed Storage Array (SCI)
Hypervisor Management Tool (Management System)
500kv Relay at medium Substation (Medium BCA)
Centralized PACS System associated with Medium Impact BCS (PACS)
Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
Hypervisors associated with Medium Impact BCS (Management System)

1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: - PCA - PACS hosted om SCI - EACMS hosted on SCI Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: - PCA - PACS hosted on SCI - EACMS hosted on SCI SCI with dial-up hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	~~Where technically feasible,~~ ~~p~~Perform authentication when establishing Dial-up Connectivity with applicable ~~Cyber Assets~~ systems, per system capability.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

Proposed CIP-005 R1 Part 1.5

slido.com
#2016-02


Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

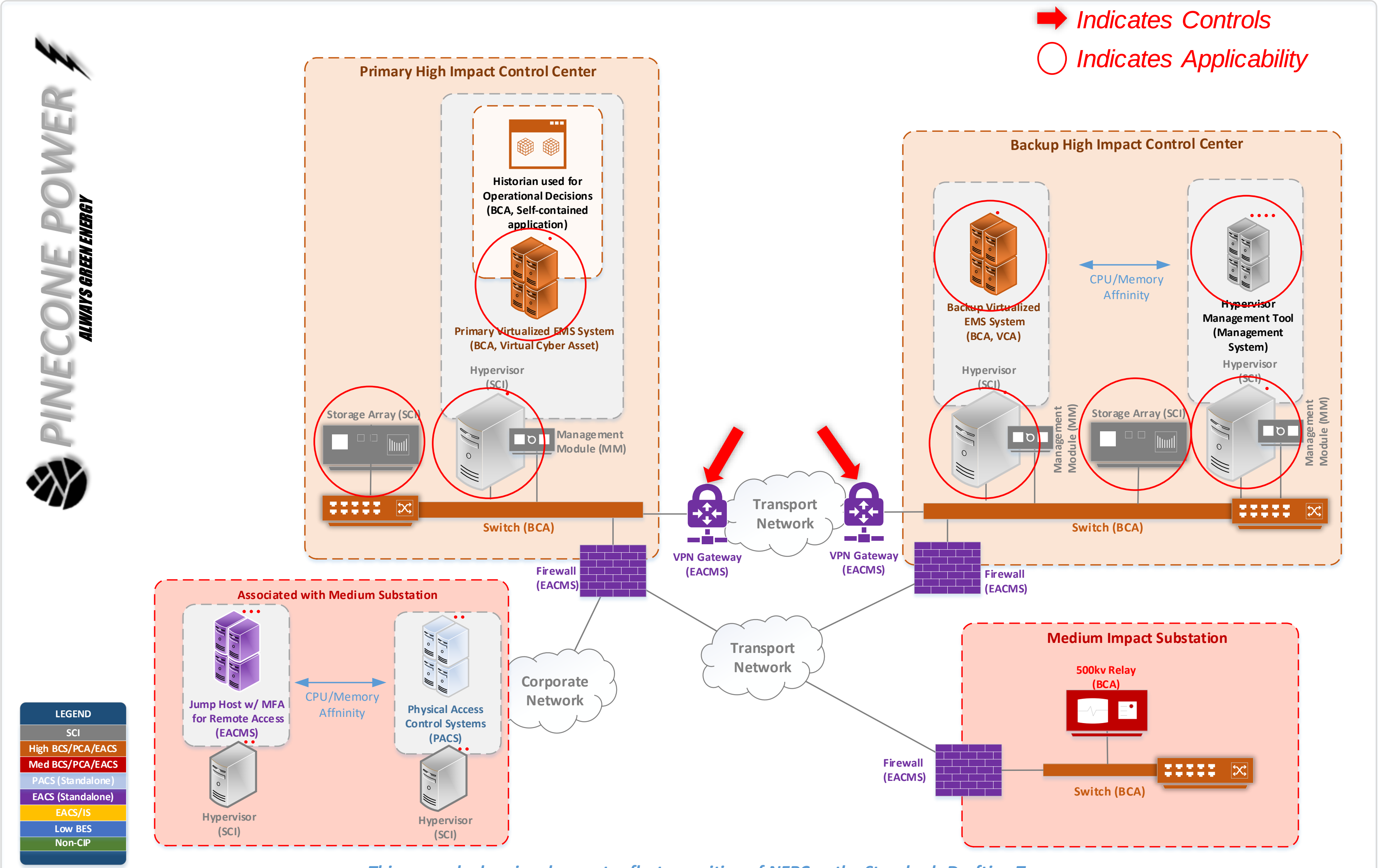
Hypervisors associated with Medium Impact BCS (Management System)

1.5	~~Electronic Access Points for~~ High Impact BES Cyber Systems and their associated: ● PCA ● PACS hosted on SCI ● EACMS hosted on SCI Medium Impact BES Cyber Systems at Control Centers and their associated: ● PCA ● PACS hosted on SCI ● EACMS hosted on SCI SCI at Control Centers hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. ~~Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers~~	Have one or more methods for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving the isolation required by Part 1.1 or Part 1.2.2. ~~for both inbound and outbound communications.~~	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

CIP-005 R1 Part 1.5

slido.com
#2016-02

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R1 Part 1.5

Have one or more methods for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving the isolation required by Part 1.1 or Part 1.2.2.

Implemented Protection – Option 1

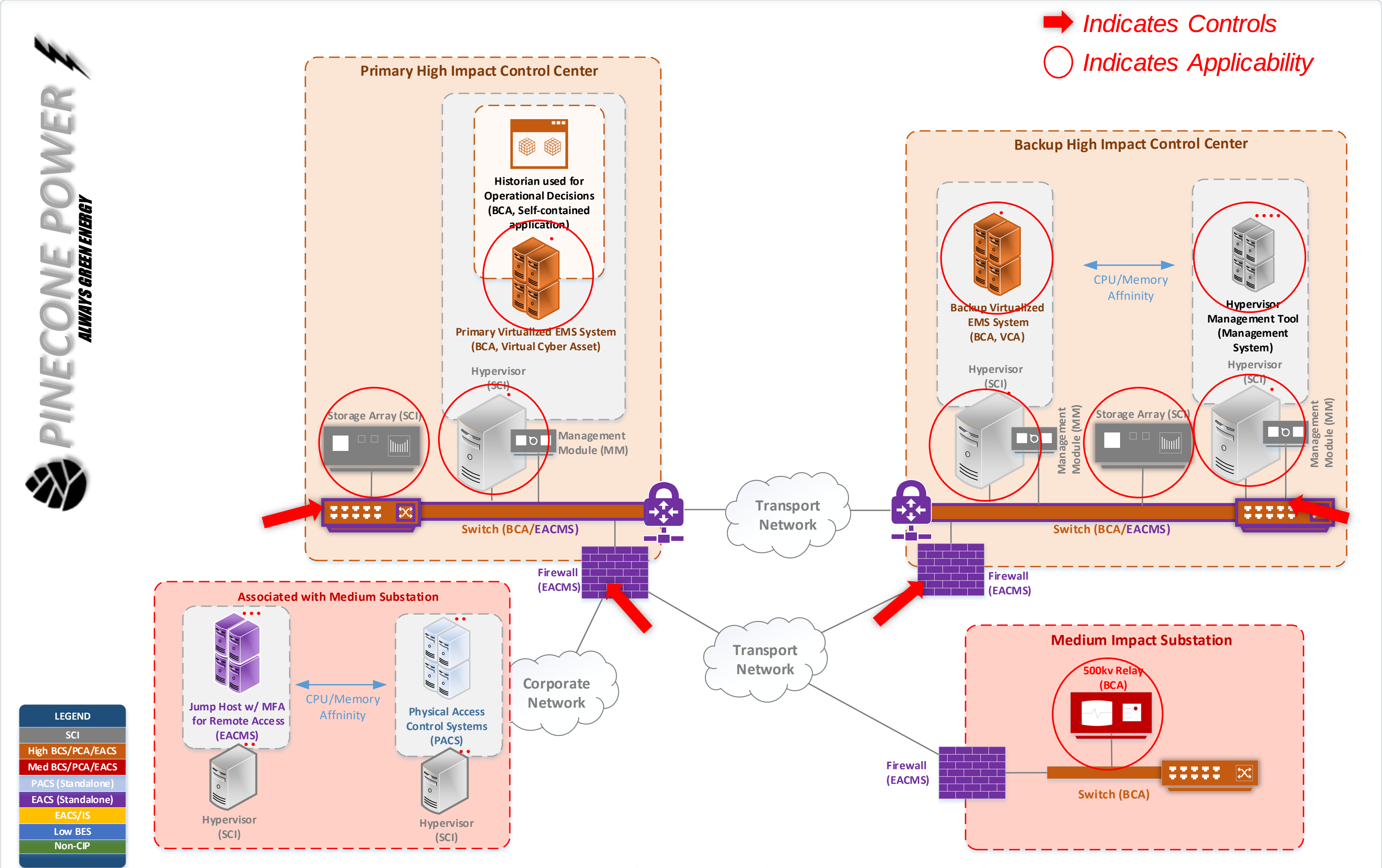
- Passive IDS Taps Implemented at points where inbound and outbound communications are controlled

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-005 R1 Part 1.5

slido.com
#2016-02

Workshop Sample Infrastructure – VLAN Model (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R1 Part 1.5

Have one or more methods for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving the isolation required by Part 1.1 or Part 1.2.2.

Implemented Protection – Option 1

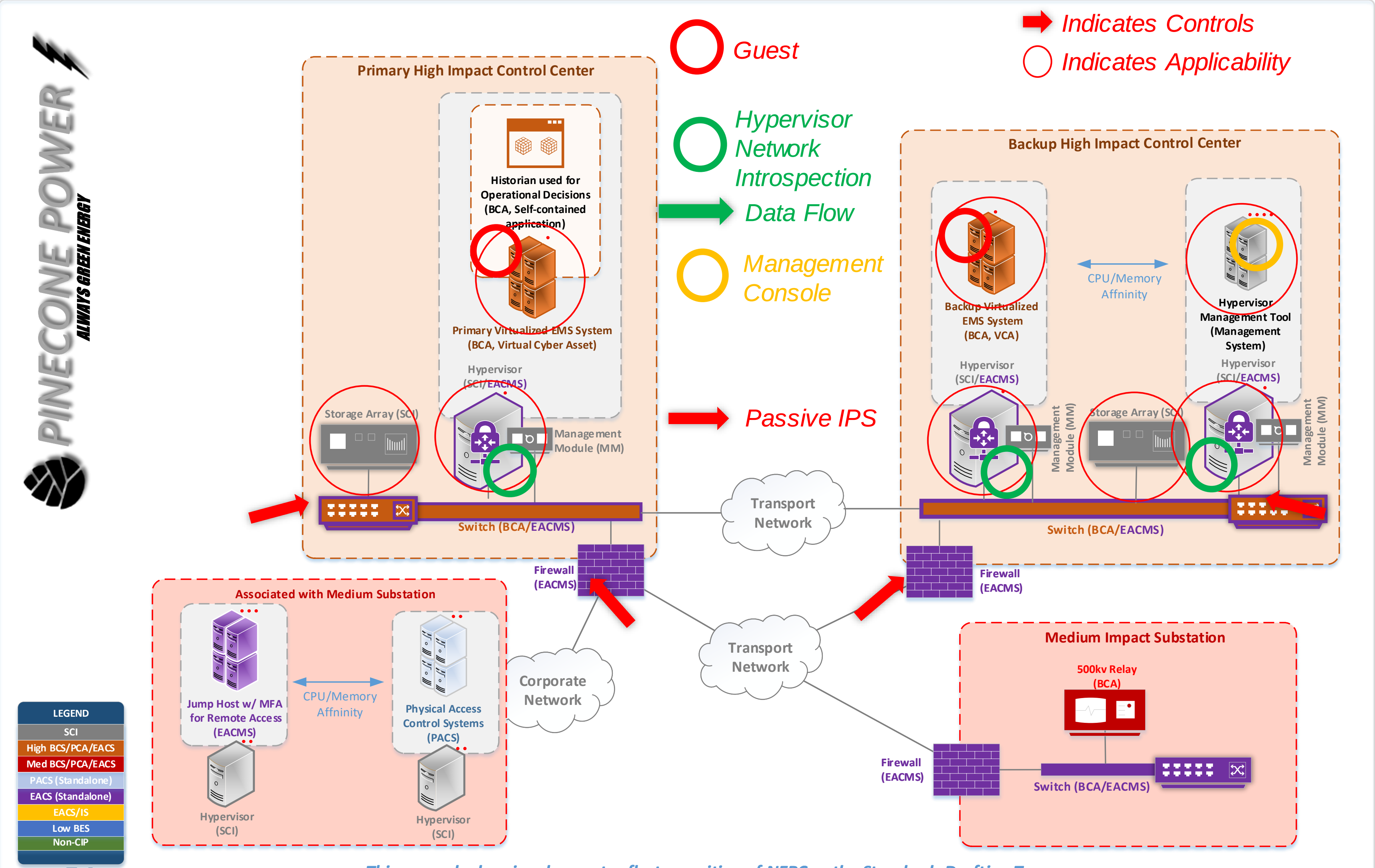
- Passive IDS Taps Implemented at points where inbound and outbound communications are controlled

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-005 R1 Part 1.5 – Zero Trust

slido.com
#2016-02

Workshop Sample Infrastructure – Zero Trust Model (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R1 Part 1.5

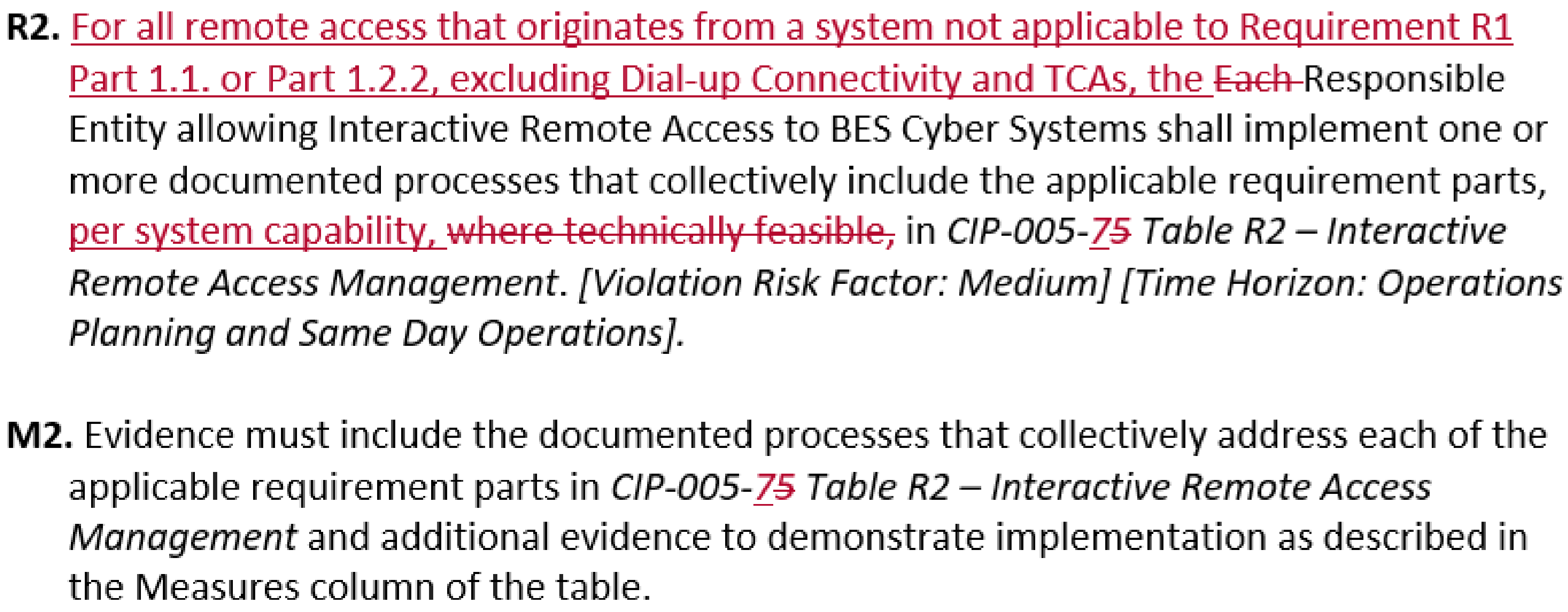
Have one or more methods for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving the isolation required by Part 1.1 or Part 1.2.2.

Implemented Protection – Option 2

- Passive IPS Taps and Network Introspection implemented at points where inbound and outbound communications are controlled

Proposed CIP-005 Requirement R2

slido.com
#2016-02



R2. For all remote access that originates from a system not applicable to Requirement R1 Part 1.1. or Part 1.2.2, excluding Dial-up Connectivity and TCAs, the ~~Each~~ Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, ~~where technically feasible,~~ in *CIP-005-7~~5~~ Table R2 – Interactive Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7~~5~~ Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Proposed CIP-005 R2 Part 2.1

Simplified Asset List

- Contrainerized Historian used for Operational Decisions (BCA, SCA)
- Geographically Distributed Virtual EMS System (BCA, VCA)
- Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)
- Lights Out Management Module (MM)
- Geographically Distributed Storage Array (SCI)
- Hypervisor Management Tool (Management System)

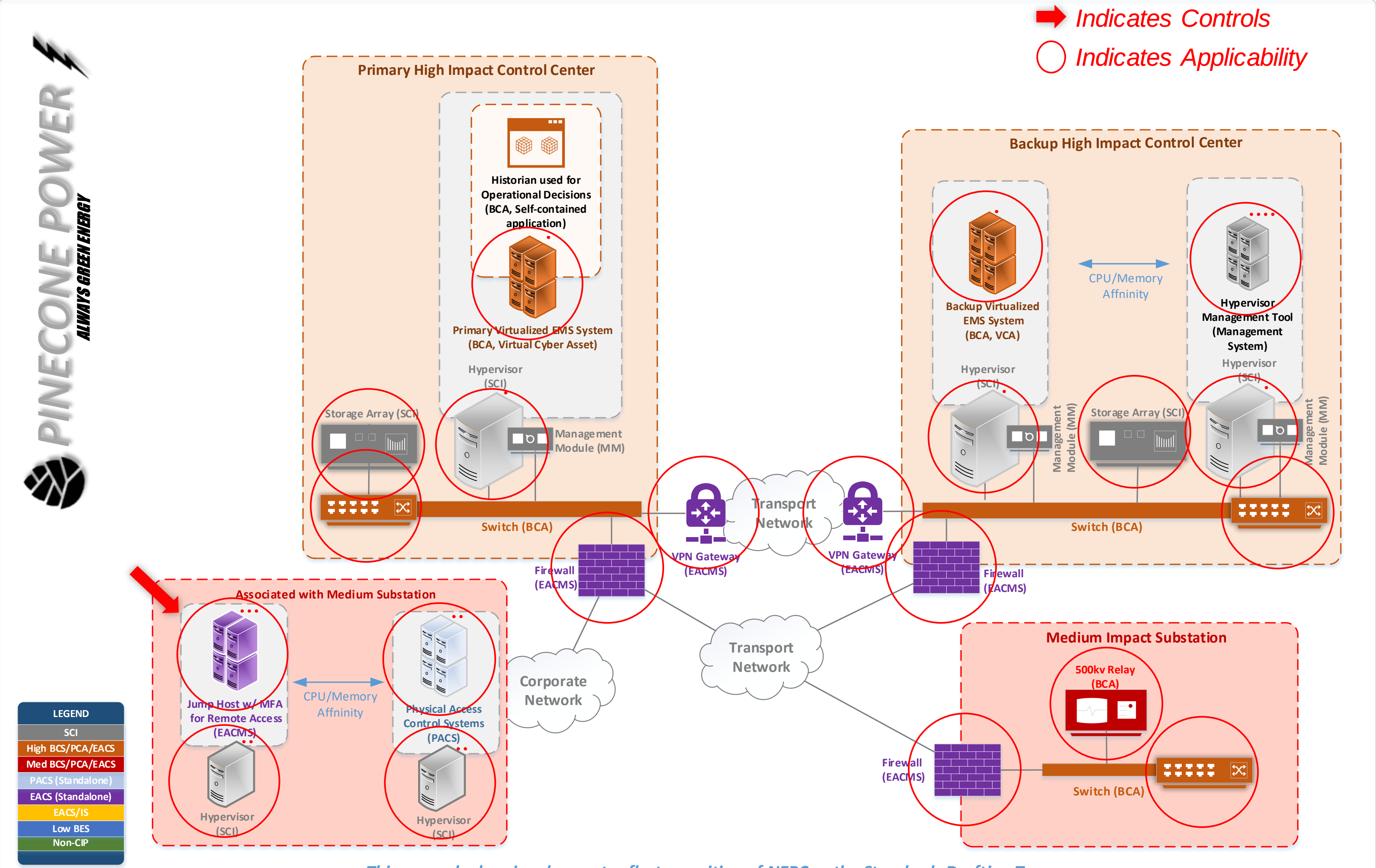
- 500kv Relay at medium Substation (Medium BCA)
- Centralized PACS System associated with Medium Impact BCS (PACS)
- Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
- Hypervisors associated with Medium Impact BCS (Management System)

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated ~~:~~PCA. Medium Impact BES Cyber Systems with IRA ~~External Routable Connectivity~~ and their associated ~~:~~PCA. SCI with IRA hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules with IRA of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	~~For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating~~ Ensure that authorized Interactive Remote Access is through an Intermediate System. ~~does not directly access an applicable Cyber Asset.~~	Examples of evidence may include, but are not limited to, network diagrams~~, or~~ architecture documents, or Management Systems reports that show all IRA is through an IS.

CIP-005 R2 Part 2.1

slido.com
#2016-02

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R2 Part 2.1

Ensure that authorized Interactive Remote Access is through an Intermediate System.

Proposed CIP-005 R2 Part 2.2

Simplified Asset List

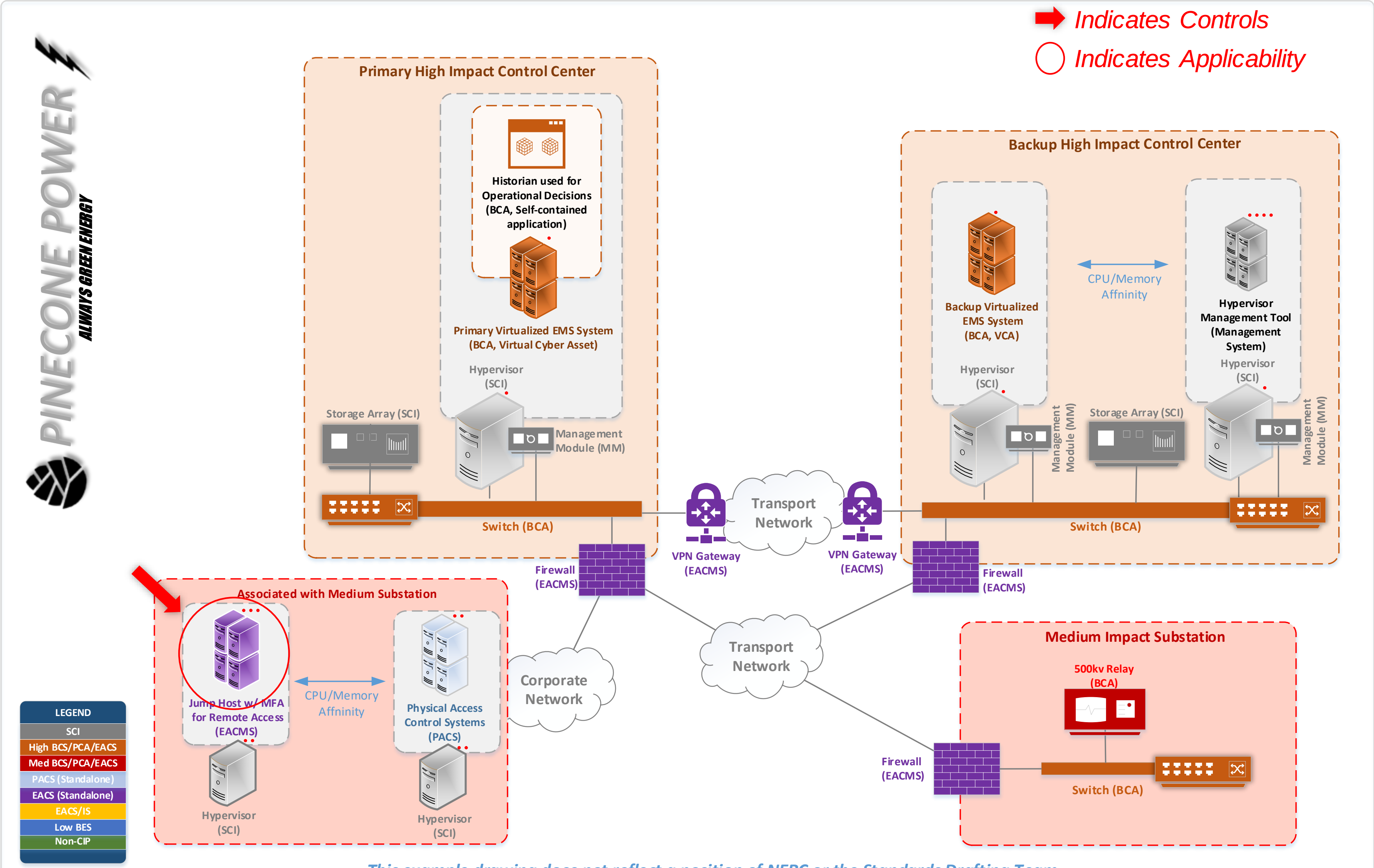
- Contrainerized Historian used for Operational Decisions (BCA, SCA)
- Geographically Distributed Virtual EMS System (BCA, VCA)
- Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)
- Lights Out Management Module (MM)
- Geographically Distributed Storage Array (SCI)
- Hypervisor Management Tool (Management System)

- 500kv Relay at medium Substation (Medium BCA)
- Centralized PACS System associated with Medium Impact BCS (PACS)
- Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
- Hypervisors associated with Medium Impact BCS (Management System)

2.2	Intermediate Systems used to access applicable systems of Part 2.1. ~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~• PCA~~	~~For all Interactive Remote Access sessions, utilize encryption that terminates at an~~ Protect the confidentiality and integrity of authorized Interactive Remote Access between the client and the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where ~~encryption~~ confidentiality and integrity controls initiates and terminates.

CIP-005 R2 Part 2.2

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



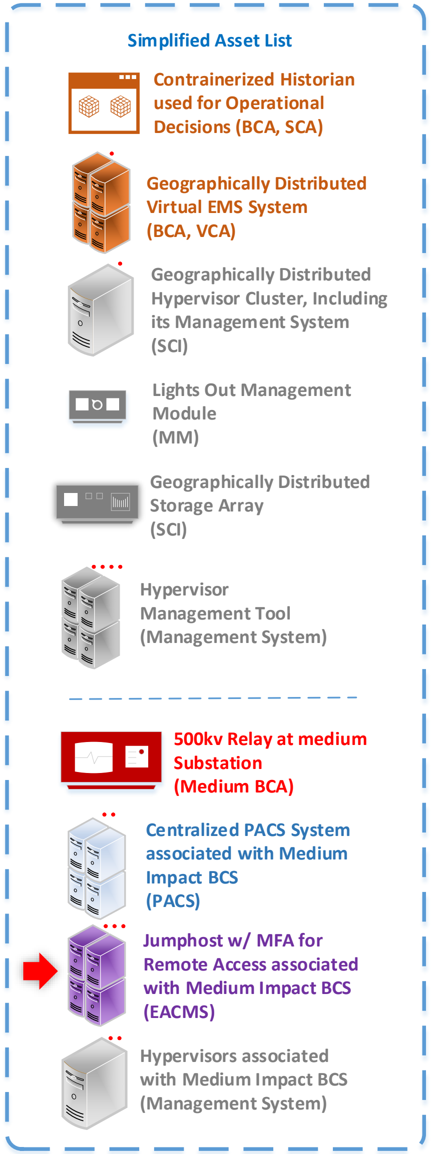
This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R2 Part 2.2

Protect the confidentiality and integrity of authorized Interactive Remote Access between the client and the Intermediate System.

Proposed CIP-005 R2 Part 2.3

slido.com
#2016-02


Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

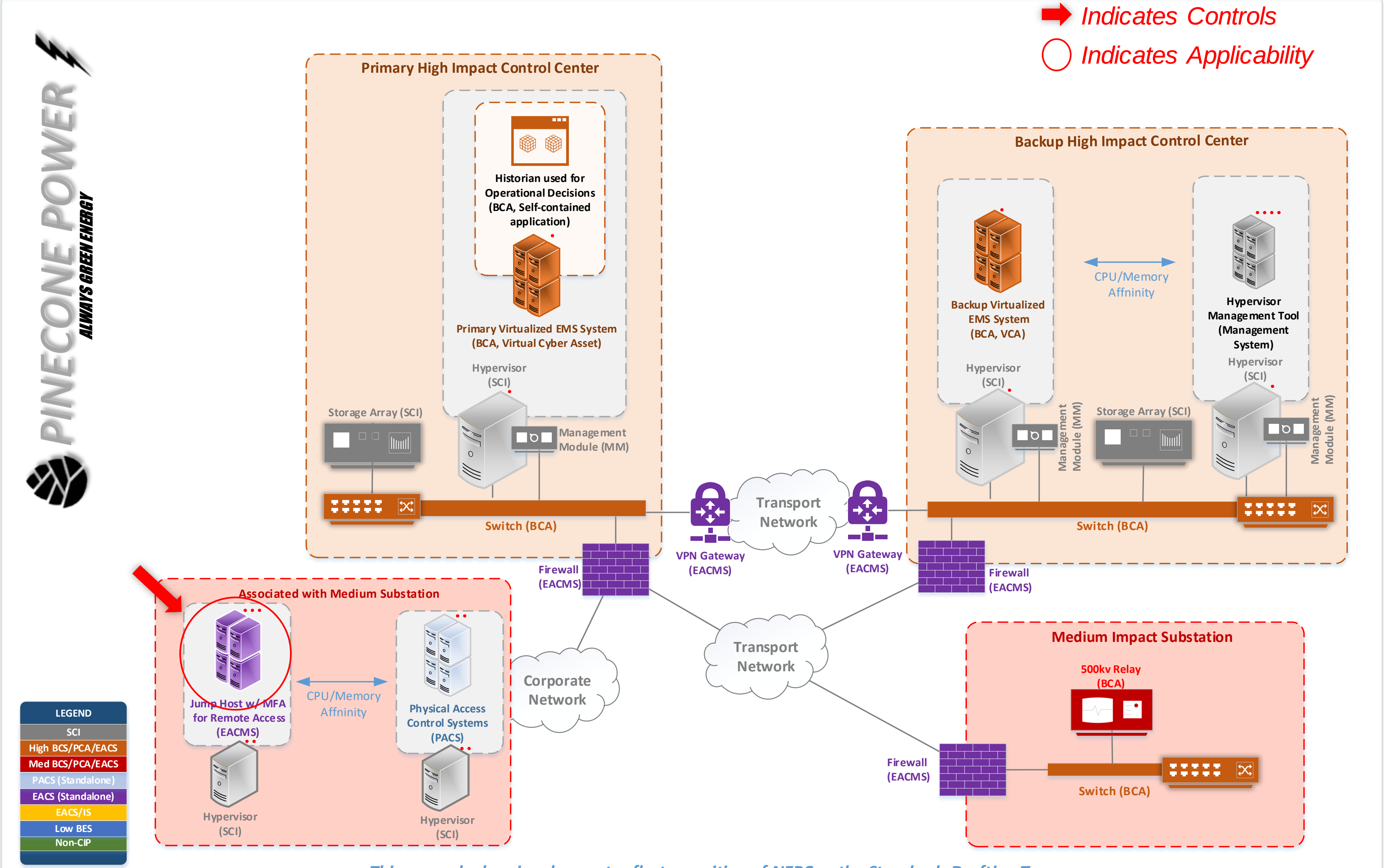
Hypervisors associated with Medium Impact BCS (Management System)

2.3	Intermediate Systems used to access applicable systems of Part 2.1. ~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~• PCA~~	Require multi-factor authentication ~~for all Interactive Remote Access sessions~~to the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005 R2 Part 2.3

slido.com
#2016-02

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)

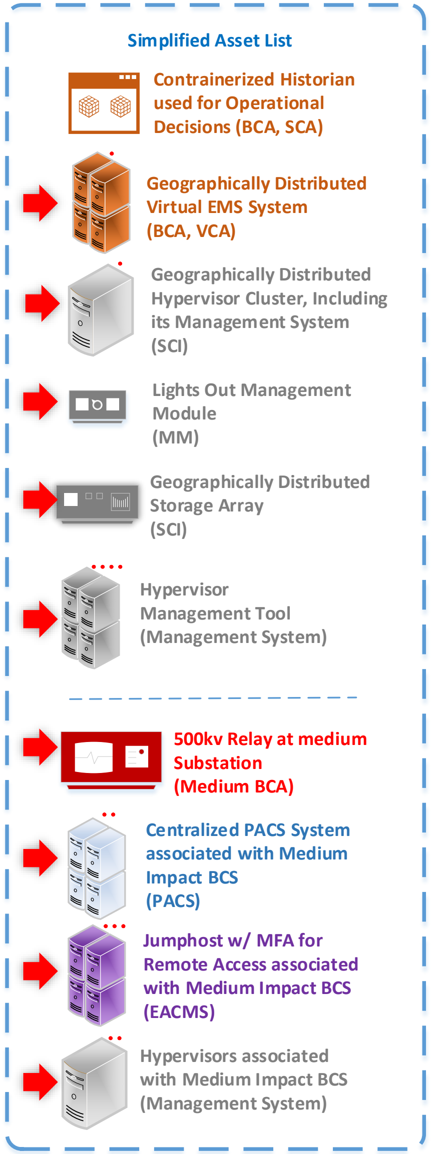


This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R2 Part 2.3

Require multi-factor authentication to the Intermediate System.

Proposed CIP-005 R2 Part 2.4



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

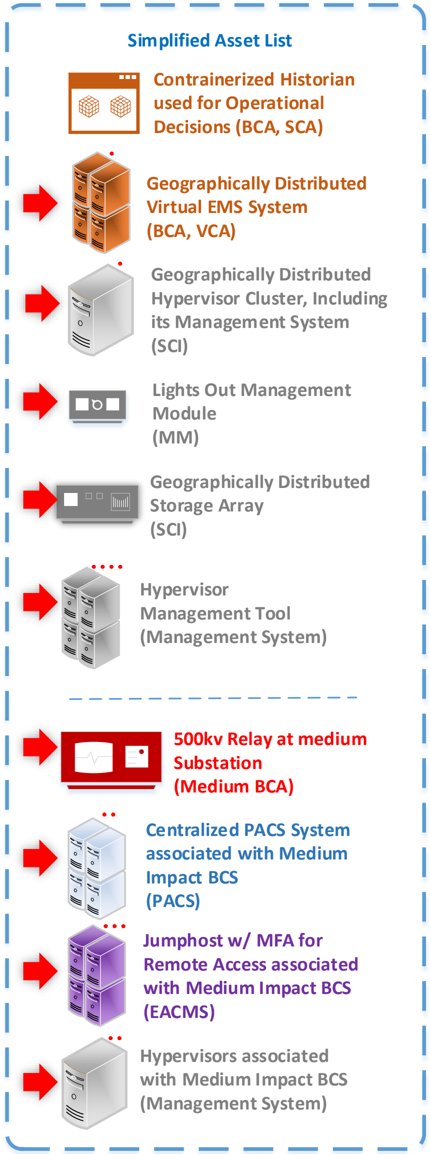
Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

2.4	High Impact BES Cyber Systems and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI • Medium Impact BES Cyber Systems ~~with External Routable Connectivity~~ and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

Proposed CIP-005 R2 Part 2.5

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

Part	Applicable Systems	Requirements	Measures
2.5	High Impact BES Cyber Systems and their associated: PCA • ~~SCI~~ • PACS hosted on SCI • EACMS hosted on SCI • Medium Impact BES Cyber Systems ~~with External Routable Connectivity~~ and their associated: PCA • ~~SCI~~ • PACS hosted on SCI • EACMS hosted on SCI SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. • Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).~~; such as:~~ • ~~Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or~~ • ~~Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.~~ •

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-005 R2 Part 2.5

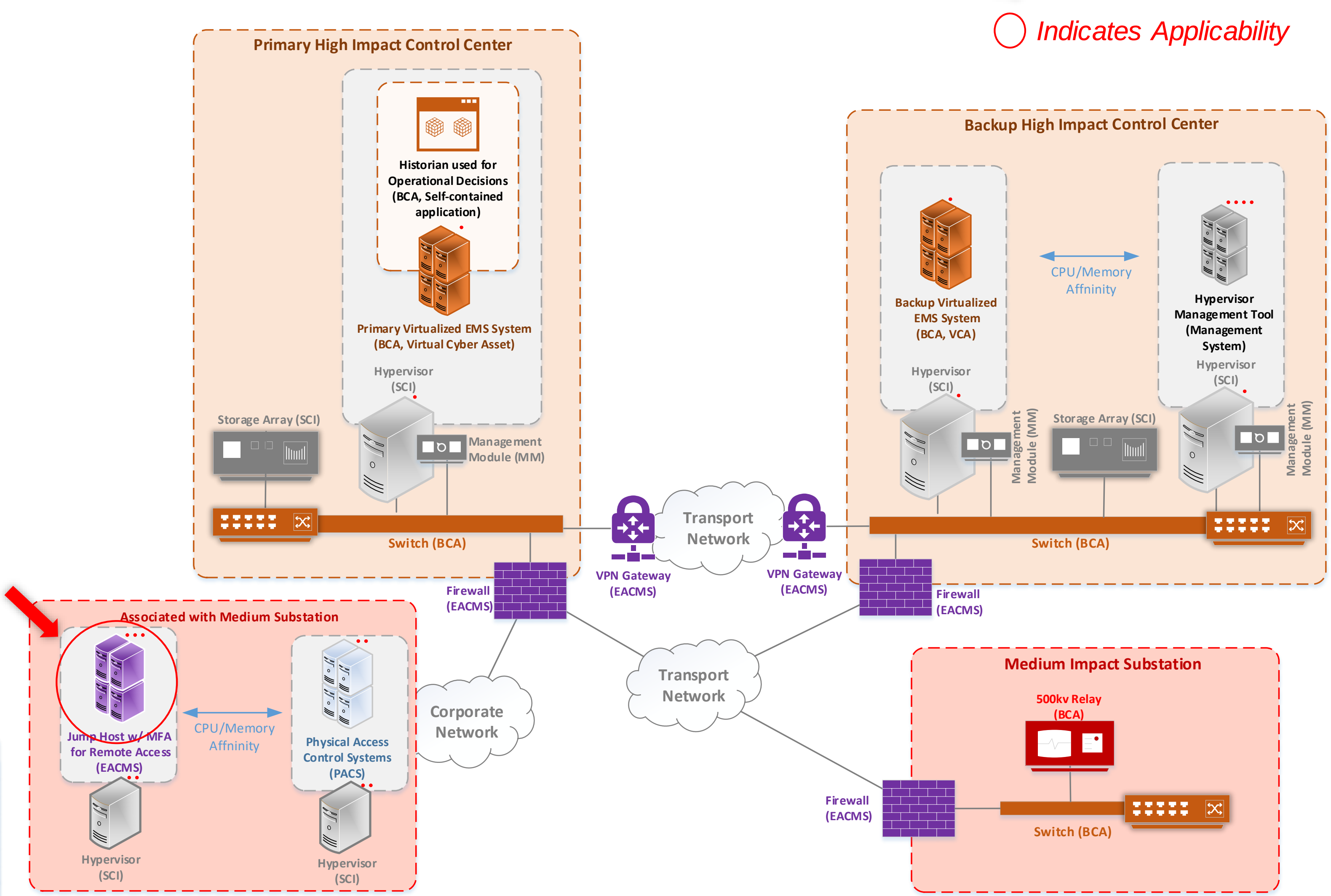
slido.com
#2016-02

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)

Indicates Controls

Indicates Applicability

PINECONE POWER
ALWAYS GREEN ENERGY


Primary High Impact Control Center
Historian used for Operational Decisions (BCA, Self-contained application)
Primary Virtualized EMS System (BCA, Virtual Cyber Asset)
Hypervisor (SCI)
Storage Array (SCI)
Management Module (MM)
Switch (BCA)
Firewall (EACMS)
VPN Gateway (EACMS)
Transport Network
VPN Gateway (EACMS)
Backup High Impact Control Center
Backup Virtualized EMS System (BCA, VCA)
CPU/Memory Affinity
Hypervisor Management Tool (Management System)
Hypervisor (SCI)
Hypervisor (SCI)
Management Module (MM)
Storage Array (SCI)
Management Module (MM)
Switch (BCA)
Firewall (EACMS)
Associated with Medium Substation
Jump Host w/ MFA for Remote Access (EACMS)
CPU/Memory Affinity
Physical Access Control Systems (PACS)
Hypervisor (SCI)
Hypervisor (SCI)
Corporate Network
Transport Network
Medium Impact Substation
500kv Relay (BCA)
Switch (BCA)
Firewall (EACMS)

LEGEND
SCI
High BCS/PCA/EACS
Med BCS/PCA/EACS
PACS (Standalone)
EACS (Standalone)
EACS/IS
Low BES
Non-CIP

This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R1 Part 2.5

Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).

Proposed CIP-005 R2 Part 2.6

slido.com
#2016-02

Simplified Asset List

- Contrainerized Historian used for Operational Decisions (BCA, SCA)
- Geographically Distributed Virtual EMS System (BCA, VCA)
- Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)
- Lights Out Management Module (MM)
- Geographically Distributed Storage Array (SCI)
- Hypervisor Management Tool (Management System)

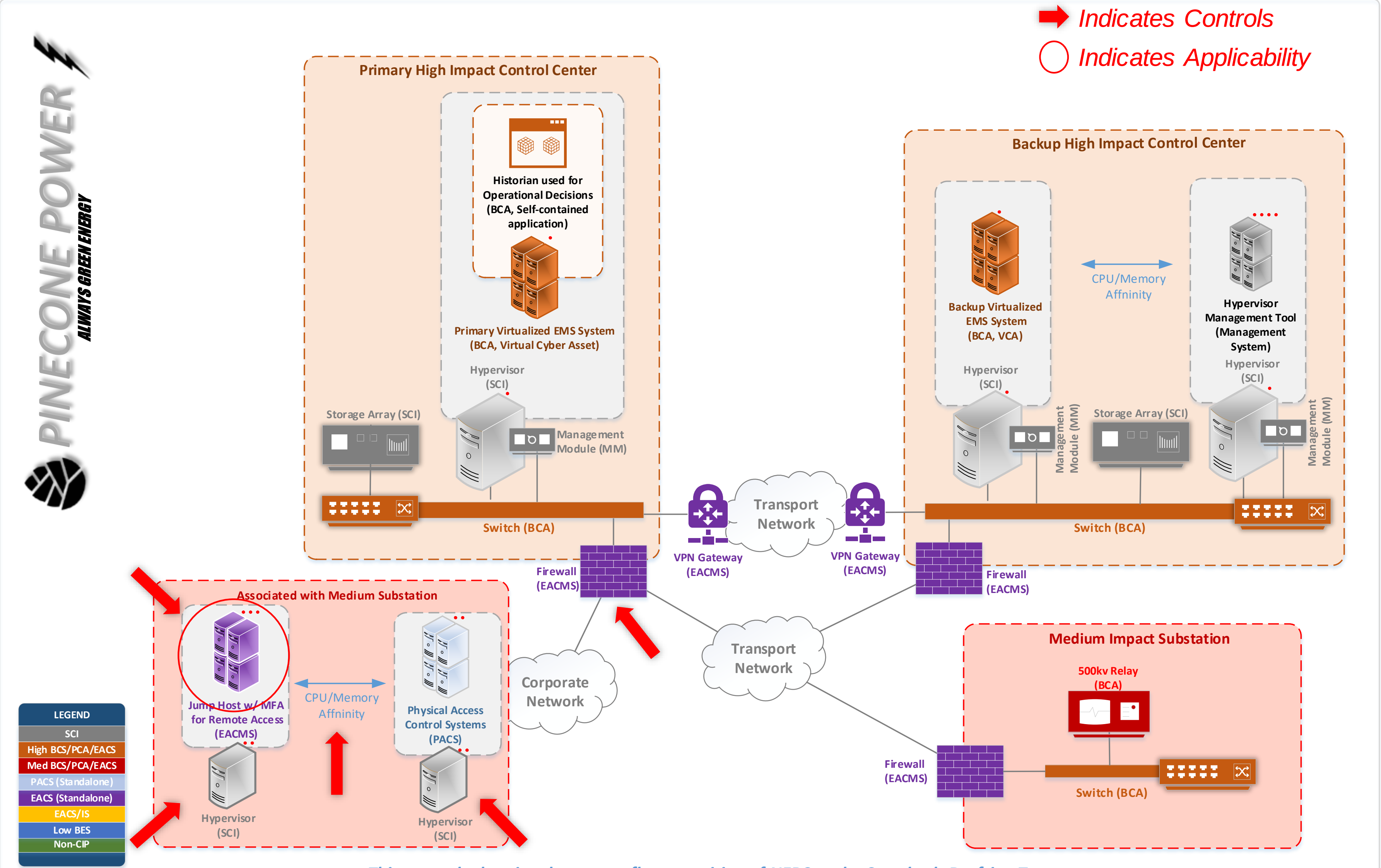
- 500kv Relay at medium Substation (Medium BCA)
- Centralized PACS System associated with Medium Impact BCS (PACS)
- ➡ Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
- Hypervisors associated with Medium Impact BCS (Management System)

CIP-005-6 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.6	Intermediate Systems used to access applicable systems of Part 2.1.	**2.6.1.** Intermediate Systems may only share CPU and memory with other Intermediate Systems and its associated SCI. **2.6.2.** Have one or more methods for permitting only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1.	An example of evidence may include, but is not limited to, documentation that includes the following: • Configuration showing that the CPU and memory can only be shared with other IS. • Configuration showing how communications are controlled between the IS and applicable systems.

CIP-005 R2 Part 2.6

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-005 R2 Part 2.6.1

Intermediate Systems may only share CPU and memory with other Intermediate Systems and its associated SCI.

CIP-005 R2 Part 2.6.2

Have one or more methods for permitting only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Q&A Response

Join at
slido.com
#2016-02

RELIABILITY | RESILIENCE | SECURITY

Break

We will return at X:XX p.m. Eastern

Join at

slido.com

#2016-02

RELIABILITY | RESILIENCE | SECURITY

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Q&A Response

Join at

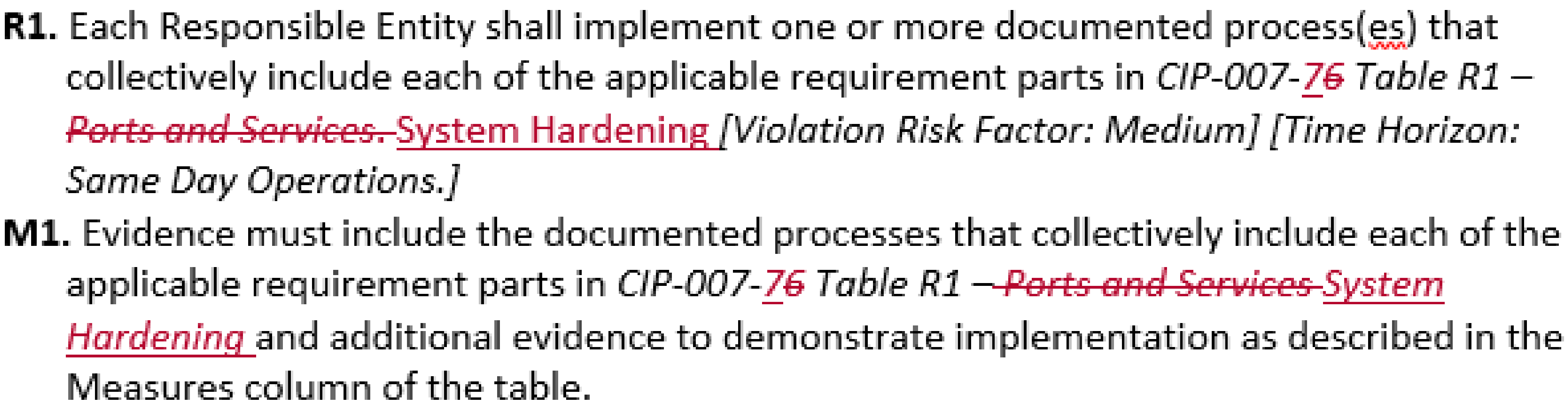
slido.com

#2016-02

RELIABILITY | RESILIENCE | SECURITY

CIP-007 Requirement R1

slido.com
#2016-02



R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R1 – ~~Ports and Services.~~ System Hardening [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R1 –~~Ports and Services~~ System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007 R1 Part 1.1

slido.com
#2016-02

Simplified Asset List

- Contrainerized Historian used for Operational Decisions (BCA, SCA)
- ➡ Geographically Distributed Virtual EMS System (BCA, VCA)
- Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)
- Lights Out Management Module (MM)
- Geographically Distributed Storage Array (SCI)
- Hypervisor Management Tool (Management System)

- ➡ 500kv Relay at medium Substation (Medium BCA)
- ➡ Centralized PACS System associated with Medium Impact BCS (PACS)
- ➡ Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
- Hypervisors associated with Medium Impact BCS (SCI)

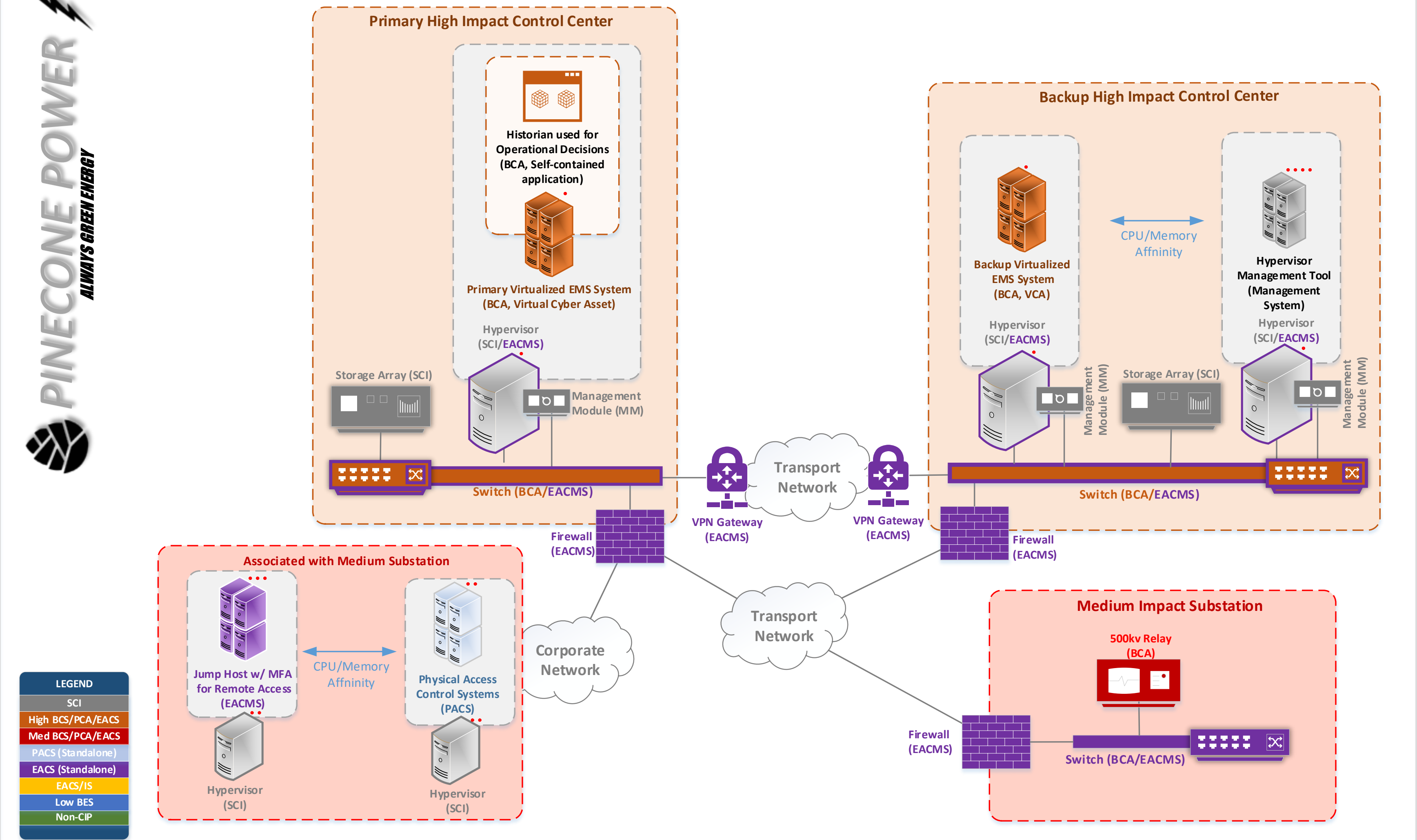
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	~~Where technically feasible, e~~Enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports, per system capability. If a ~~device~~ system has no provision for disabling or restricting logical ports ~~on the device~~ then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports ~~on all applicable Cyber Assets and Electronic Access Points,~~ individually or by group. • Listings of the listening ~~ports on the Cyber Assets,~~ individually or by group, from either ~~the device~~ configuration files, command output (such as netstat), or network scans of open ports; or • Configuration ~~files~~ of host-based firewalls, policy, or other ~~device level~~ mechanisms that only allow needed ports and deny all others.

CIP-007 R1 Part 1.1

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)

➡ *Indicates Controls*

○ *Indicates Applicability*



This example drawing does not reflect a position of NERC or the Standards Drafting Team

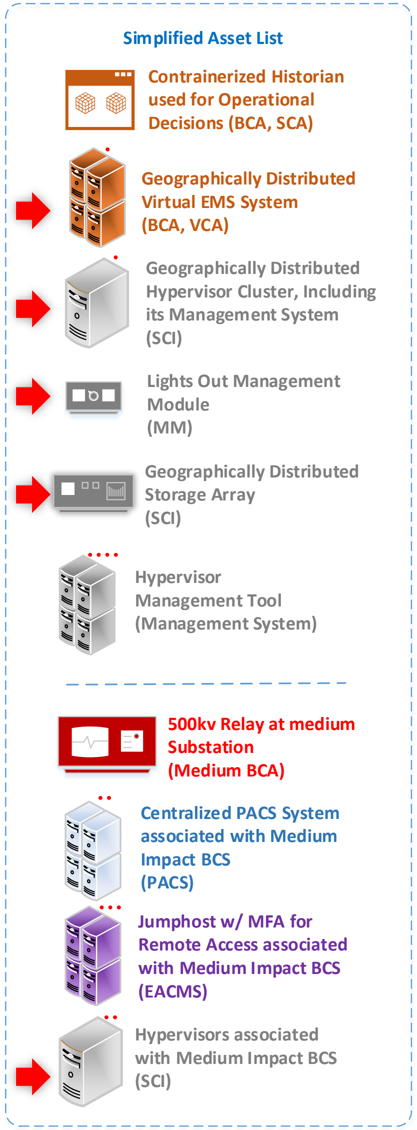
Requirement

Enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports, per system capability If a system has no provision for disabling or restricting logical ports then those ports that are open are deemed needed.

Option 2

Zero Trust Model

CIP-007 R1 Part 1.2



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

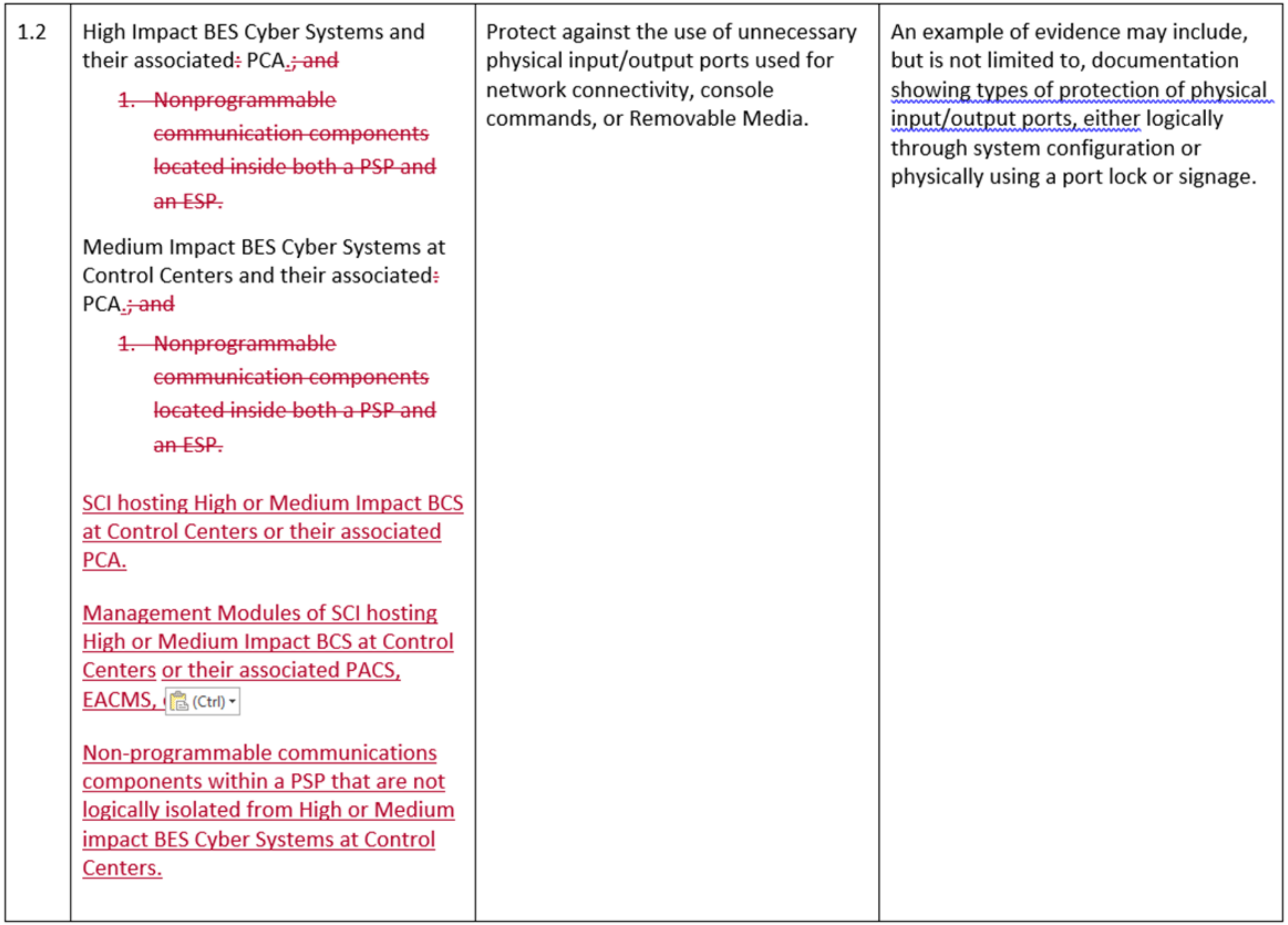
Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

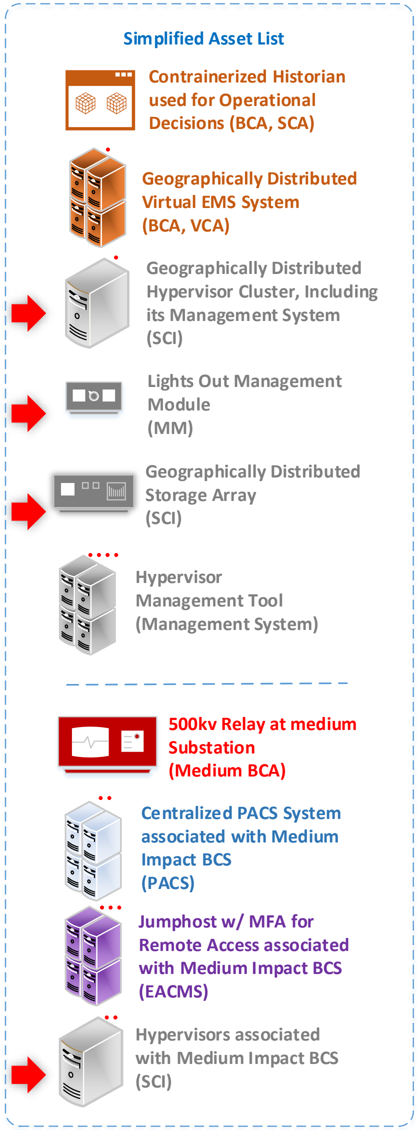
Hypervisors associated with Medium Impact BCS (SCI)



1.2	High Impact BES Cyber Systems and their associated~~:~~ PCA.~~; and~~ ~~1. Nonprogrammable communication components located inside both a PSP and an ESP.~~ Medium Impact BES Cyber Systems at Control Centers and their associated~~:~~ PCA.~~; and~~ ~~1. Nonprogrammable communication components located inside both a PSP and an ESP.~~ SCI hosting High or Medium Impact BCS at Control Centers or their associated PCA. Management Modules of SCI hosting High or Medium Impact BCS at Control Centers or their associated PACS, EACMS, (Ctrl) Non-programmable communications components within a PSP that are not logically isolated from High or Medium impact BES Cyber Systems at Control Centers.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

CIP-007 R1 Part 1.3

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (SCI)

1.3	SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	Enable only services that have been determined to be needed by the Responsible Entity, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of implemented hardening guidelines • Configuration management reporting

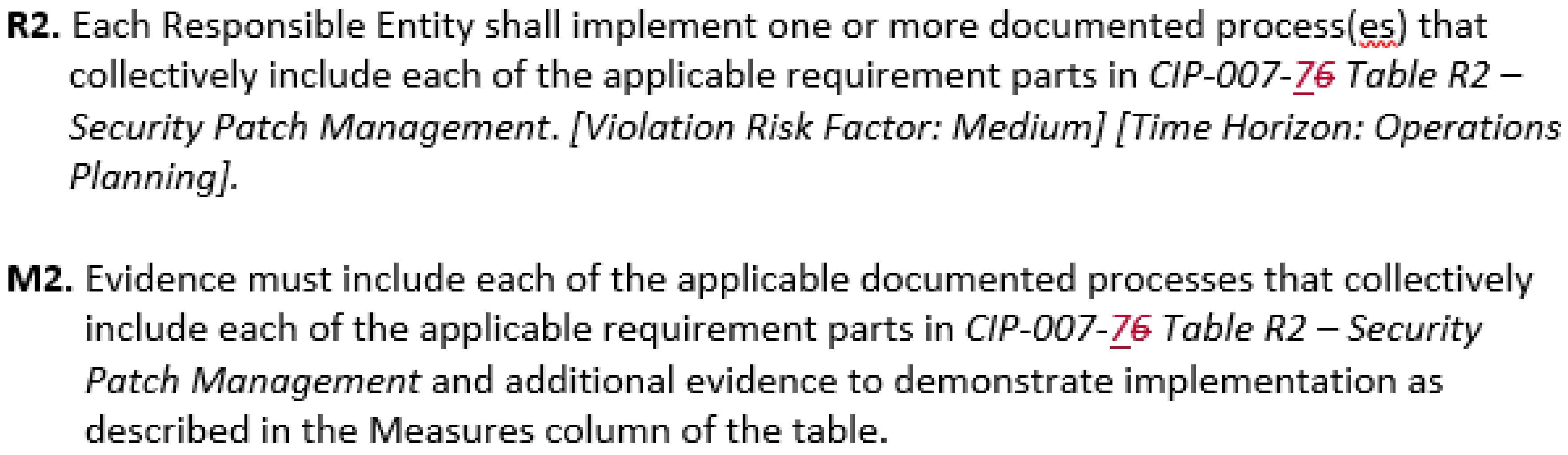
Q&A Response

Join at

slido.com

#2016-02

Proposed CIP-007 Requirement R2

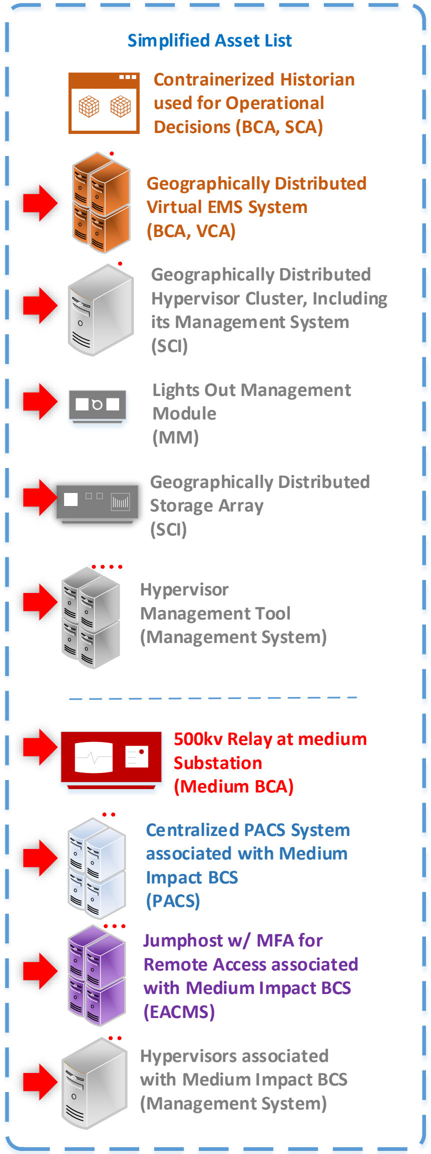


R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Proposed CIP-007 R2 Part 2.1

slido.com #2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

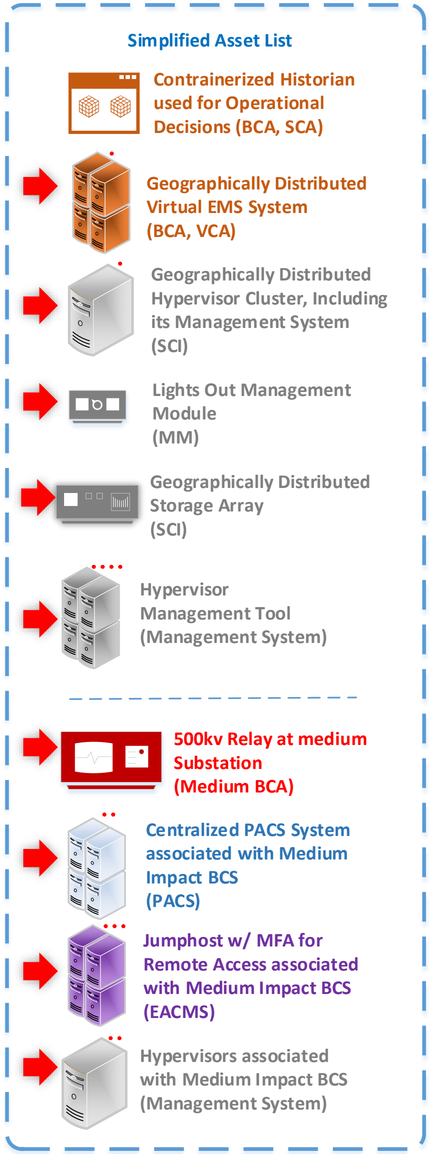
Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	A patch management process for tracking, evaluating, and installing cyber security patches.~~ for applicable Cyber Assets.~~ The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for systems ~~applicable Cyber Assets~~ that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored~~, whether on an individual BES Cyber System or Cyber Asset basis.~~.

Proposed CIP-007 R2 Part 2.2

slido.com #2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

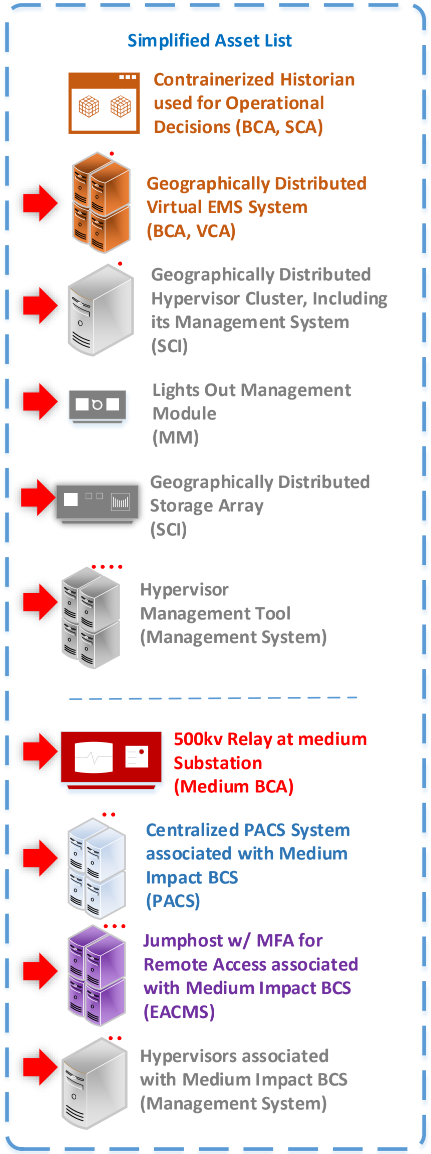
Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 1. 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

Proposed CIP-007 R2 Part 2.3

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

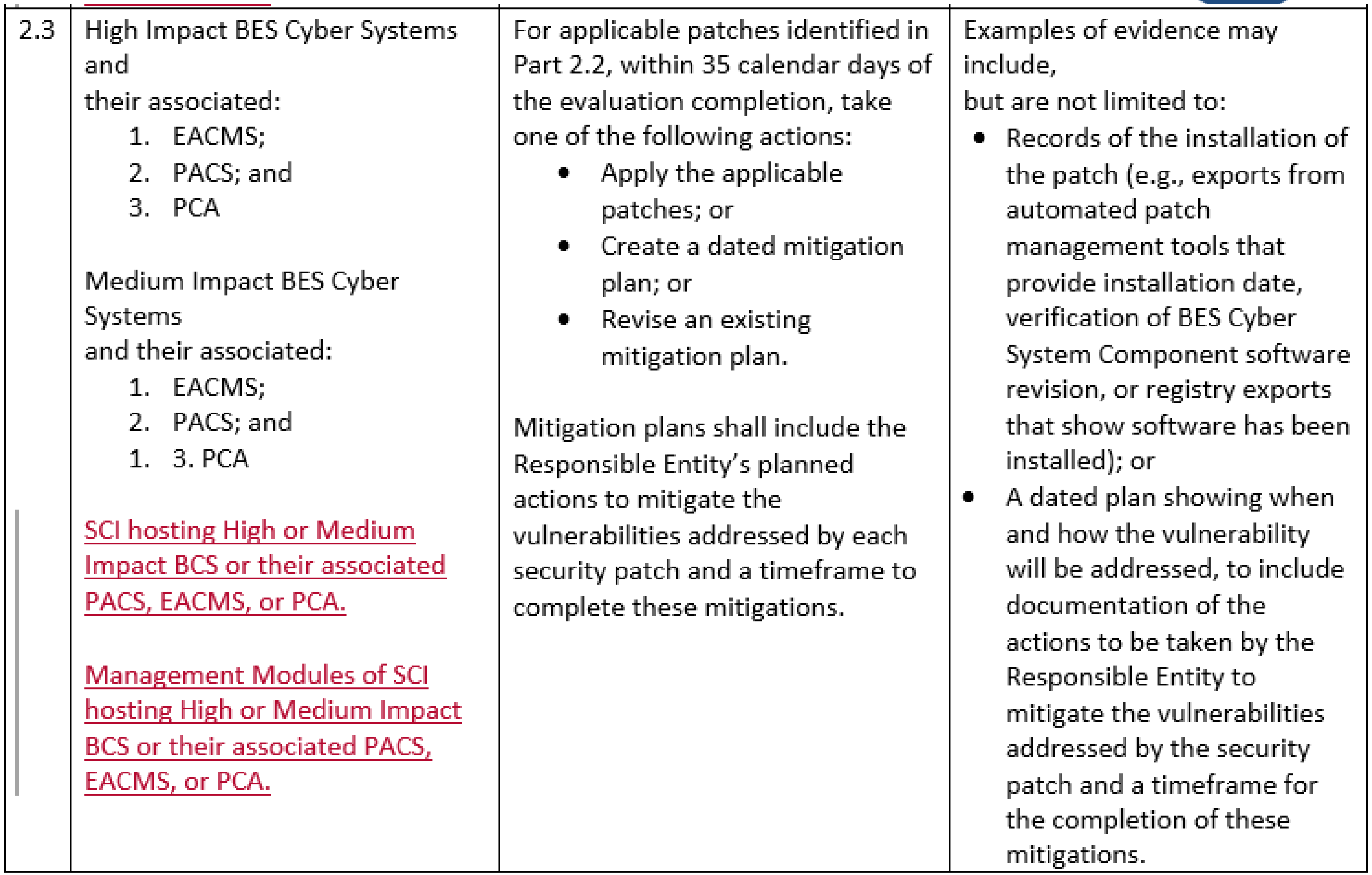
Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

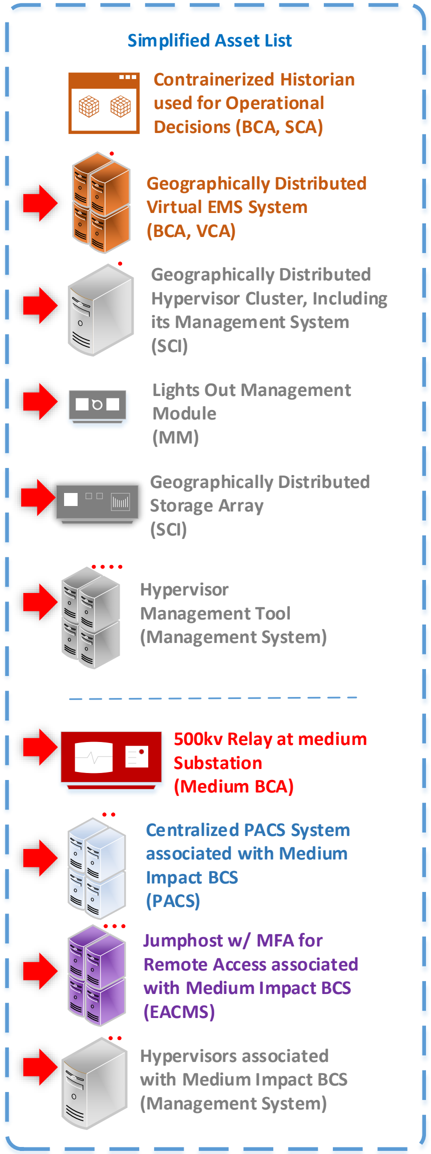
Hypervisors associated with Medium Impact BCS (Management System)



2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 1. 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

Proposed CIP-007 R2 Part 2.4

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

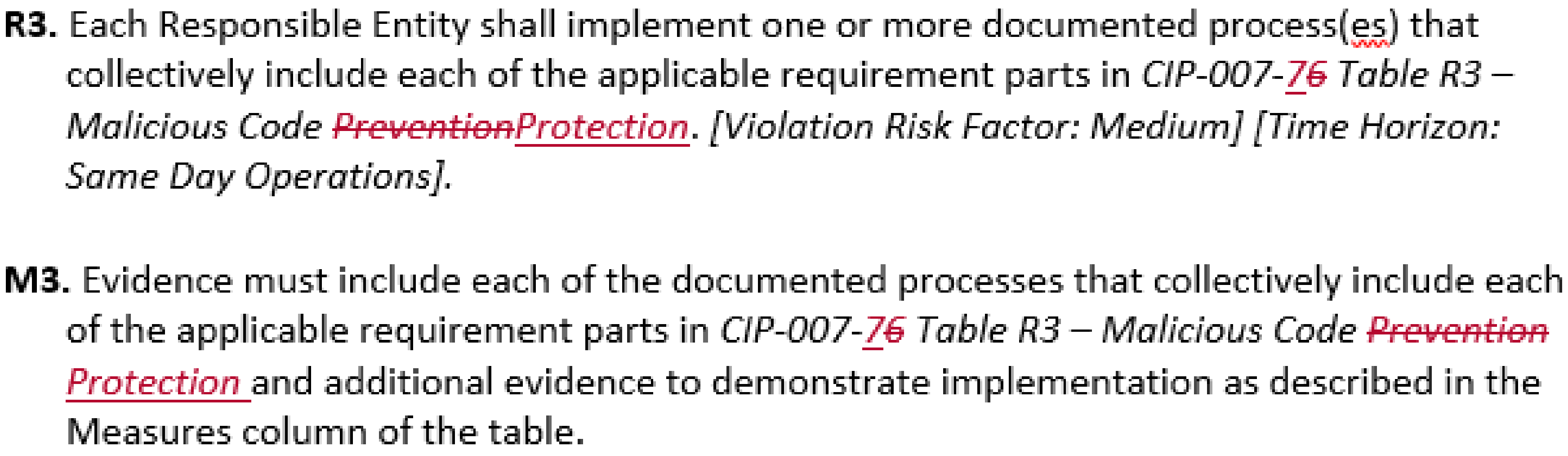
Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

Proposed CIP-007 Requirement R3

slido.com
#2016-02



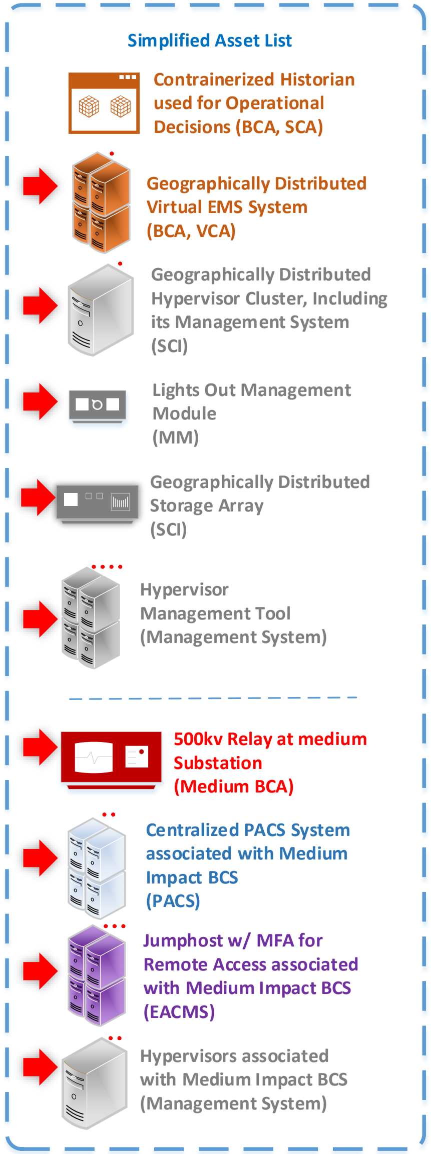
R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R3 – Malicious Code ~~Prevention~~Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*.

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R3 – Malicious Code ~~Prevention~~ Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed CIP-007 R3 Part 3.1

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

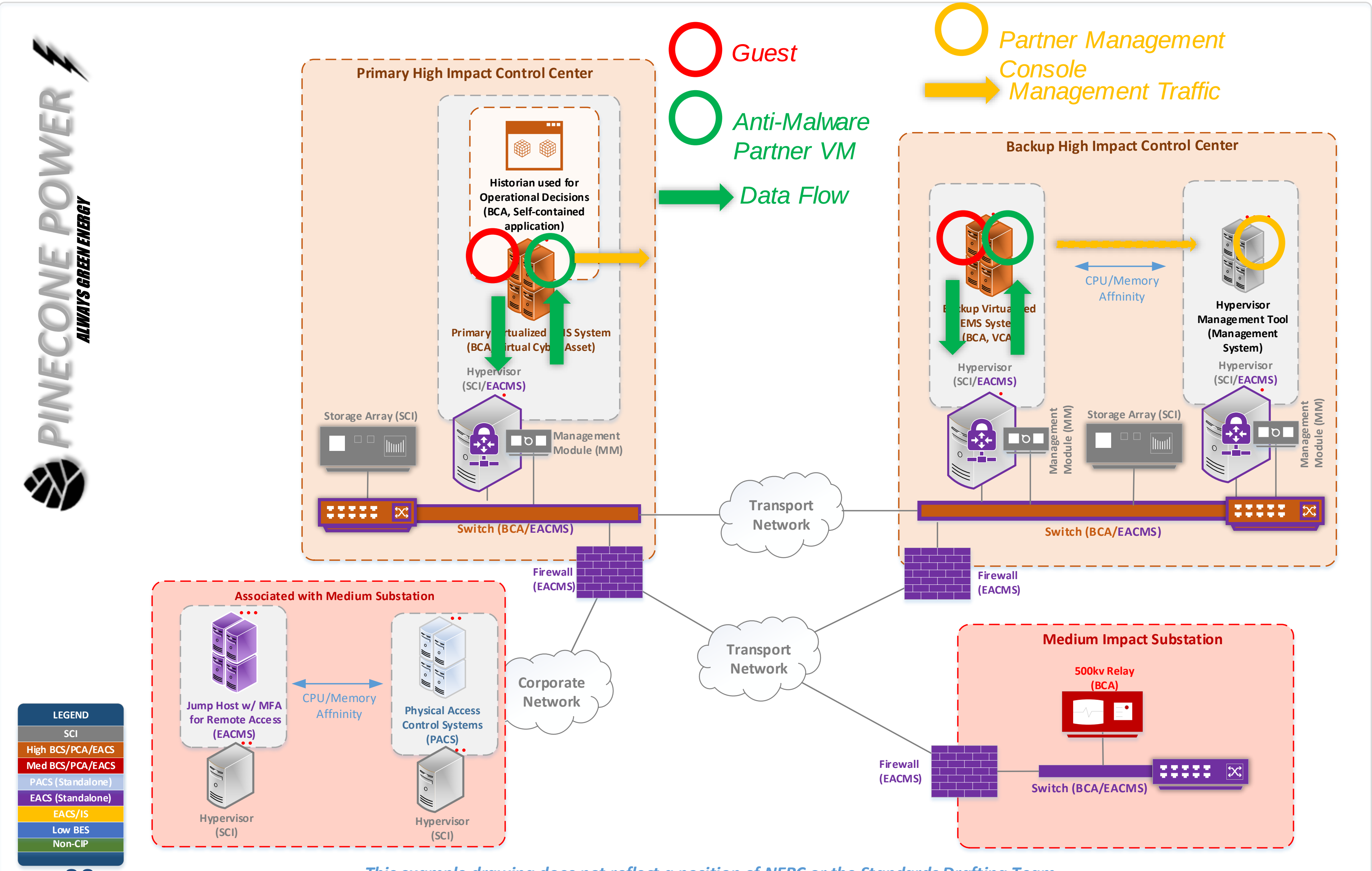
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, white-listing, privileged introspection, etc.).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007 R3 Part 3.1– Zero Trust

slido.com
#2016-02

Workshop Sample Infrastructure – Zero Trust Model (CIP-002 Evaluation Already Completed)



This example drawing does not reflect a position of NERC or the Standards Drafting Team

CIP-007 R3 Part 3.1

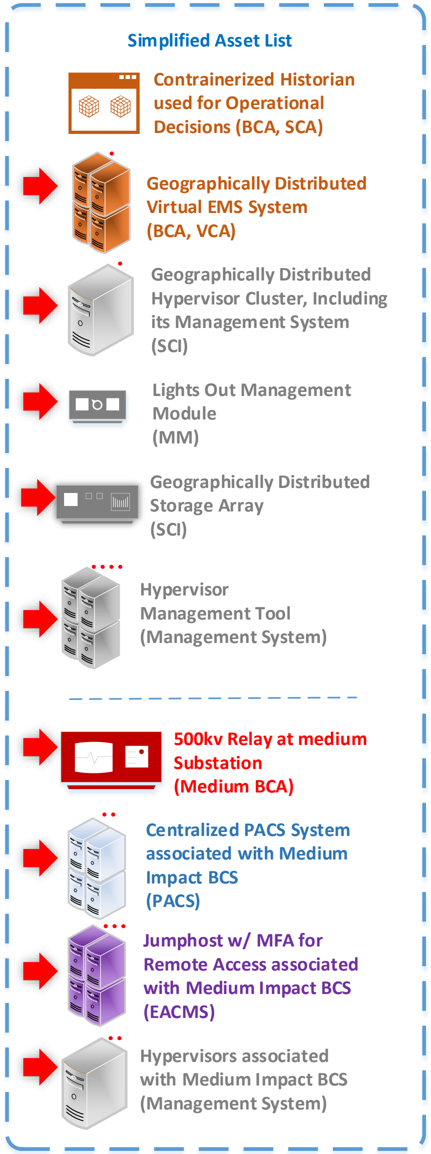
Deploy method(s) to deter, detect, or prevent malicious code.

Implemented Method Example

- Privileged/ Guest Introspection - offloads antivirus and anti-malware agent processing to a dedicated secure virtual appliance

Proposed CIP-007 R3 Part 3.2

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

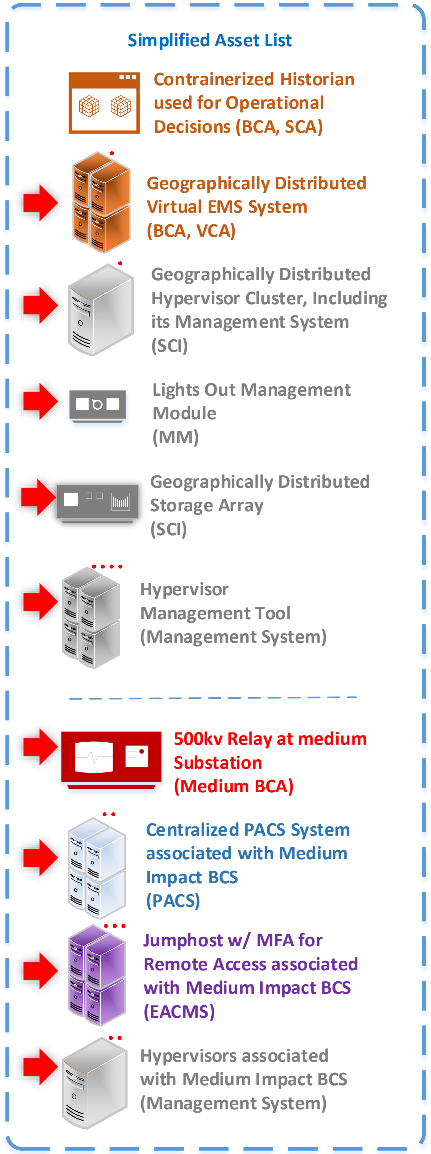
Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

Proposed CIP-007 R3 Part 3.3

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

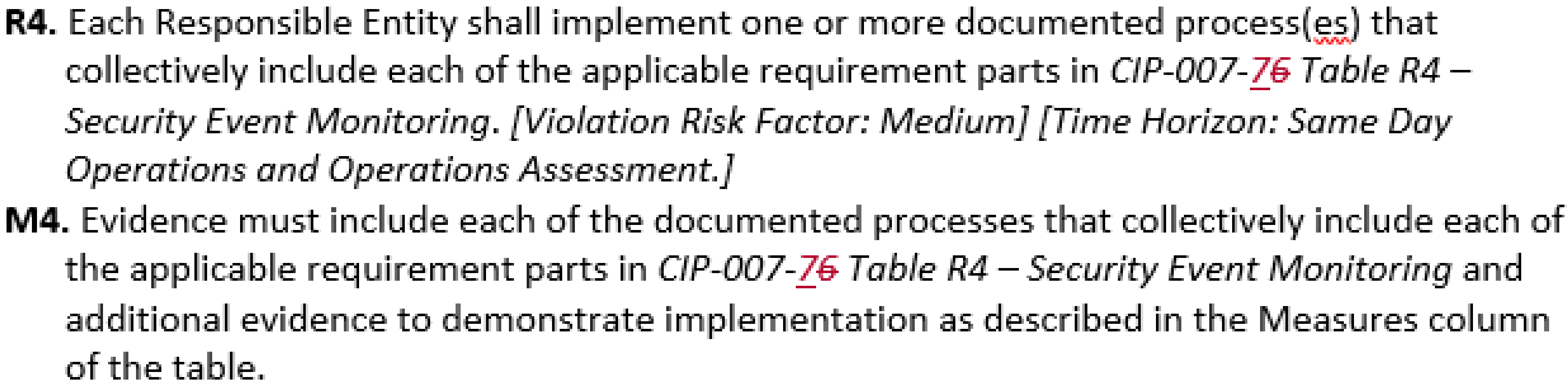
Hypervisors associated with Medium Impact BCS (Management System)

3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Proposed CIP-007 Requirement R4

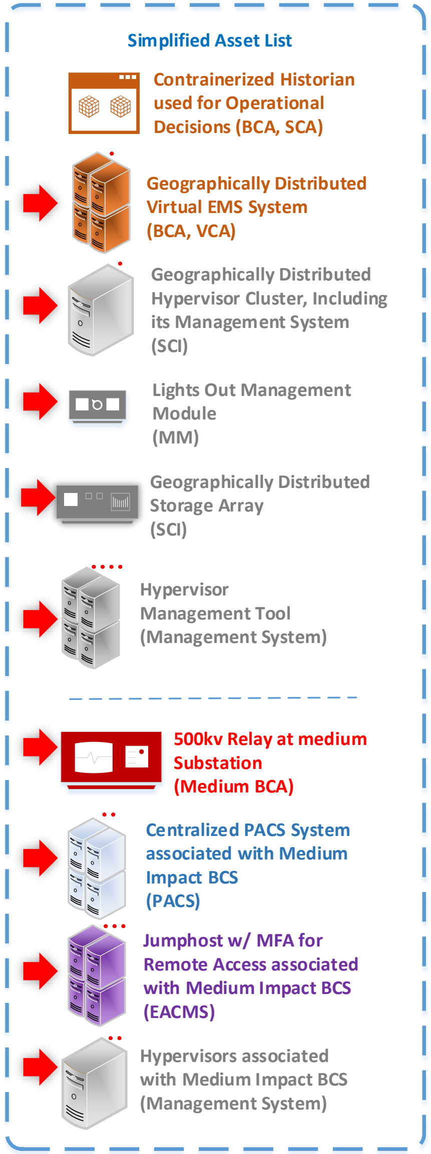
slido.com
#2016-02



R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Proposed CIP-007 R4 Part 4.1



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

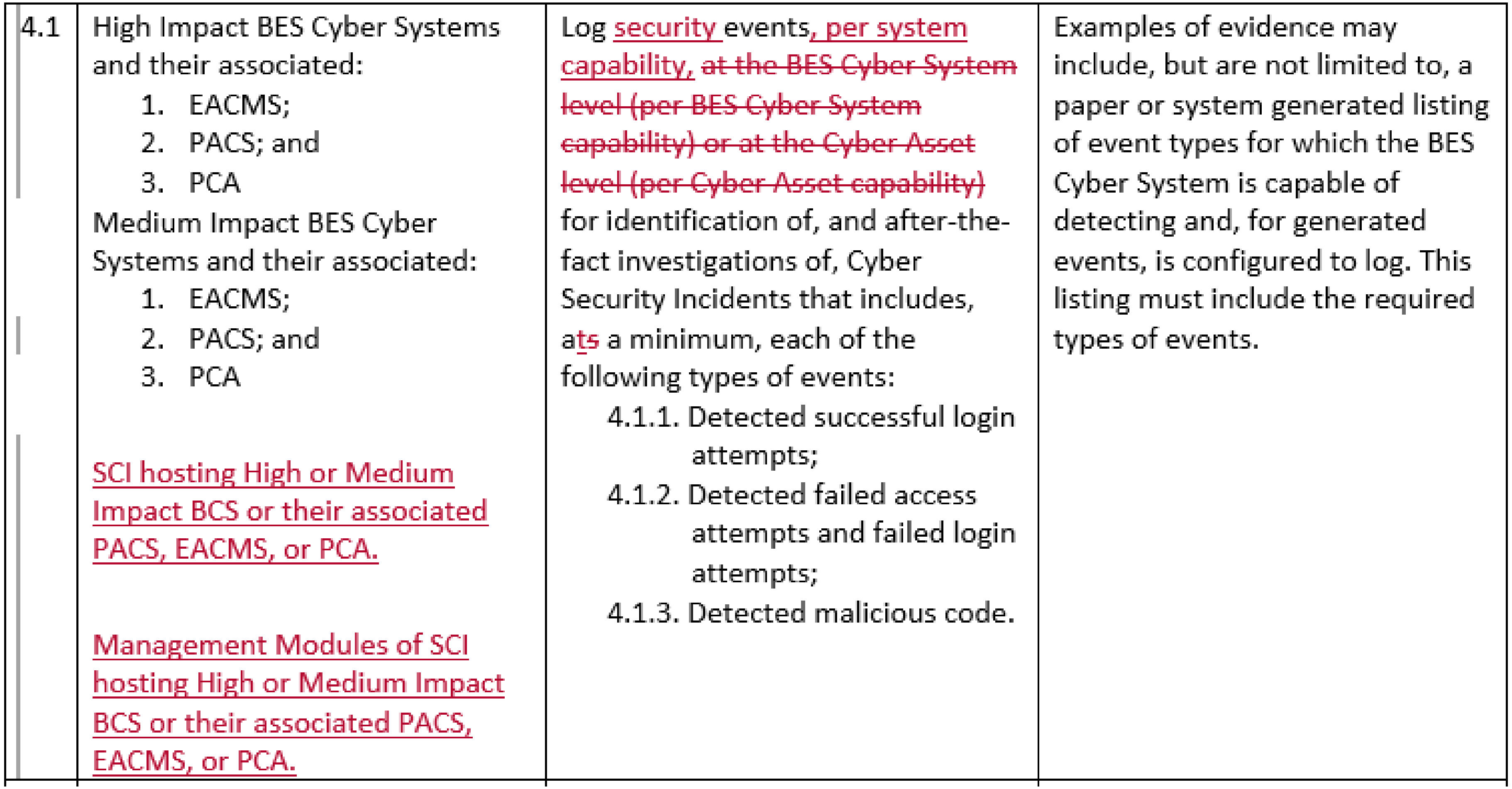
Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

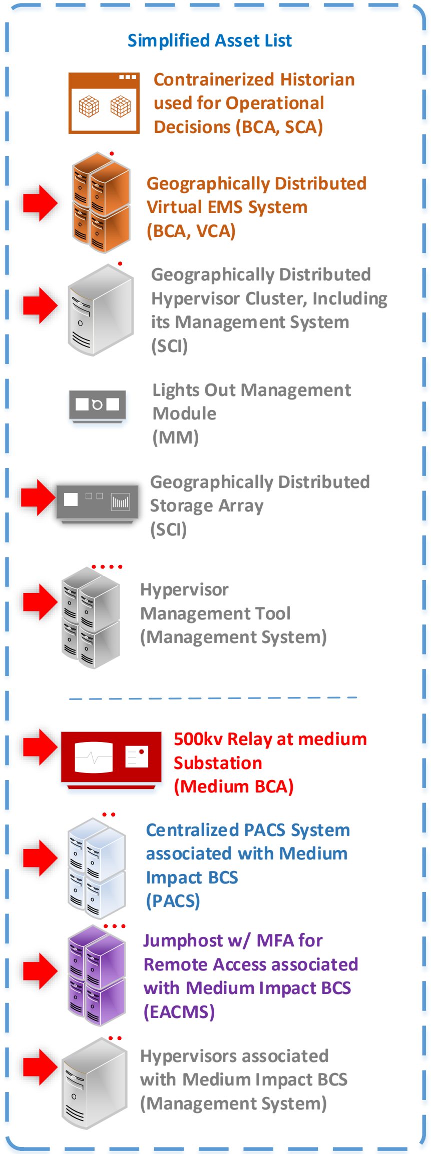
Hypervisors associated with Medium Impact BCS (Management System)



4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	Log security events, per system capability, ~~at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability)~~ for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, ats 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; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

Proposed CIP-007 R4 Part 4.2

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

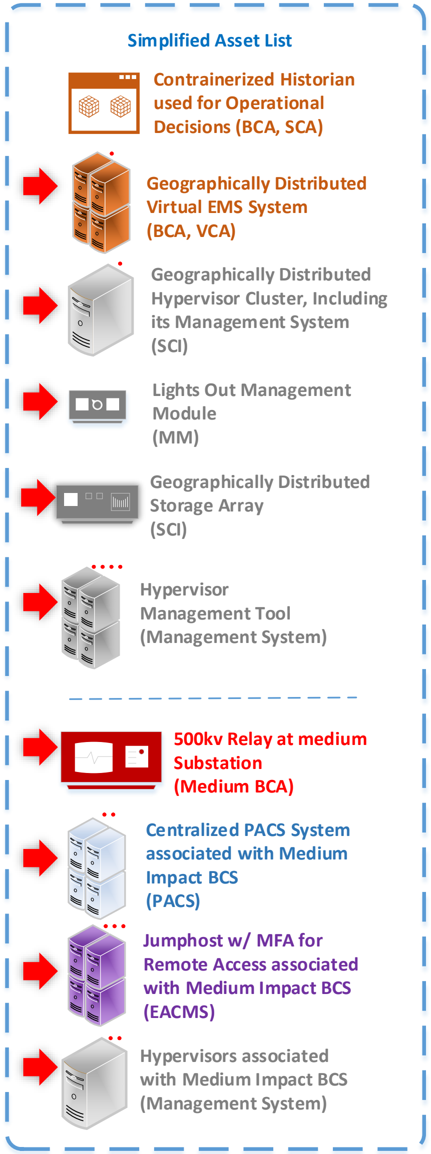
Hypervisors associated with Medium Impact BCS (Management System)

4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACM; 2. PACS; and 3. PCA SCI hosting High Impact BCS or Medium Impact BCS with ERC or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High Impact BCS or Medium Impact BCS with ERC or their associated PACS, EACMS, or PCA.	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, at~~s~~ a minimum, each of the following types of events, (per ~~Cyber Asset or BES Cyber~~ ~~S~~system capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed CIP-007 R4 Part 4.3

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

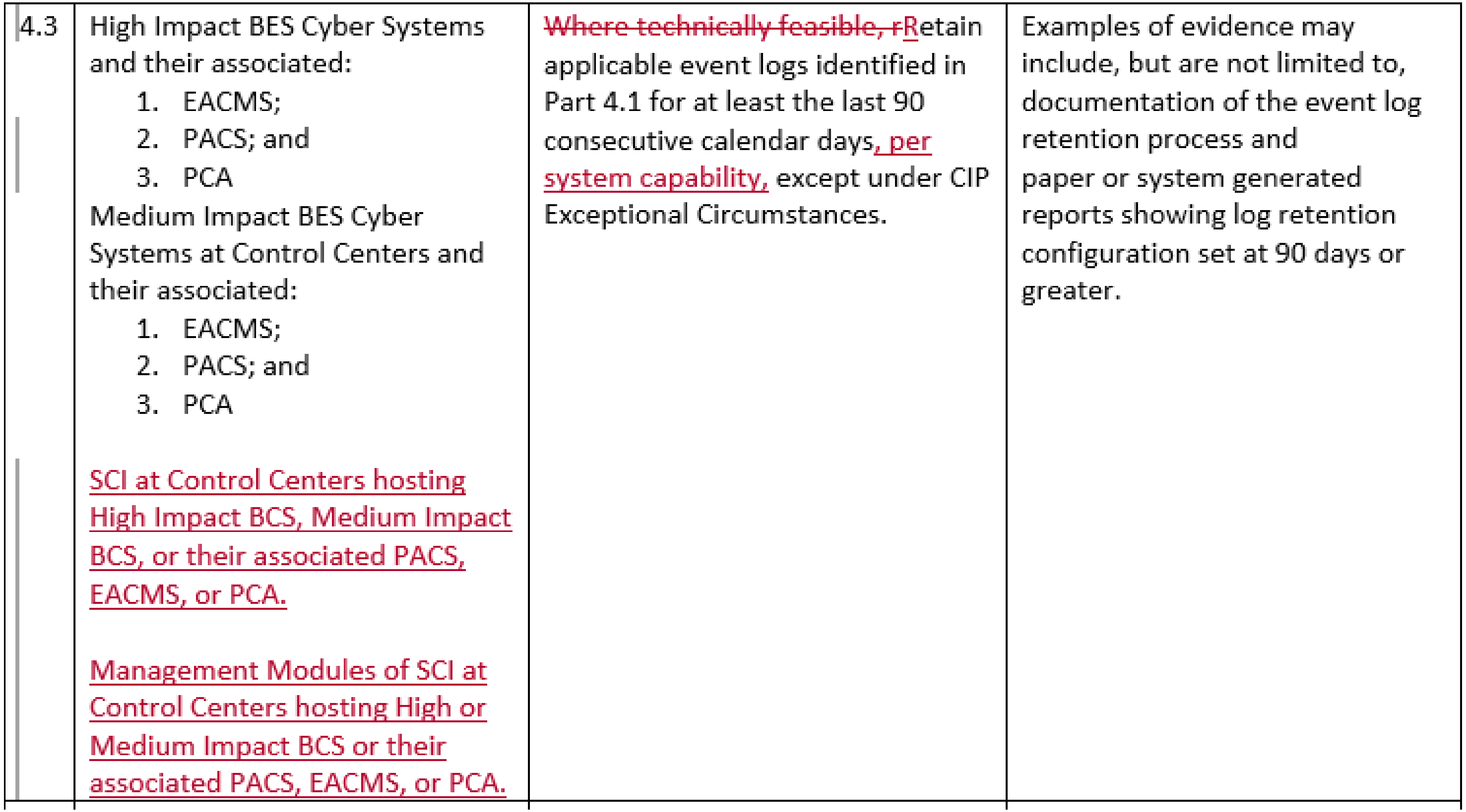
Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

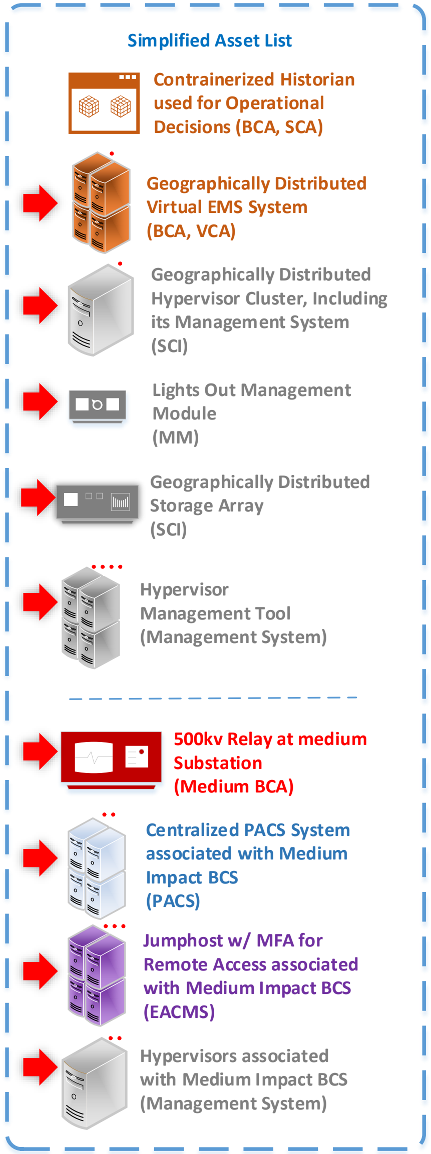
Hypervisors associated with Medium Impact BCS (Management System)

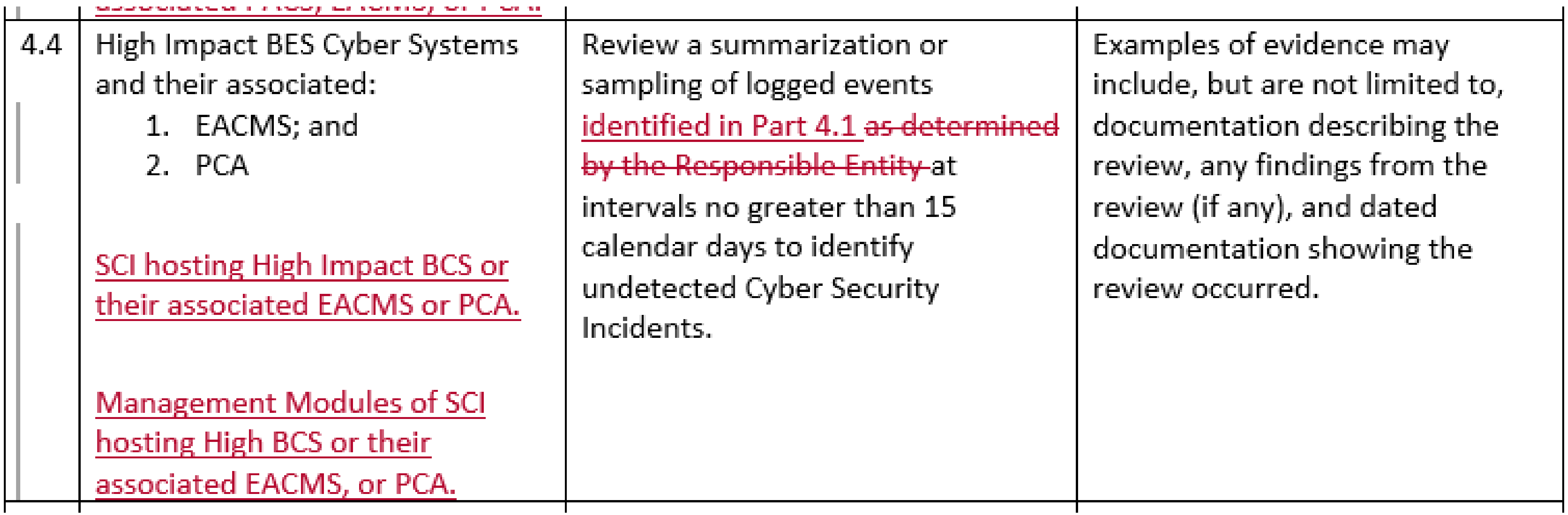


4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI at Control Centers hosting High Impact BCS, Medium Impact BCS, or their associated PACS, EACMS, or PCA. Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	~~Where technically feasible, r~~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.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.

Proposed CIP-007 R4 Part 4.4

slido.com
#2016-02

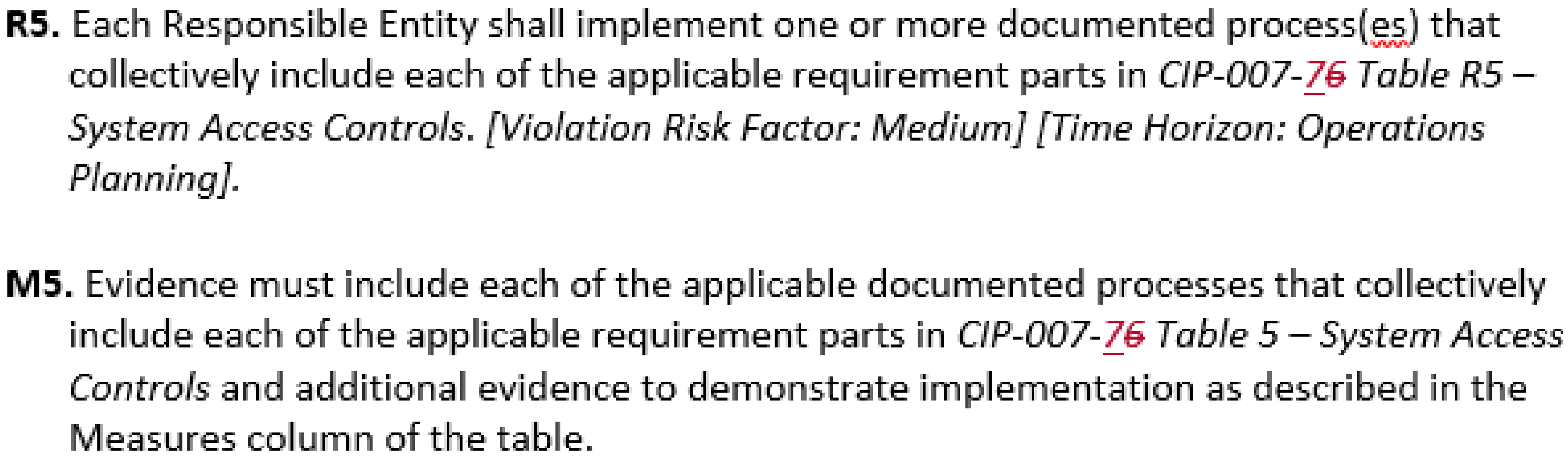

Simplified Asset List
Contrainerized Historian used for Operational Decisions (BCA, SCA)
Geographically Distributed Virtual EMS System (BCA, VCA)
Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)
Lights Out Management Module (MM)
Geographically Distributed Storage Array (SCI)
Hypervisor Management Tool (Management System)
500kv Relay at medium Substation (Medium BCA)
Centralized PACS System associated with Medium Impact BCS (PACS)
Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
Hypervisors associated with Medium Impact BCS (Management System)



	associated PACS, EACMS, or PCA.		
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated EACMS or PCA. Management Modules of SCI hosting High BCS or their associated EACMS, or PCA.	Review a summarization or sampling of logged events identified in Part 4.1 ~~as determined by the Responsible Entity~~ at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

Proposed CIP-007 Requirement R5

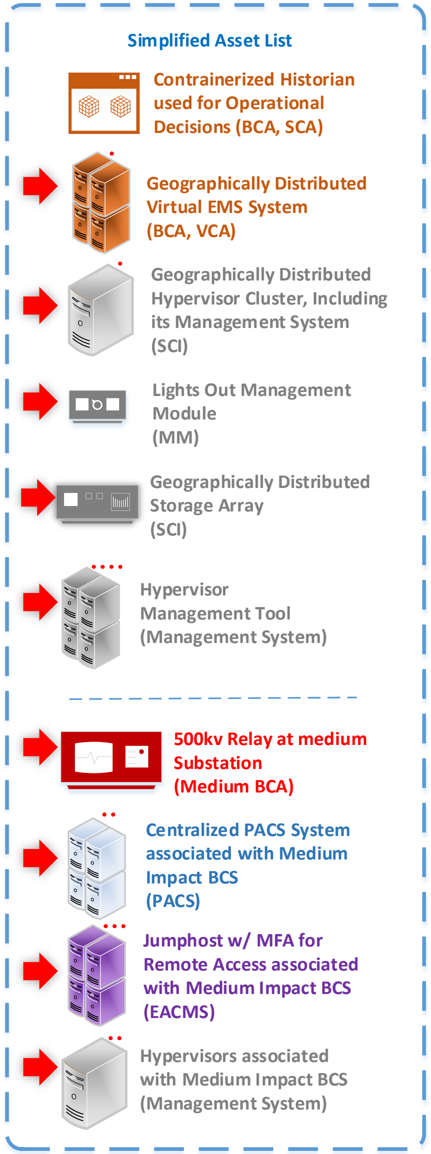
slido.com
#2016-02



R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

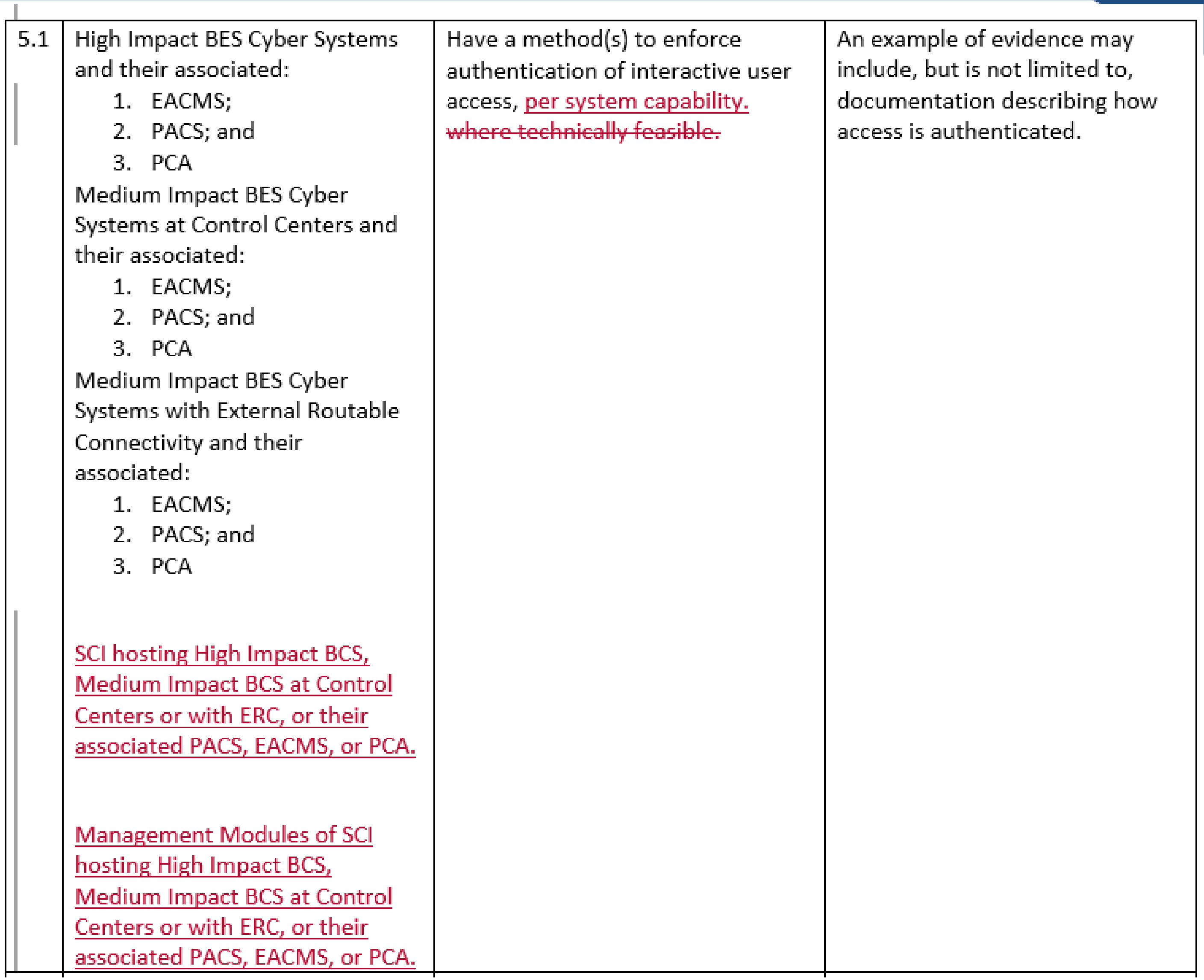
M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Proposed CIP-007 R5 Part 5.1



Simplified Asset List

- Contrainerized Historian used for Operational Decisions (BCA, SCA)
- Geographically Distributed Virtual EMS System (BCA, VCA)
- Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)
- Lights Out Management Module (MM)
- Geographically Distributed Storage Array (SCI)
- Hypervisor Management Tool (Management System)
- 500kv Relay at medium Substation (Medium BCA)
- Centralized PACS System associated with Medium Impact BCS (PACS)
- Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
- Hypervisors associated with Medium Impact BCS (Management System)

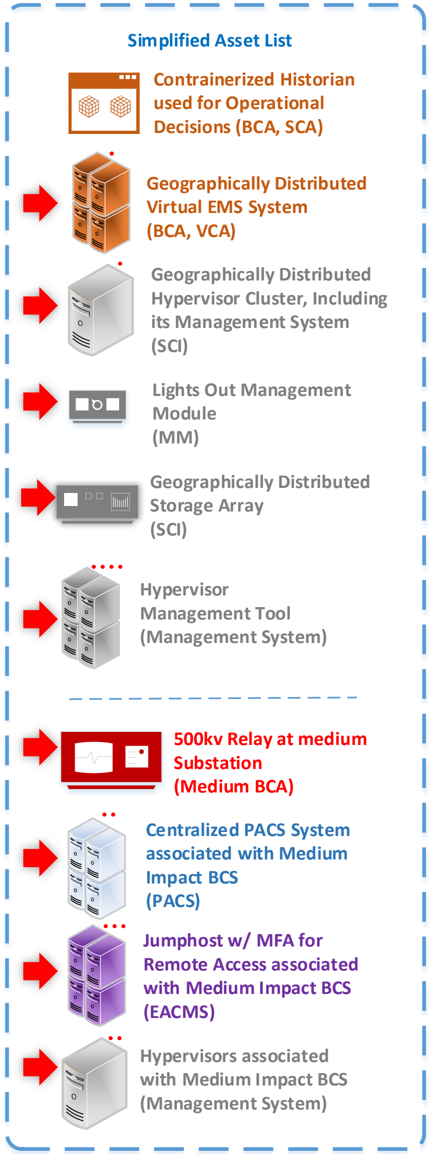


5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High Impact BCS, Medium Impact BCS at Control Centers or with ERC, or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High Impact BCS, Medium Impact BCS at Control Centers or with ERC, or their associated PACS, EACMS, or PCA.	Have a method(s) to enforce authentication of interactive user access, per system capability. ~~where technically feasible.~~	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed CIP-007 R5 Part 5.2

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use. ~~for the BES Cyber System.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed CIP-007 R5 Part 5.3

slido.com
#2016-02

Simplified Asset List

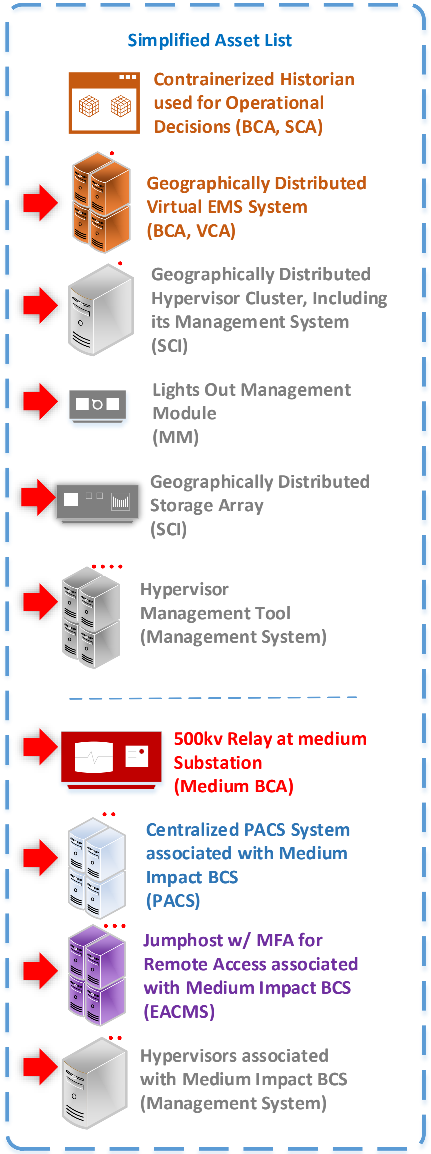
- Contrainerized Historian used for Operational Decisions (BCA, SCA)
- Geographically Distributed Virtual EMS System (BCA, VCA)
- Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)
- Lights Out Management Module (MM)
- Geographically Distributed Storage Array (SCI)
- Hypervisor Management Tool (Management System)
- 500kv Relay at medium Substation (Medium BCA)
- Centralized PACS System associated with Medium Impact BCS (PACS)
- Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
- Hypervisors associated with Medium Impact BCS (Management System)

5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High Impact BCS, Medium Impact BCS with ERC, or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High Impact BCS, Medium Impact BCS with ERC, or their associated PACS, EACMS, or PCA.	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed CIP-007 R5 Part 5.4

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

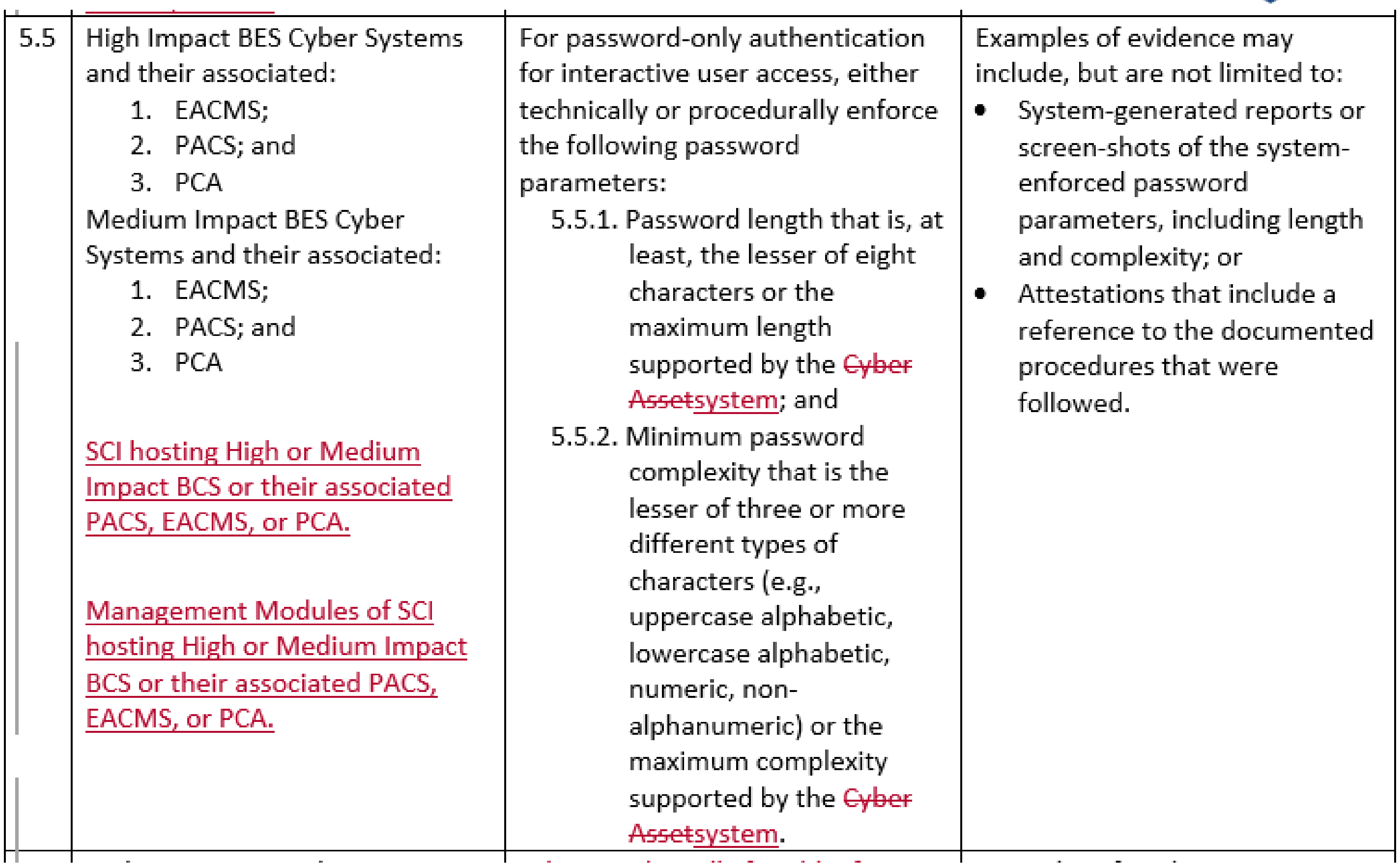
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	Change known default passwords, per ~~Cyber Asset~~system capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique. ~~to the device.~~

Proposed CIP-007 R5 Part 5.5

slido.com
#2016-02

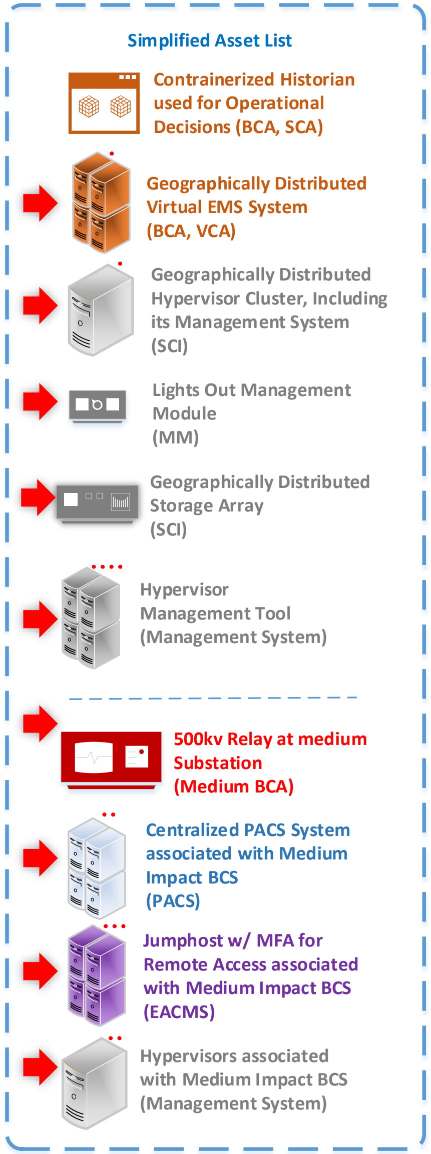
Simplified Asset List

- Contrainerized Historian used for Operational Decisions (BCA, SCA)
- Geographically Distributed Virtual EMS System (BCA, VCA)
- Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)
- Lights Out Management Module (MM)
- Geographically Distributed Storage Array (SCI)
- Hypervisor Management Tool (Management System)
- 500kv Relay at medium Substation (Medium BCA)
- Centralized PACS System associated with Medium Impact BCS (PACS)
- Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
- Hypervisors associated with Medium Impact BCS (Management System)



5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the ~~Cyber Asset~~system; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the ~~Cyber Asset~~system.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

Proposed CIP-007 R5 Part 5.6



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

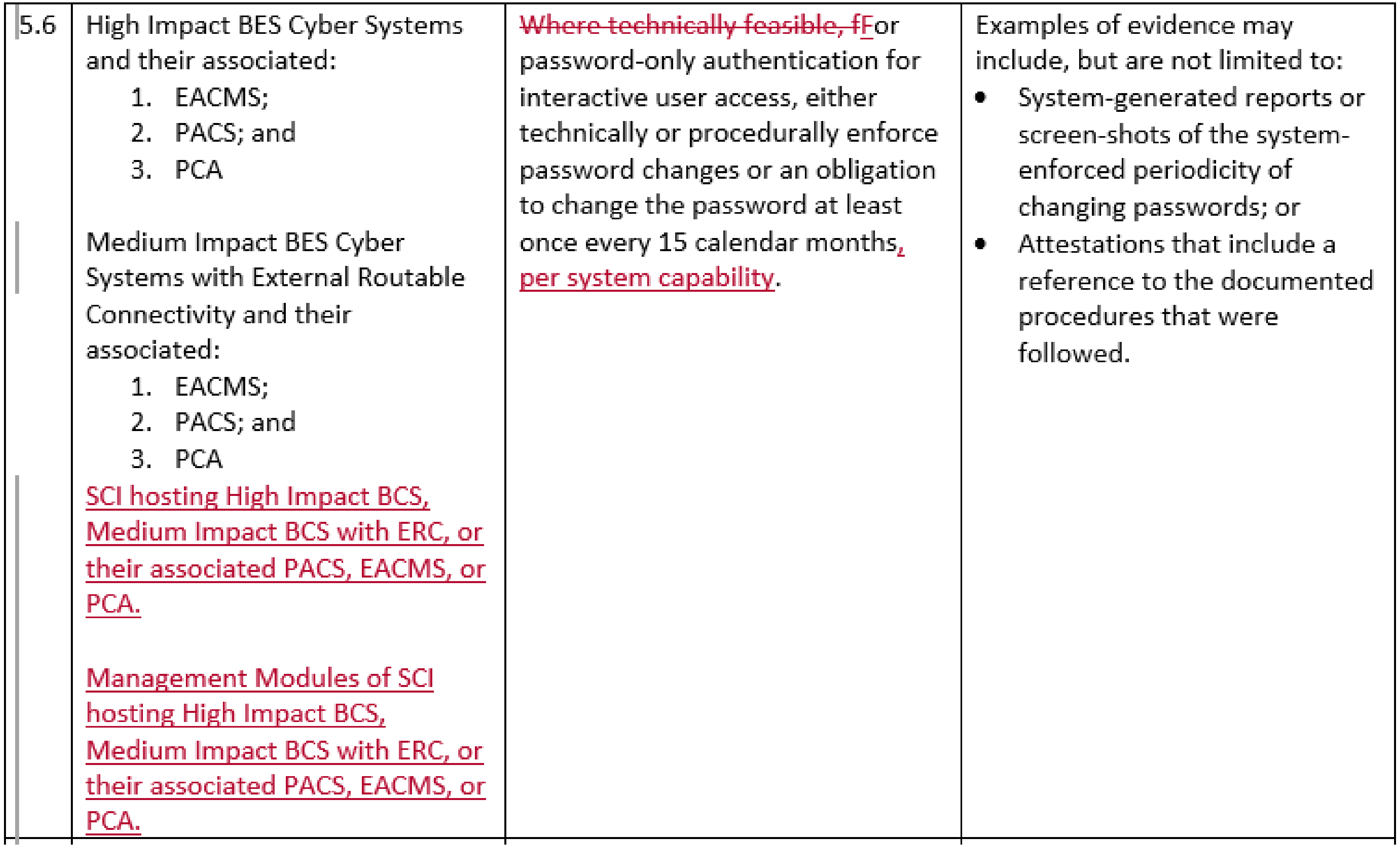
Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

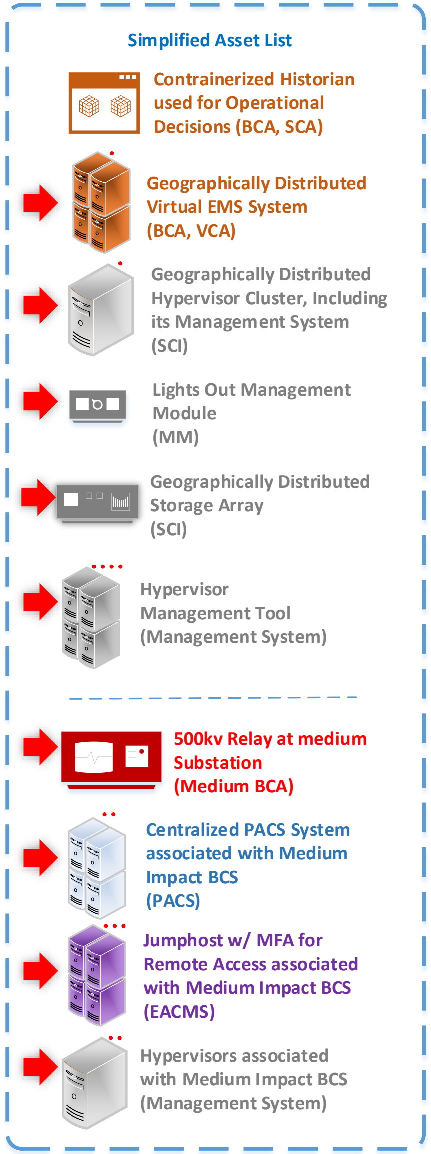
Hypervisors associated with Medium Impact BCS (Management System)

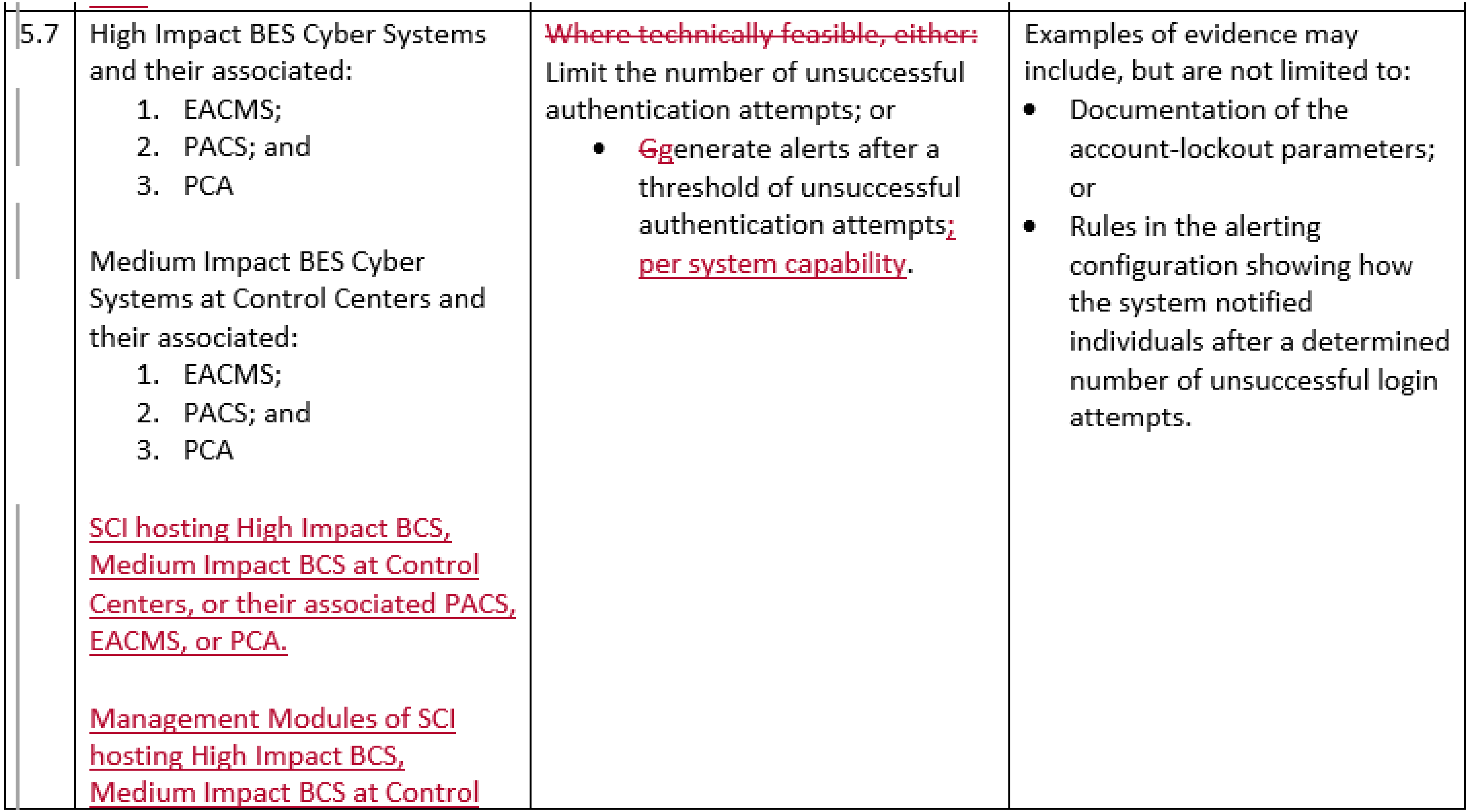


5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High Impact BCS, Medium Impact BCS with ERC, or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High Impact BCS, Medium Impact BCS with ERC, or their associated PACS, EACMS, or PCA.	~~Where technically feasible, f~~For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

Proposed CIP-007 R5 Part 5.7

slido.com #2016-02


Simplified Asset List
Contrainerized Historian used for Operational Decisions (BCA, SCA)
Geographically Distributed Virtual EMS System (BCA, VCA)
Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)
Lights Out Management Module (MM)
Geographically Distributed Storage Array (SCI)
Hypervisor Management Tool (Management System)
500kv Relay at medium Substation (Medium BCA)
Centralized PACS System associated with Medium Impact BCS (PACS)
Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
Hypervisors associated with Medium Impact BCS (Management System)



5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High Impact BCS, Medium Impact BCS at Control Centers, or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High Impact BCS, Medium Impact BCS at Control	~~Where technically feasible, either:~~ Limit the number of unsuccessful authentication attempts; or • ~~G~~generate alerts after a threshold of unsuccessful authentication attempts; per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Q&A Response

Join at
slido.com
#2016-02

RELIABILITY | RESILIENCE | SECURITY

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Break

We will return at X:XX p.m. Eastern

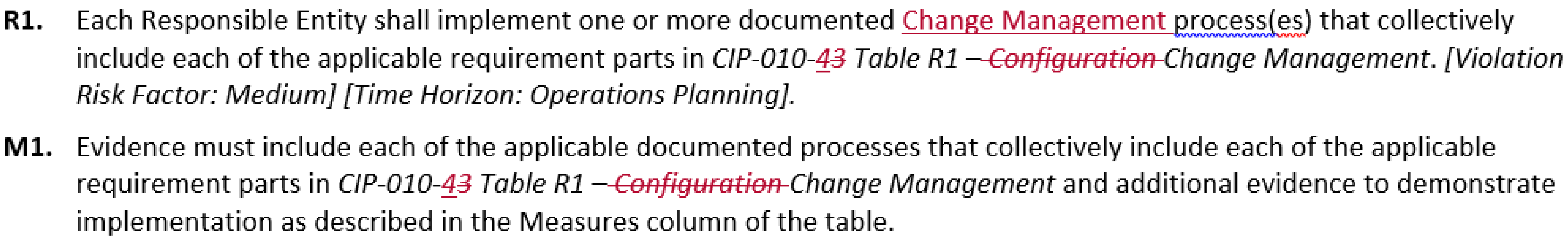
Join at

slido.com

#2016-02

RELIABILITY | RESILIENCE | SECURITY

Proposed CIP-010 Requirement R1

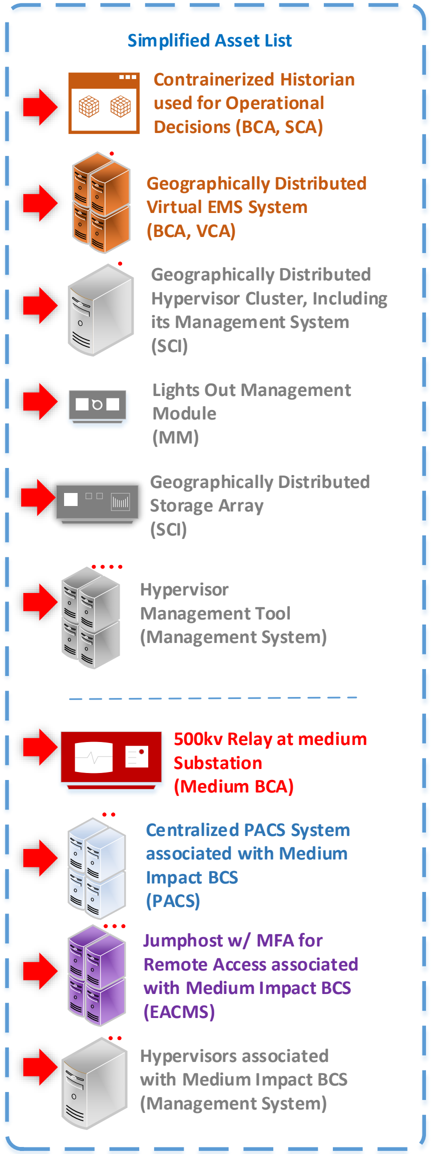


R1. Each Responsible Entity shall implement one or more documented Change Management process(es) that collectively include each of the applicable requirement parts in *CIP-010-4~~3~~ Table R1 – ~~Configuration~~ Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4~~3~~ Table R1 – ~~Configuration~~ Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Proposed CIP-010 R1 Part 1.1

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

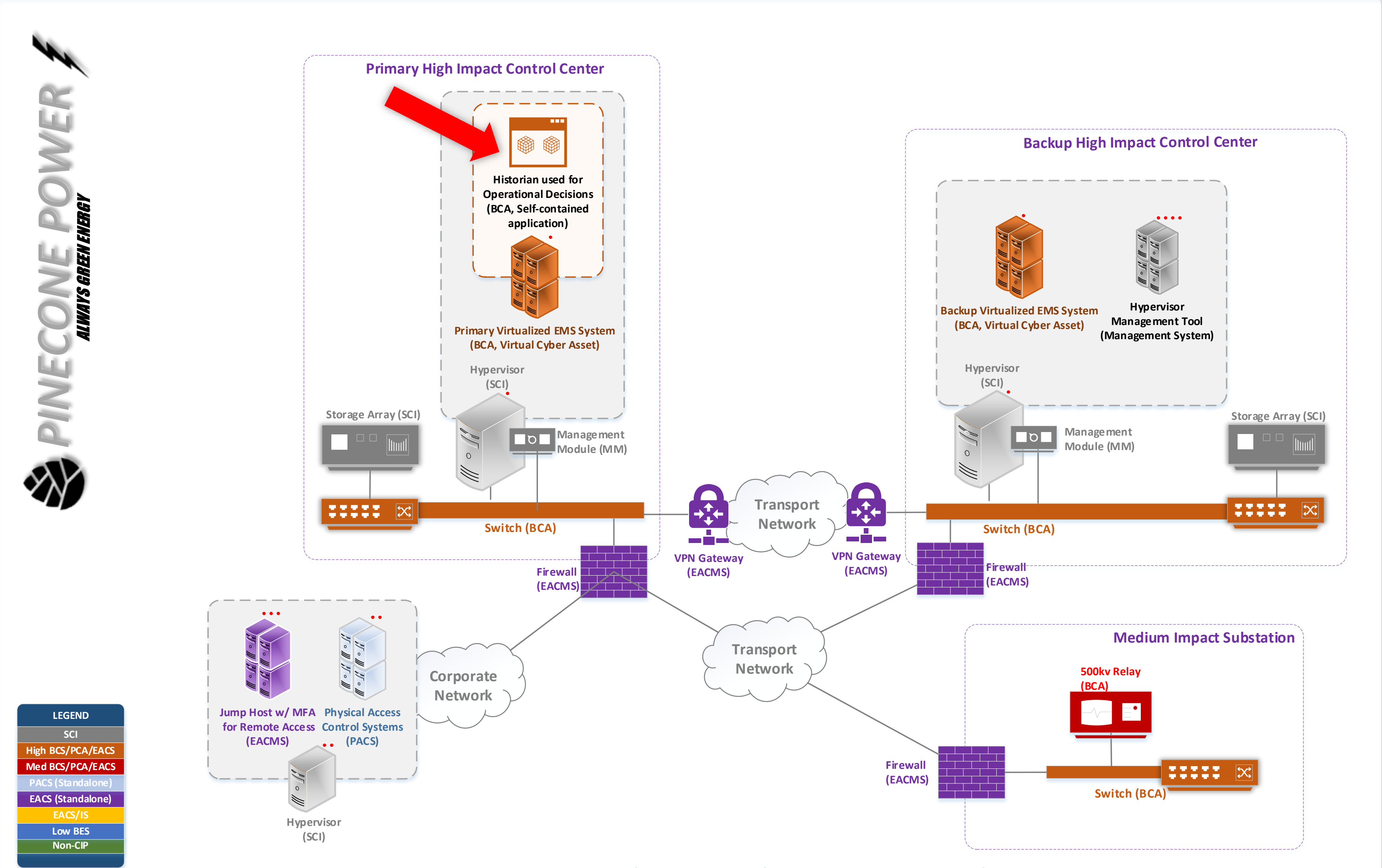
Hypervisors associated with Medium Impact BCS (Management System)

1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	Authorize changes to~~Develop a baseline configuration, individually or by group, which shall include the following items~~: 1.1.1. Operating system(s) ~~(including version)~~ or firmware ~~where no independent operating system exists;~~ or images used to derive operating systems or firmware; 1.1.2. ~~Any c~~Commercially available or open-source application software including Self-Contained Applications ~~(including version) intentionally installed~~; 1.1.3. ~~Any c~~Custom software installed including Self-Contained Applications; 1.1.4. ~~Any l~~Logical network ~~accessible ports~~connectivity; and 1.1.5. ~~Any s~~Security patches applied; 1.1.6. SCI configuration that: 1.1.6.1. Enforces electronic access control that permits only needed and controlled communication between systems with different impact ratings hosted on SCI; 1.1.6.2. Enforces logical isolation between systems with different impact ratings hosted on SCI; 1.1.6.3. Prevents sharing of CPU/Memory between systems with different impact ratings hosted on SCI; and 1.1.6.4. Enables or disables services on SCI .	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change.~~spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or~~ • ~~A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.~~

Containerized Historian used for Operational Decisions

slido.com
#2016-02

Workshop Sample Infrastructure (CIP-002 Evaluation Already Completed)



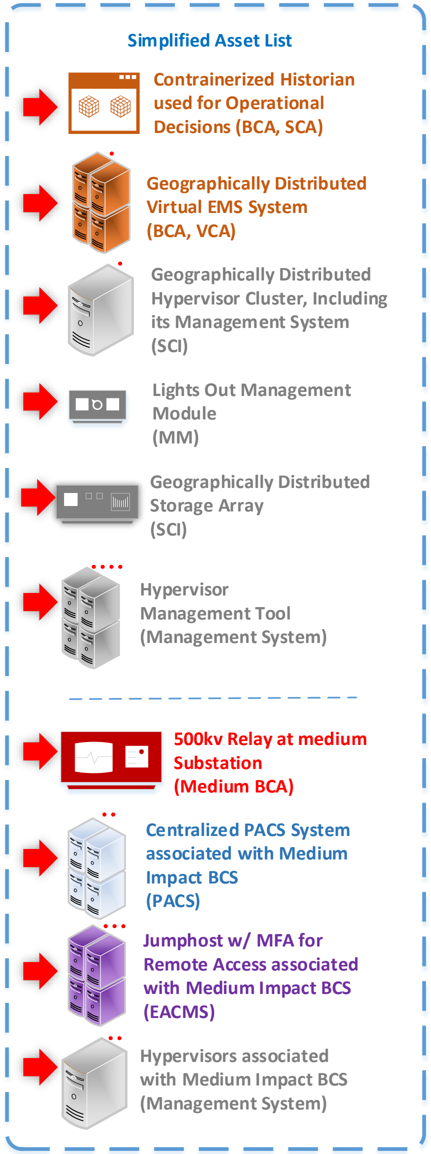
This example drawing does not reflect a position of NERC or the Standards Drafting Team

Self-Contained Application

Immutable software binaries containing operating system dependencies and application software packaged to execute in an isolated environment.

Proposed CIP-010 R1 Part 1.1 (Clean)

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	Authorize changes to: **1.1.1.** Operating system(s) or firmware or images used to derive operating systems or firmware; **1.1.2.** Commercially available or open-source application software including Self-Contained Applications ; **1.1.3.** Custom software installed including Self-Contained Applications; **1.1.4.** Logical network connectivity; **1.1.5.** Security patches applied; **1.1.6.** SCI configuration that: 1.1.6.1. Enforces electronic access control that permits only needed and controlled communication between systems with different impact ratings hosted on SCI; 1.1.6.2. Enforces logical isolation between systems with different impact ratings hosted on SCI;	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change

CIP-010 R1 Part 1.1 (Clean)

slido.com
#2016-02

Simplified Asset List

- Contrainerized Historian used for Operational Decisions (BCA, SCA)
- Geographically Distributed Virtual EMS System (BCA, VCA)
- Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)
- Lights Out Management Module (MM)
- Geographically Distributed Storage Array (SCI)
- Hypervisor Management Tool (Management System)

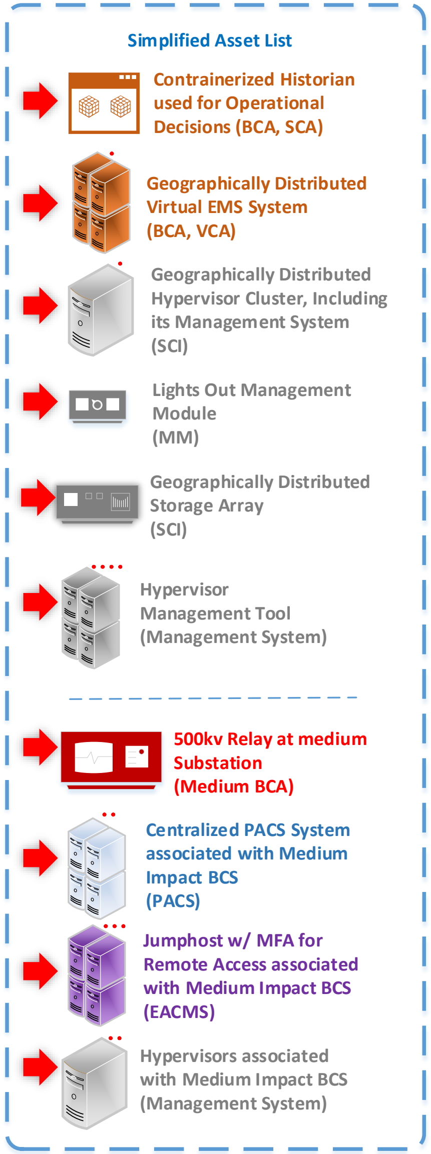
- 500kv Relay at medium Substation (Medium BCA)
- Centralized PACS System associated with Medium Impact BCS (PACS)
- Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
- Hypervisors associated with Medium Impact BCS (Management System)

		1.1.6.3. Prevents sharing of CPU/Memory between systems with different impact ratings hosted on SCI; and 1.1.6.4. Enables or disables services on SCI.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed CIP-010 R1 Part 1.2

slido.com
#2016-02


Simplified Asset List
Contrainerized Historian used for Operational Decisions (BCA, SCA)
Geographically Distributed Virtual EMS System (BCA, VCA)
Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)
Lights Out Management Module (MM)
Geographically Distributed Storage Array (SCI)
Hypervisor Management Tool (Management System)
500kv Relay at medium Substation (Medium BCA)
Centralized PACS System associated with Medium Impact BCS (PACS)
Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
Hypervisors associated with Medium Impact BCS (Management System)

<table>
<tr><th colspan="4">CIP-010-4~~3~~ Table R1 – ~~Configuration~~ Change Management</th></tr>
<tr><th>Part</th><th>Applicable Systems</th><th>Requirements</th><th>Measures</th></tr>
<tr><td>1.24</td><td>High Impact BES Cyber Systems and their associated:
1. EACMS;
2. PACS; and
3. PCA

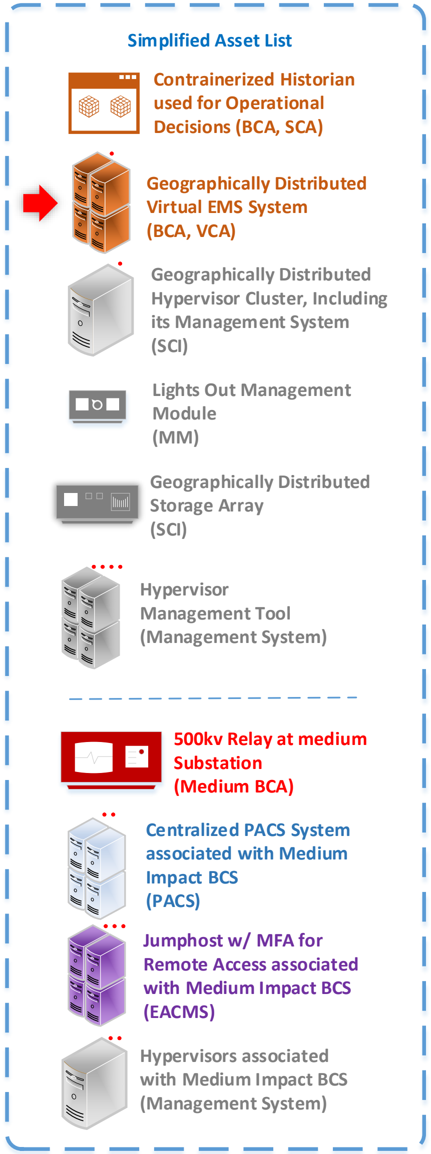
Medium Impact BES Cyber Systems and their associated:
1. EACMS;
2. PACS; and
3. PCA

SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.

Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.</td><td>For ~~a~~ each change to the items listed in Part 1.1~~that deviates from the existing baseline configuration~~:
1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;
1.4.2. Following the change, verify that required cyber security controls determined in 1.24.1 are not adversely affected; and
1.4.3. Document the results of the verification.</td><td>An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.</td></tr>
</table>

Proposed CIP-010 R1 Part 1.3

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

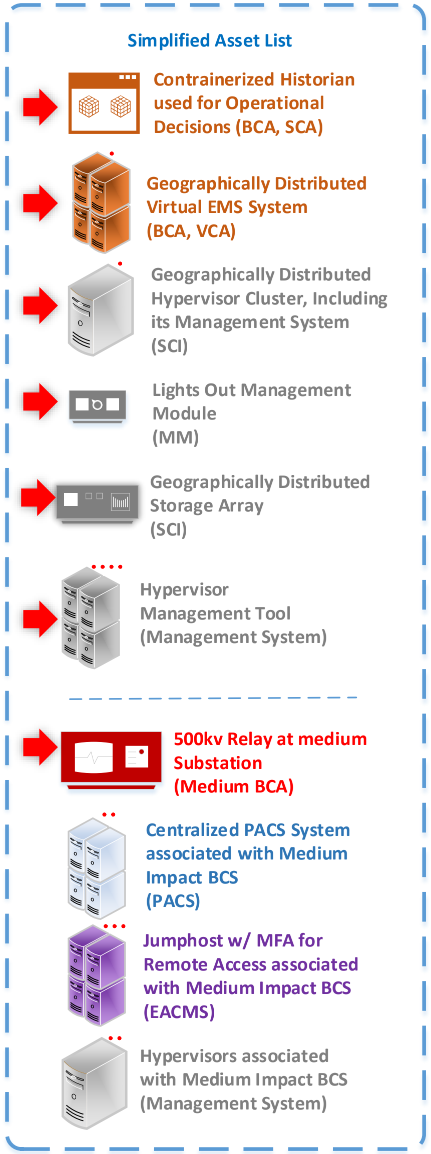
Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

1.3~~5~~	High Impact BES Cyber Systems.	~~Where technically feasible, f~~For each change to the items listed in Part 1.1 ~~that deviates from the existing baseline configuration~~, per system capability: 1.3.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects and differences with the production environment ~~, that models the baseline configuration~~ to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.3.2. 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	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

Proposed CIP-010 R1 Part 1.4

slido.com
#2016-02



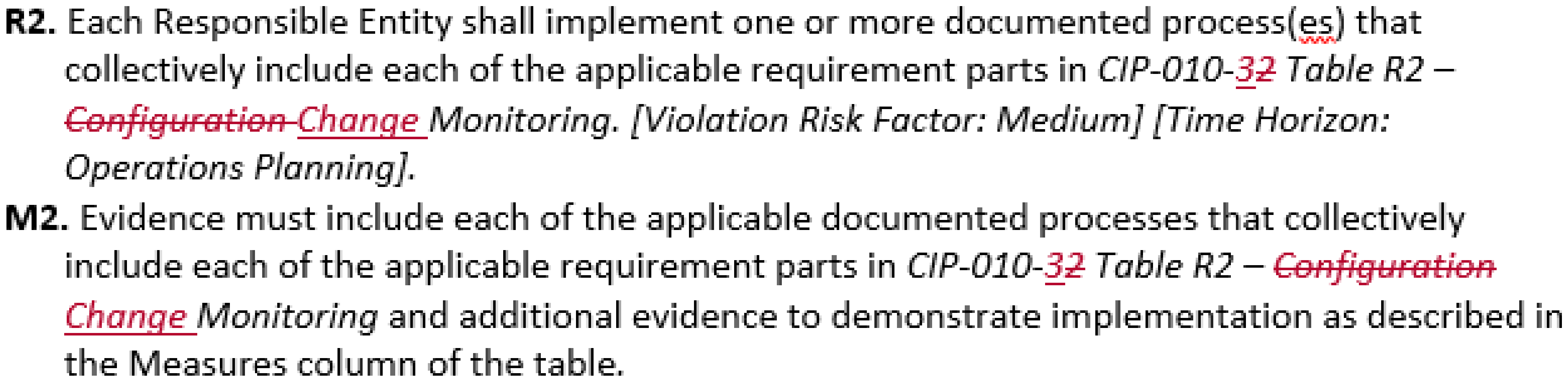
Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)
Geographically Distributed Virtual EMS System (BCA, VCA)
Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)
Lights Out Management Module (MM)
Geographically Distributed Storage Array (SCI)
Hypervisor Management Tool (Management System)
500kv Relay at medium Substation (Medium BCA)
Centralized PACS System associated with Medium Impact BCS (PACS)
Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)
Hypervisors associated with Medium Impact BCS (Management System)

Part	Applicable Systems	Requirements	Measures
		between the test and production environments.	
1.4~~6~~	High Impact BES Cyber Systems Medium Impact BES Cyber Systems SCI hosting High or Medium Impact BCS. Management Modules of SCI hosting High or Medium Impact BCS. Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change ~~that deviates from the existing baseline configuration~~ associated with ~~baseline items in~~Requirement Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.~~6~~4.1. -Verify the identity of the software source; and 1.~~6~~4.2. -Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

slido.com
#2016-02

Proposed CIP-010 Requirement R2



R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3~~2~~ Table R2 – ~~Configuration~~ Change Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3~~2~~ Table R2 – ~~Configuration~~ Change Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Proposed CIP-010 R2 Part 2.1

slido.com
#2016-02

Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

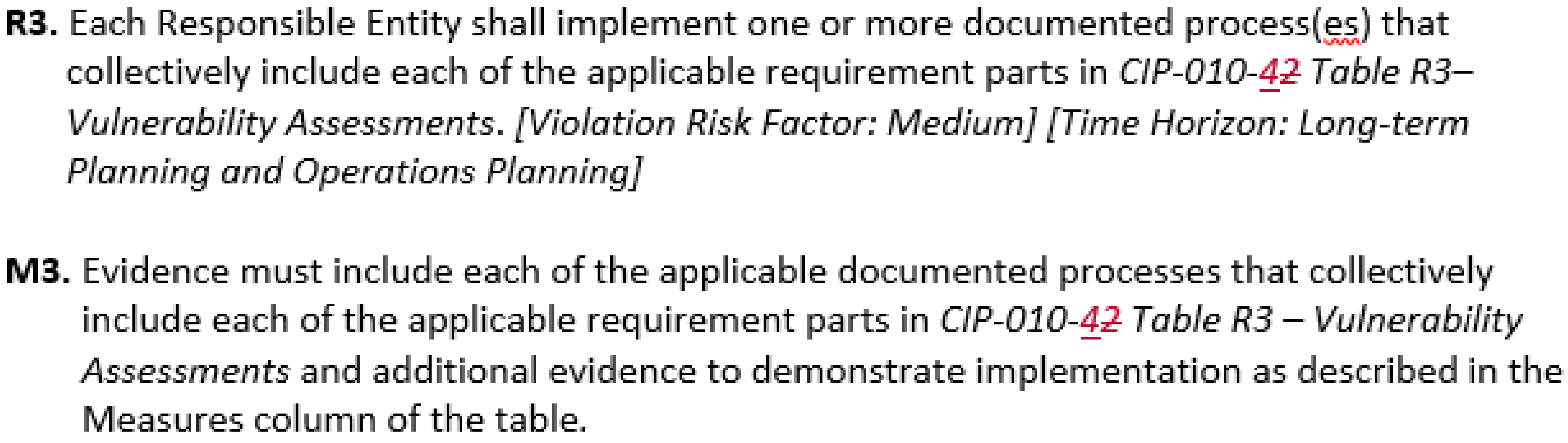
Hypervisors associated with Medium Impact BCS (Management System)

2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for unauthorized changes to the ~~baseline configuration~~ items ~~(as~~ described in Requirement R1, Part 1.1~~)~~. Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed CIP-010 Requirement R3

slido.com
#2016-02

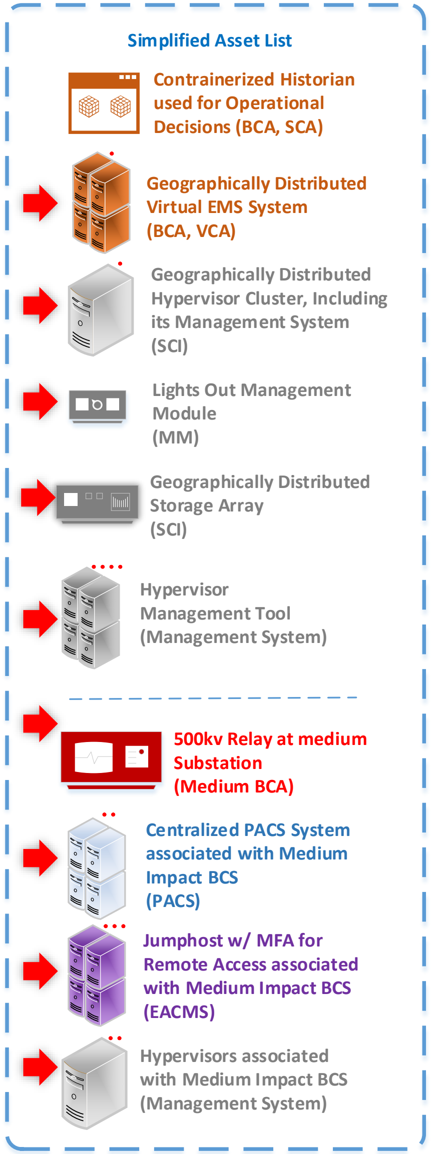


R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4~~2~~ Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4~~2~~ Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Proposed CIP-010 R3 Part 3.1

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

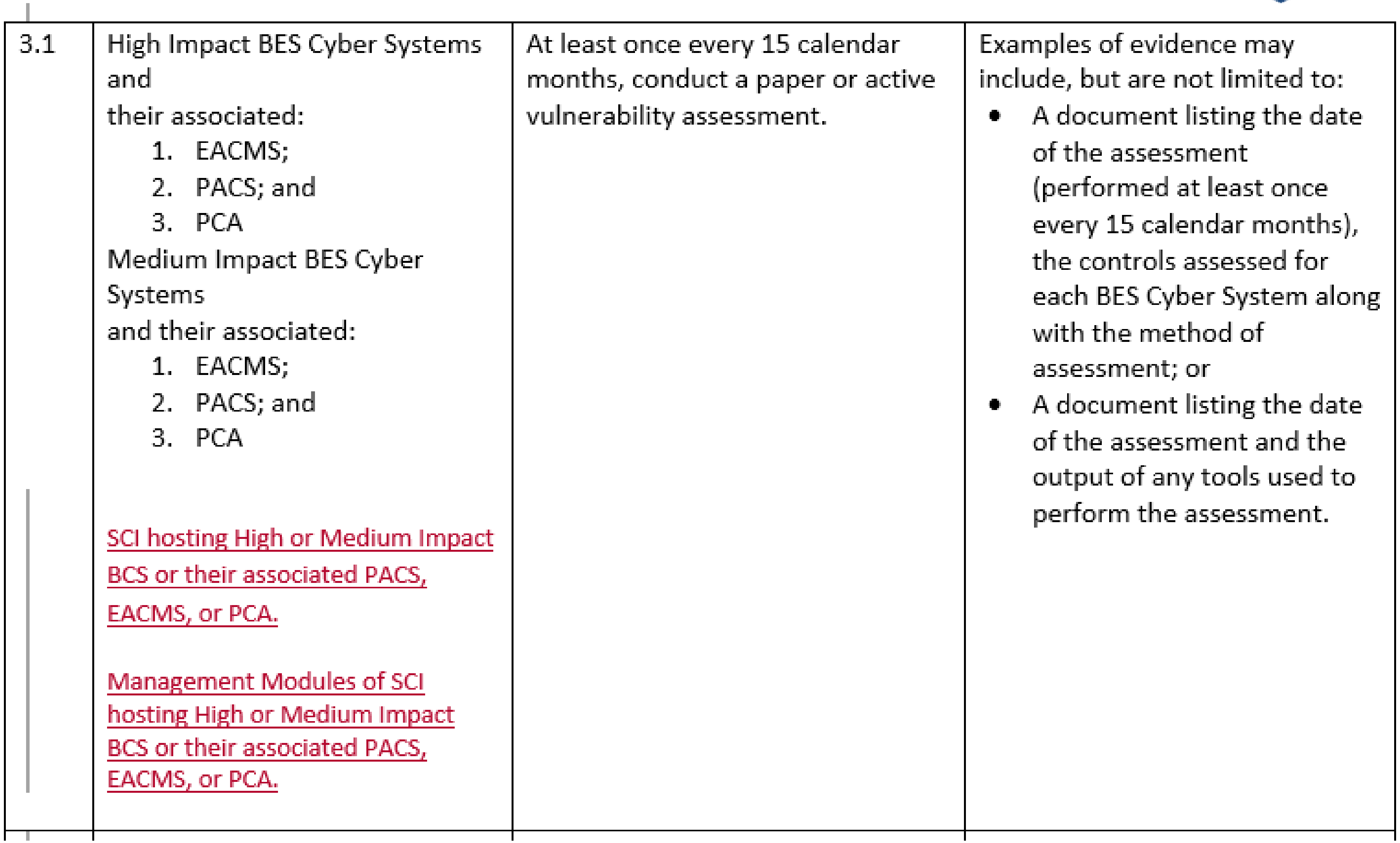
Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

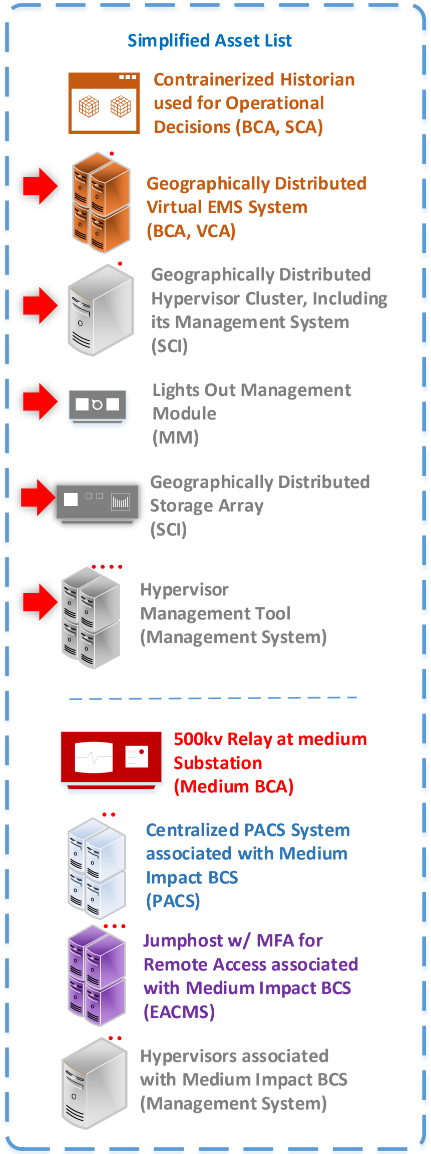
Hypervisors associated with Medium Impact BCS (Management System)



3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA <u>SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.</u> <u>Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.</u>	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

Proposed CIP-010 R3 Part 3.2

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

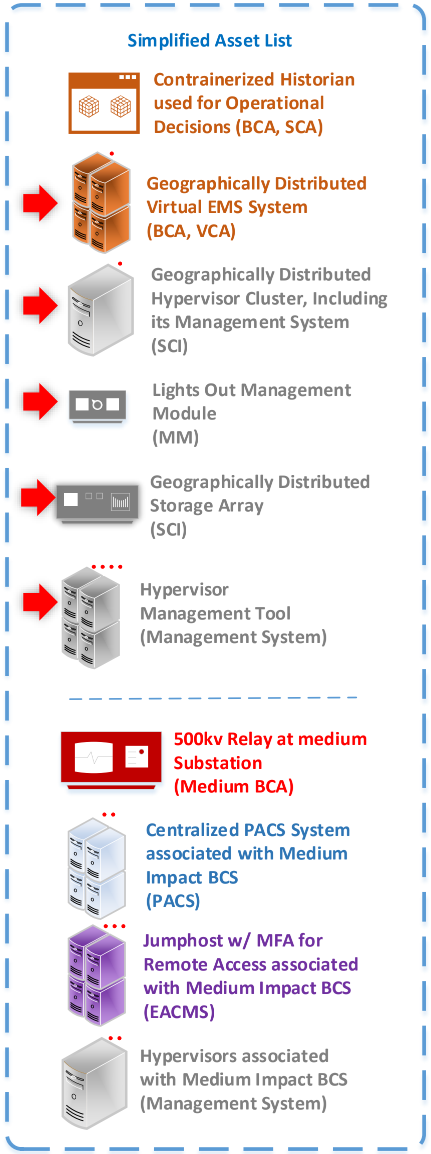
Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

3.2	High Impact BES Cyber Systems SCI hosting High Impact BCS. Management Modules of SCI hosting High Impact BCS.	~~Where technically feasible, a~~At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects~~,~~ and differences with the production environment ~~that models the baseline configuration of the BES Cyber System in a production environment~~; 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.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

Proposed CIP-010 R3 Part 3.3

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

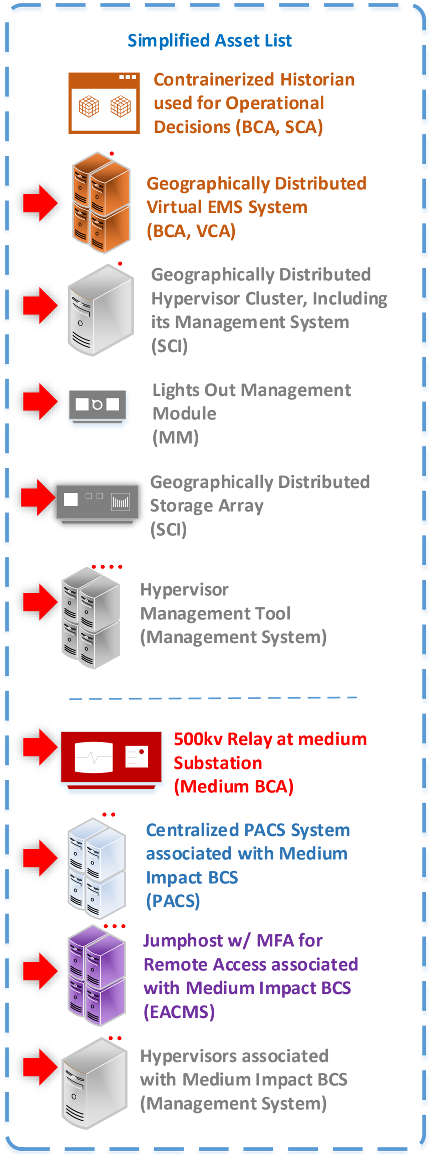
Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)

3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA SCI hosting High Impact BES Cyber Systems or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High Impact BCS or their associated EACMS, or PCA.	Perform an active vulnerability assessment prior to logically connecting an additional applicable Virtual Cyber Asset, Cyber Asset, or Shared Cyber Infrastructure to a production ~~Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset,~~ except for CIP Exceptional Circumstances and ~~like replacements~~ deployments of the same type ~~of Cyber Asset~~ with a previously assessed ~~baseline~~ configuration. The production environment does not include devices being actively remediated and logically isolated.~~that models an existing baseline configuration of the previous or other existing Cyber Asset.~~	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure) and the output of any tools or Management Systems used to perform the assessment.

Proposed CIP-010 R3 Part 3.4

slido.com
#2016-02



Simplified Asset List

Contrainerized Historian used for Operational Decisions (BCA, SCA)

Geographically Distributed Virtual EMS System (BCA, VCA)

Geographically Distributed Hypervisor Cluster, Including its Management System (SCI)

Lights Out Management Module (MM)

Geographically Distributed Storage Array (SCI)

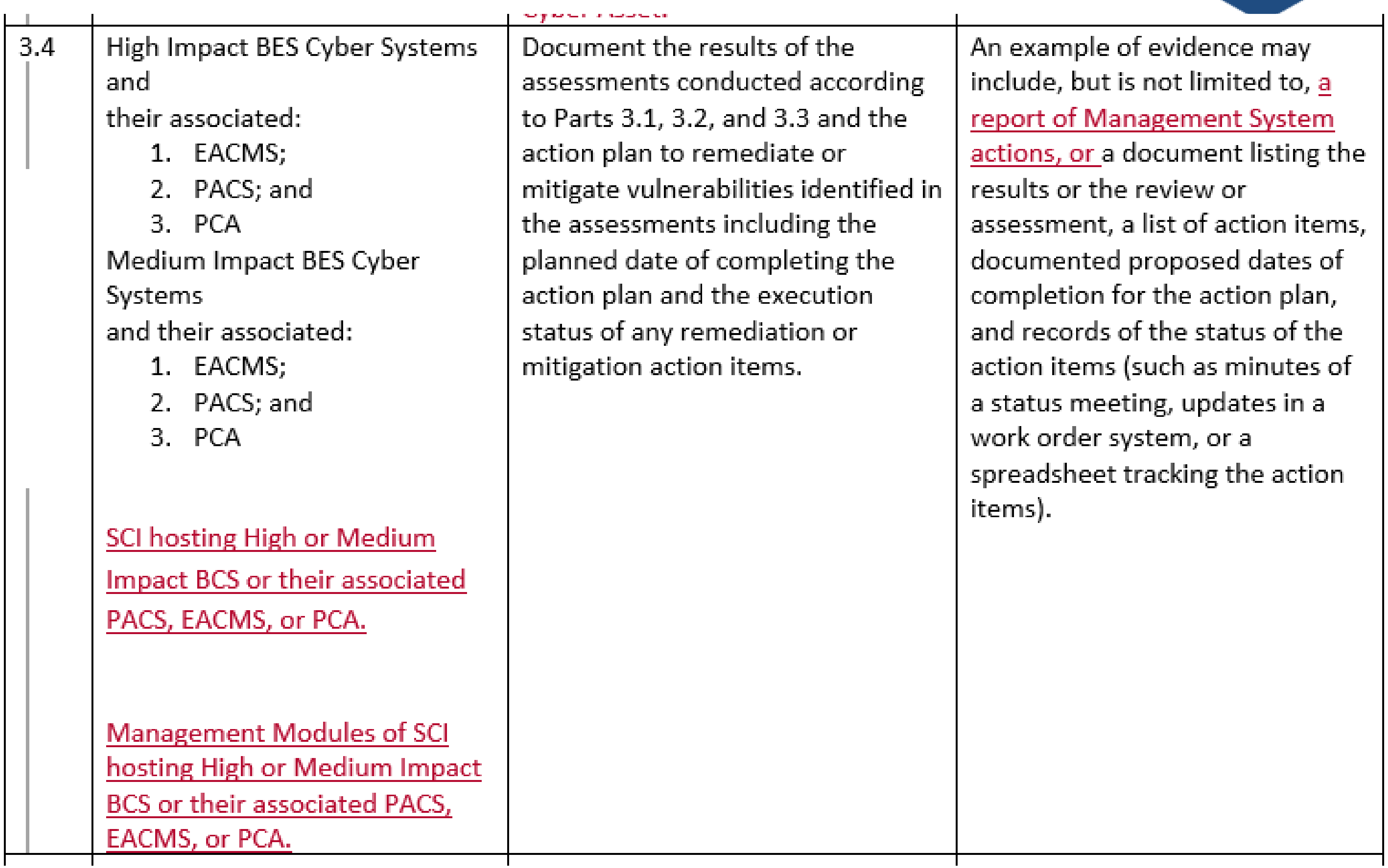
Hypervisor Management Tool (Management System)

500kv Relay at medium Substation (Medium BCA)

Centralized PACS System associated with Medium Impact BCS (PACS)

Jumphost w/ MFA for Remote Access associated with Medium Impact BCS (EACMS)

Hypervisors associated with Medium Impact BCS (Management System)



3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a report of Management System actions, or a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Break

We will return at X:XX p.m. Eastern

Join at
slido.com
#2016-02

RELIABILITY | RESILIENCE | SECURITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Final Survey

Join at

slido.com

#2016-02

RELIABILITY | RESILIENCE | SECURITY

Q&A Objectives

slido.com
#2016-02

- Informal Discussion
  - Via the Q&A feature
  - Chat only goes to the host, not panelists
  - Respond to stakeholder questions
- Other
  - Some questions may require future team consideration
  - Please reference slide number, standard section, etc., if applicable
  - Team will address as many questions as possible
  - Webinar and chat comments are not a part of the official project record
  - Questions regarding compliance with existing Reliability Standards should be directed to ERO Enterprise compliance staff, not the Standard Drafting Team.

slido.com
#2016-02

Questions and Answers