NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2016-02

Modifications to CIP Standards

Webinar on CIP-005 and Definitions Informal Posting

September 12, 2019

RELIABILITY | ACCOUNTABILITY

NERC Antitrust Compliance Guidelines

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

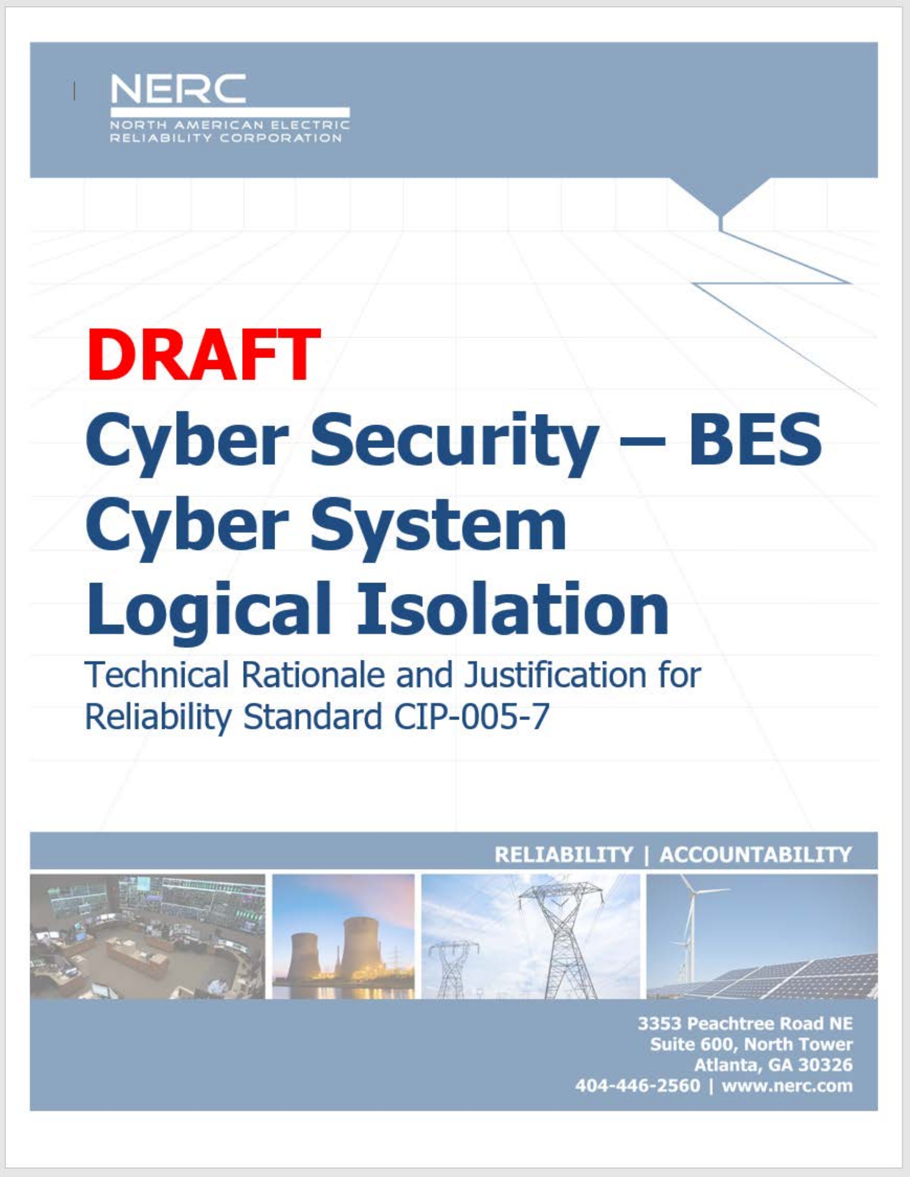
Agenda

- Modifications to CIP Standards Overview
- To the Cloud and Back
- Definitions
- Logical Isolation
- Logical Access Control
- Aligning the Requirements
- CIP-005 Overview
- Management Plane Separation
- Backwards Compatibility
- Q&A

Overview / roadmap, where in the process

- Case for change white paper
- CIP-005 and Definitions informal comment period
- CIP-007/CIP-010 modifications
- Conforming changes to other standards
- Formal posting and ballot

Technical Rationale Document



DRAFT

Cyber Security – BES Cyber System Logical Isolation

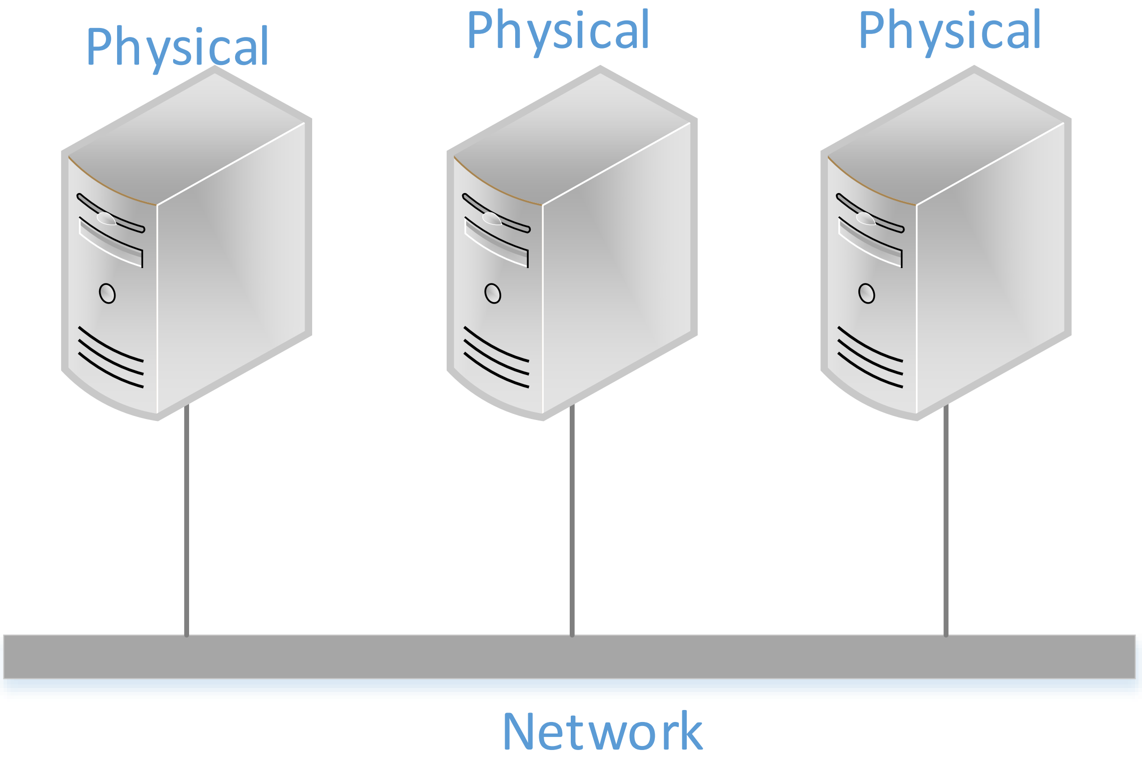
Technical Rationale and Justification for Reliability Standard CIP-005-7

RELIABILITY | ACCOUNTABILITY

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

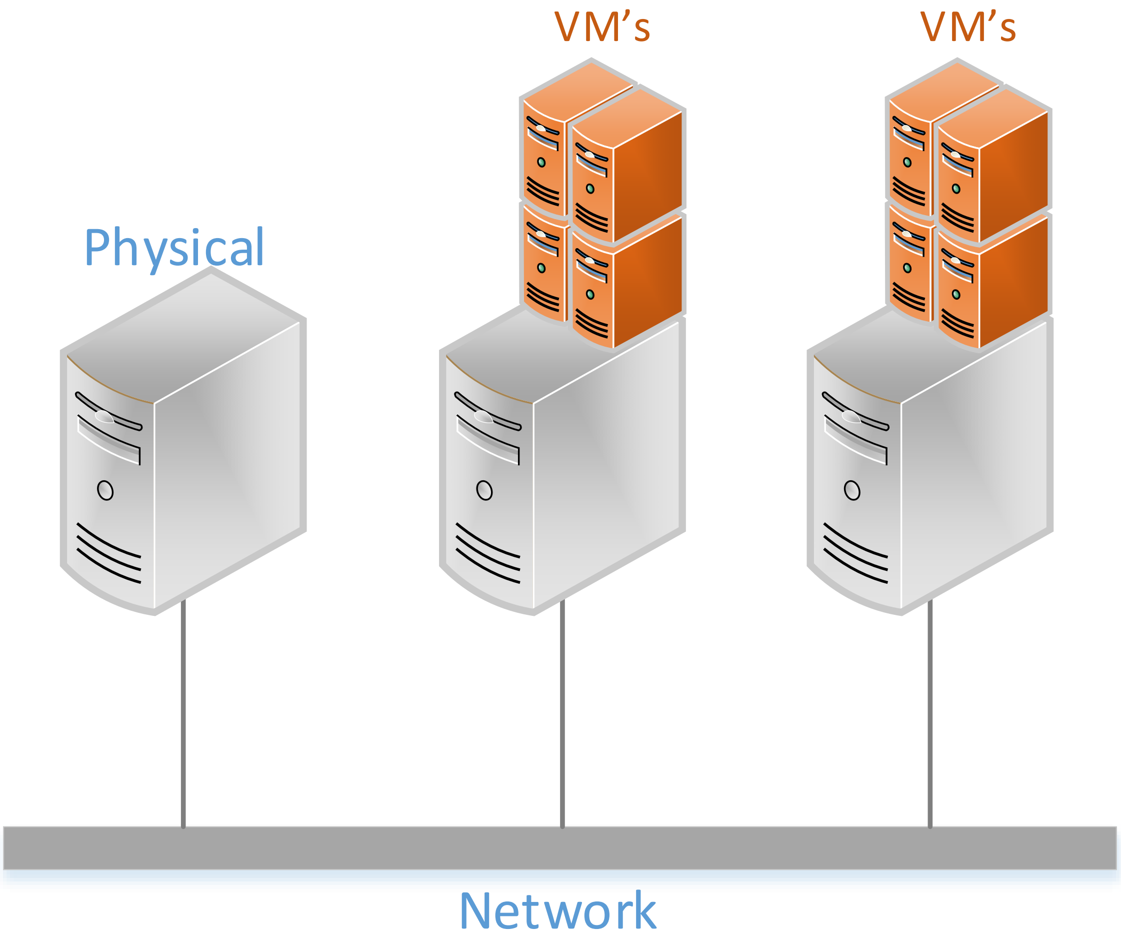
Conventional Infrastructure (Pre-Virtualization)

- IT Industry conventional model ~1994-2005



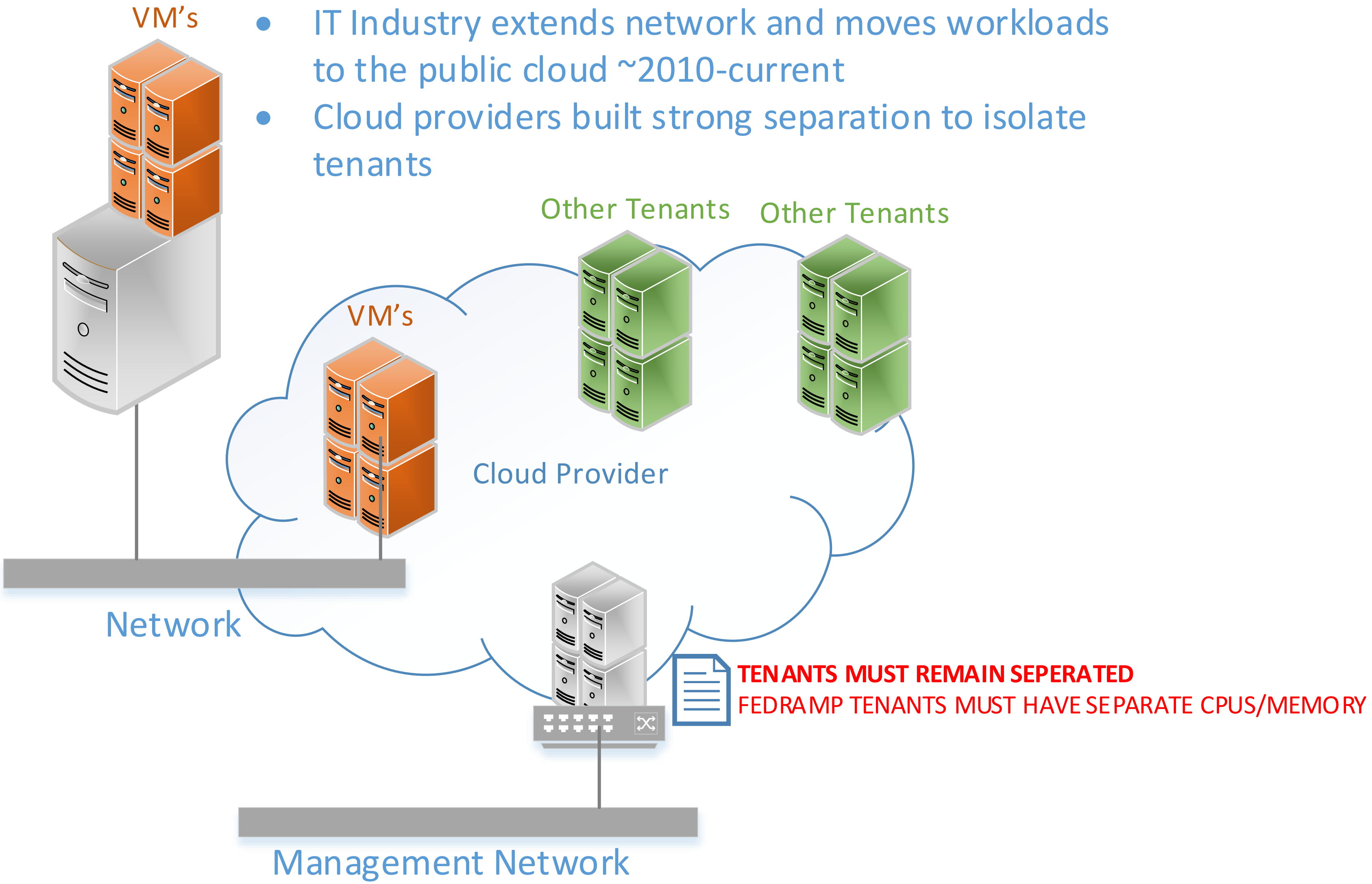
Add VM’s to Current Infrastructure

- IT Industry adds virtualization to existing infrastructure ~2005-2010



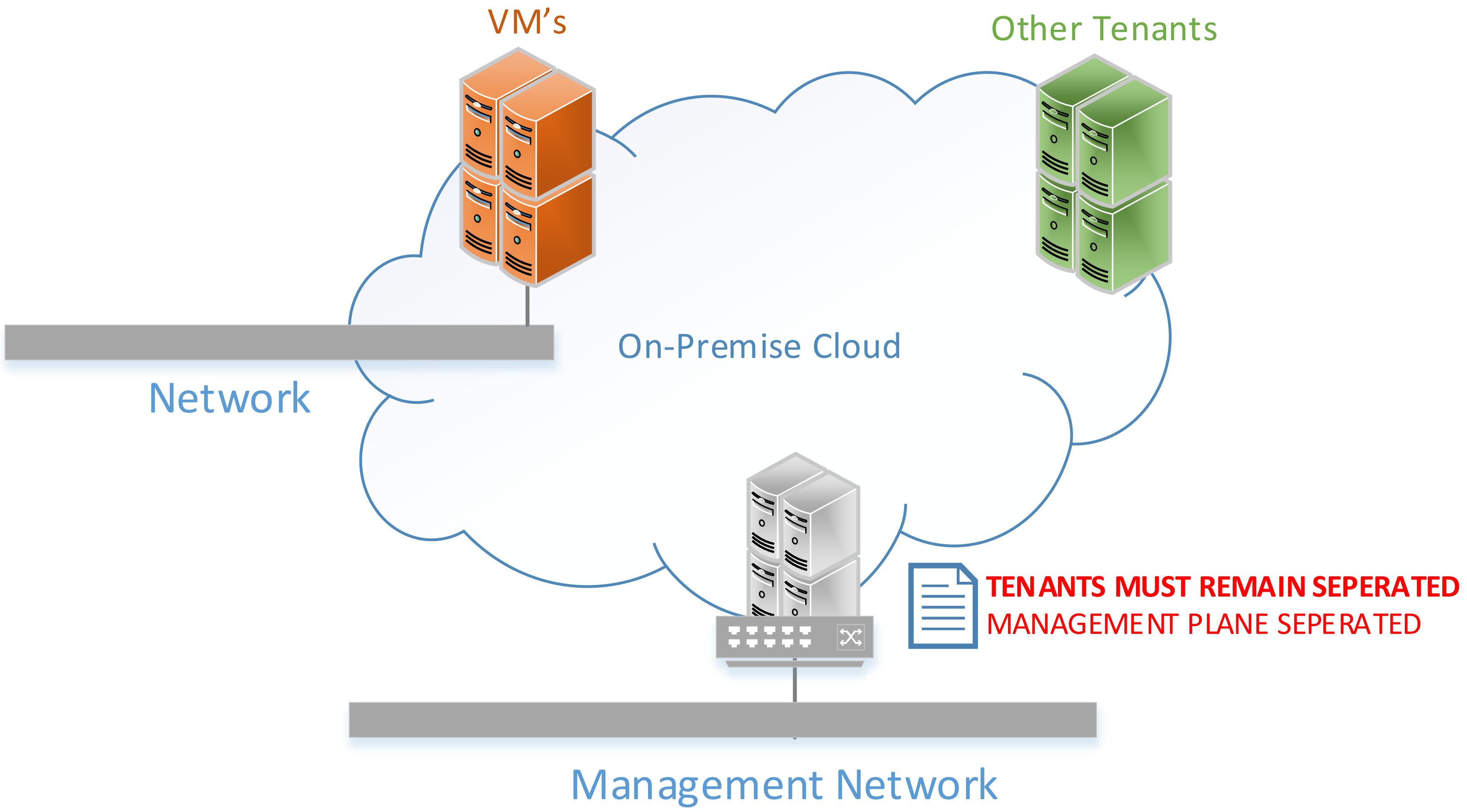
Cloud Extension Example (Electric Industry OT Skipped this)

- IT Industry extends network and moves workloads to the public cloud ~2010-current
- Cloud providers built strong separation to isolate tenants


VM’s
Other Tenants
Other Tenants
VM’s
Cloud Provider
Network
TENANTS MUST REMAIN SEPERATED
FEDRAMP TENANTS MUST HAVE SEPARATE CPUS/MEMORY
Management Network

Cloud Security Implemented Onsite

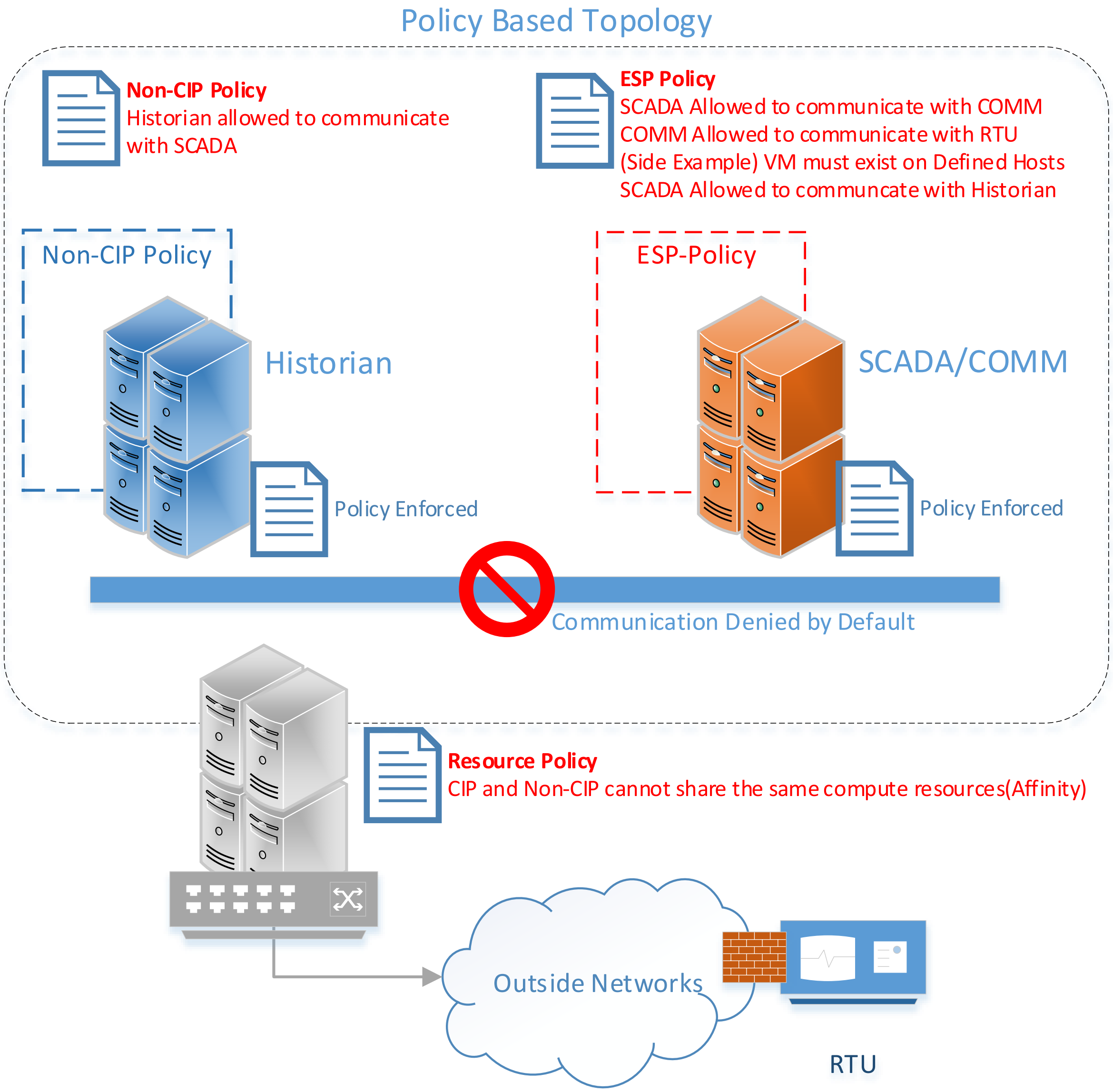
- IT Industry Moves back from cloud and uses management plane seperation strategy to create strong isolation



TENANTS MUST REMAIN SEPERATED

MANAGEMENT PLANE SEPERATED

Policy Based Topology



Policy Based Topology

Non-CIP Policy
Historian allowed to communicate with SCADA

ESP Policy
SCADA Allowed to communicate with COMM
COMM Allowed to communicate with RTU
(Side Example) VM must exist on Defined Hosts
SCADA Allowed to communcate with Historian

Resource Policy
CIP and Non-CIP cannot share the same compute resources(Affinity)

New Definitions

- **Virtual Cyber Asset (VCA):**

  A logical instance of an operating system, firmware, or self-contained application hosted on SCI.

- **Shared Cyber Infrastructure (SCI):**

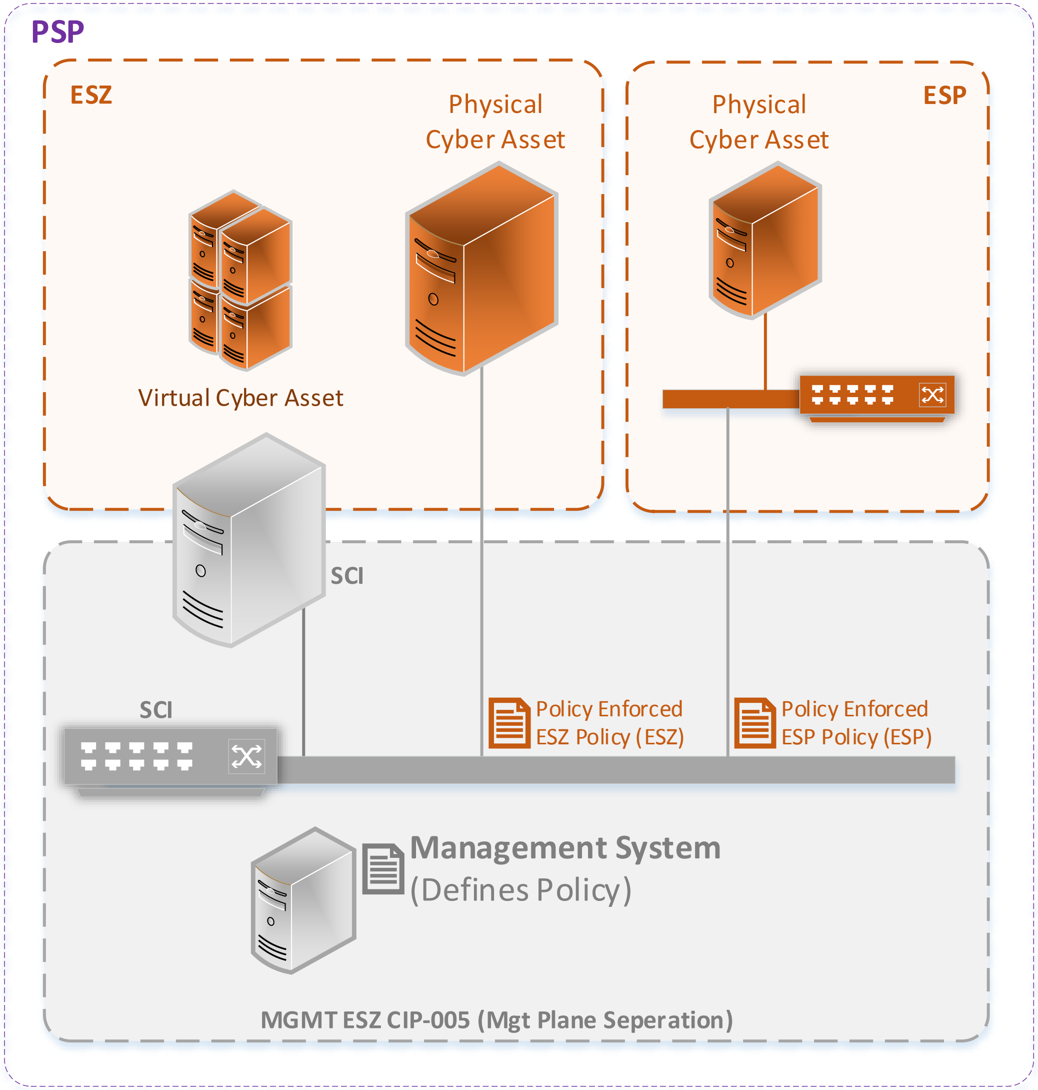
  Programmable electronic devices whose compute, storage (including network transport), or network resources are shared with one or more Virtual Cyber Assets or that perform logical isolation for an ESZ or ESP. This includes its management systems.

- **Electronic Security Zone (ESZ):**

  A segmented section of a network that contains systems and components to create logical isolation.

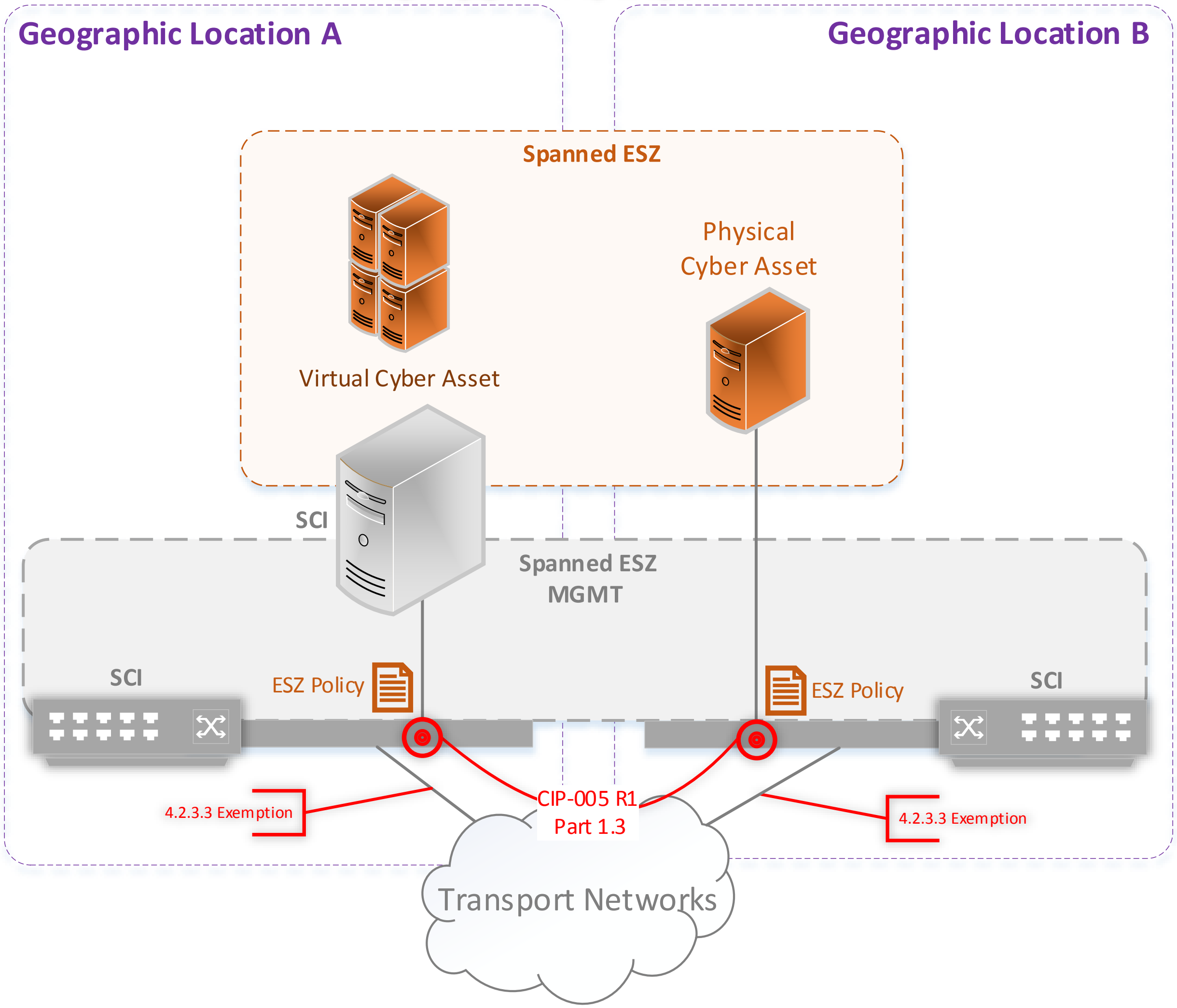
ESP / ESZ Hybrid

ESP/ESZ Hybrid Model



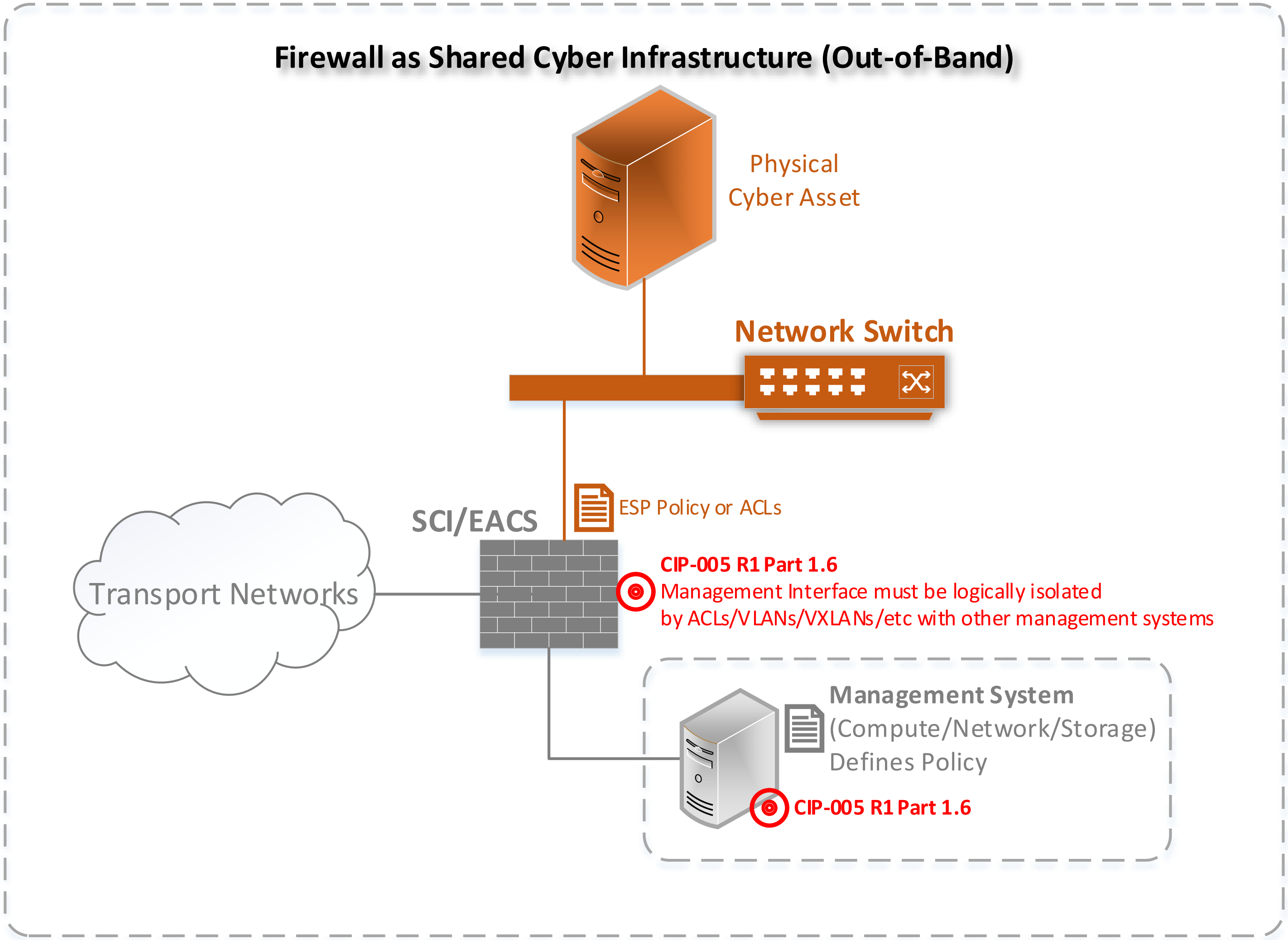
Super ESP / ESZ

Super (Spanned) ESZ/ESP Model



Firewalls as SCI

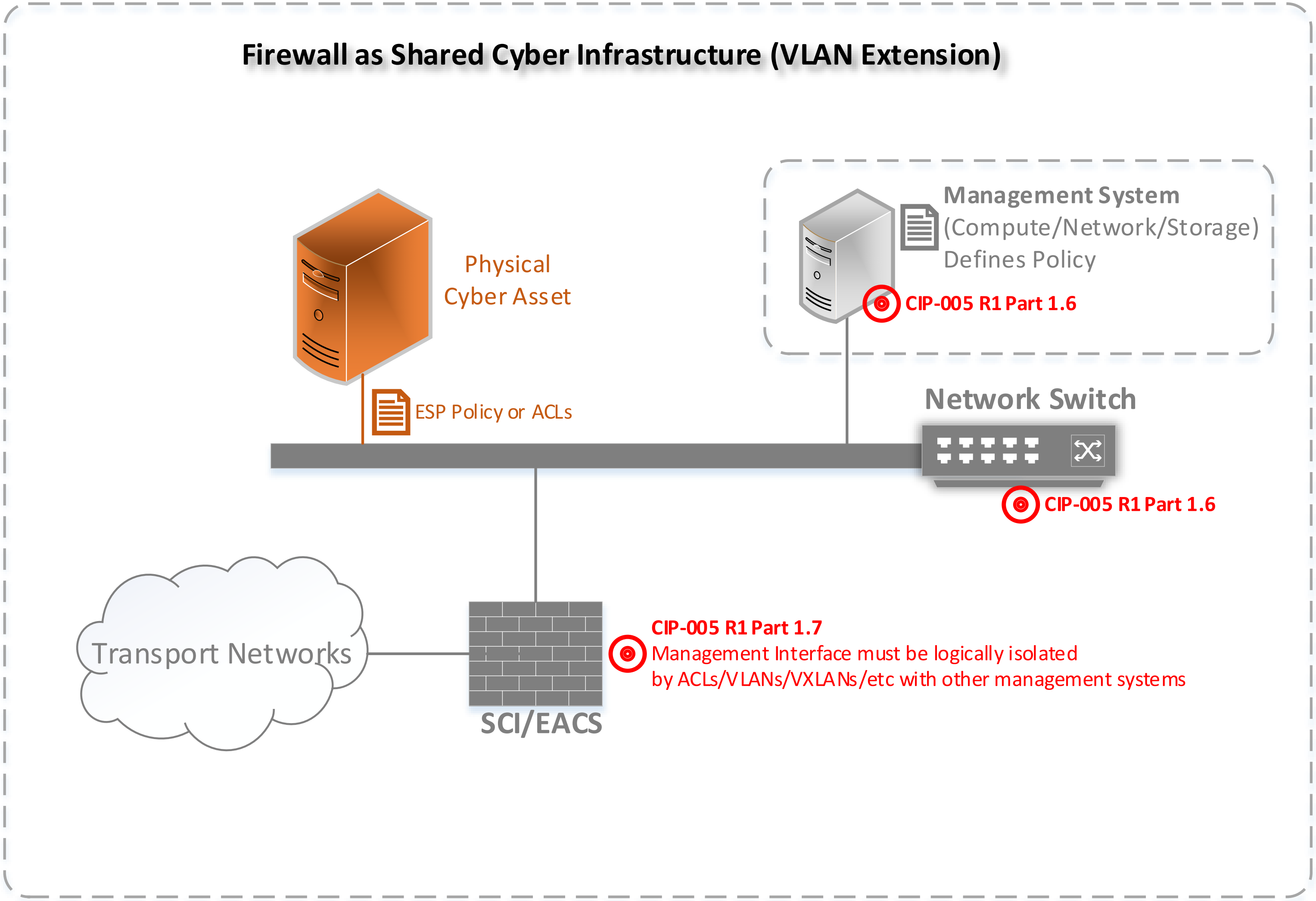
Firewall as Shared Cyber Infrastructure (Out-of-Band)



CIP-005 R1 Part 1.6
Management Interface must be logically isolated by ACLs/VLANs/VXLANs/etc with other management systems

CIP-005 R1 Part 1.6

Switches for Access Control

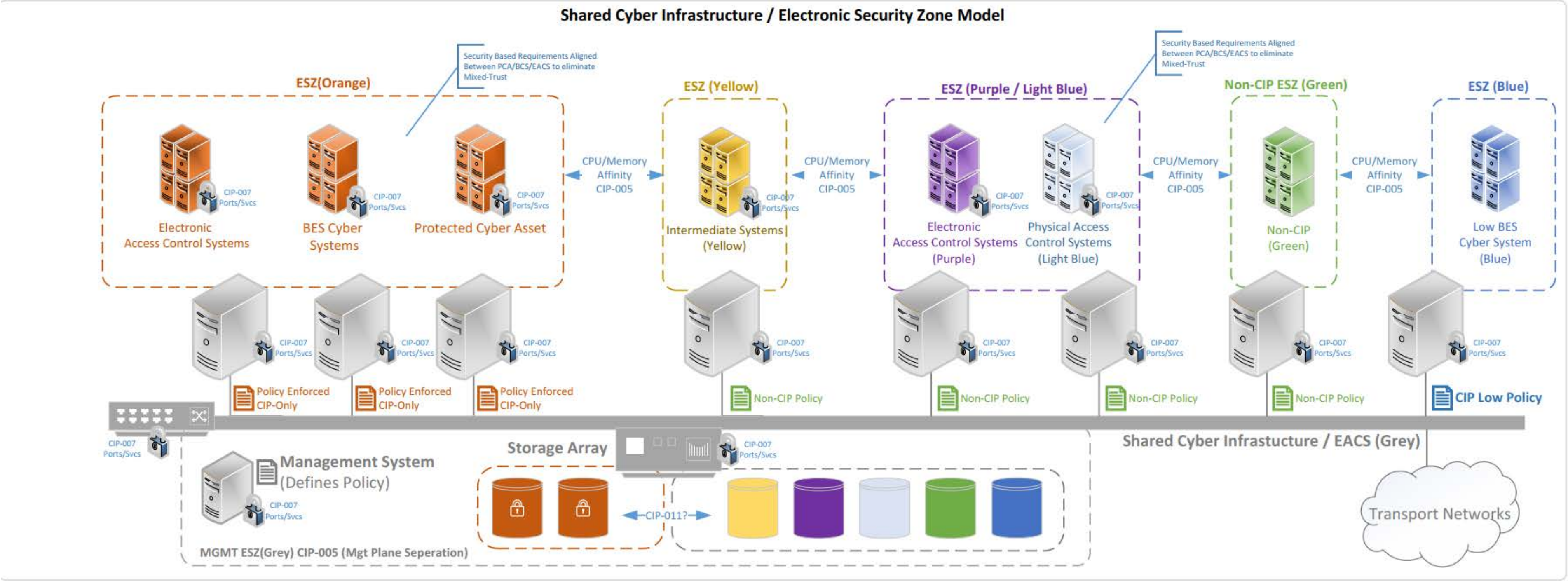


CIP-005 R1 Part 1.7
Management Interface must be logically isolated
by ACLs/VLANs/VXLANs/etc with other management systems

Handling “Mixed Trust”

- Sharing hardware resources introduces new risks from hardware based vulnerabilities
- Introducing requirements on what can reside within the same ESP/ESZ on the same hardware
- Aligning requirements WITHIN an ESP/ESZ
- Requiring affinity rules BETWEEN ESP/ESZs of different trust levels

Handling “Mixed Trust”


Shared Cyber Infrastructure / Electronic Security Zone Model
Security Based Requirements Aligned Between PCA/BCS/EACS to eliminate Mixed-Trust
ESZ(Orange)
Electronic Access Control Systems
CIP-007 Ports/Svcs
BES Cyber Systems
CIP-007 Ports/Svcs
Protected Cyber Asset
CIP-007 Ports/Svcs
CPU/Memory Affinity CIP-005
ESZ (Yellow)
Intermediate Systems (Yellow)
CIP-007 Ports/Svcs
CPU/Memory Affinity CIP-005
ESZ (Purple / Light Blue)
Security Based Requirements Aligned Between PCA/BCS/EACS to eliminate Mixed-Trust
Electronic Access Control Systems (Purple)
CIP-007 Ports/Svcs
Physical Access Control Systems (Light Blue)
CIP-007 Ports/Svcs
CPU/Memory Affinity CIP-005
Non-CIP ESZ (Green)
Non-CIP (Green)
CPU/Memory Affinity CIP-005
ESZ (Blue)
Low BES Cyber System (Blue)
CIP-007 Ports/Svcs
Policy Enforced CIP-Only
Policy Enforced CIP-Only
Policy Enforced CIP-Only
Non-CIP Policy
Non-CIP Policy
Non-CIP Policy
Non-CIP Policy
CIP Low Policy
CIP-007 Ports/Svcs
Storage Array
CIP-007 Ports/Svcs
Shared Cyber Infrastucture / EACS (Grey)
Management System (Defines Policy)
CIP-007 Ports/Svcs
CIP-011?
MGMT ESZ(Grey) CIP-005 (Mgt Plane Seperation)
Transport Networks

ERC and IRA definitions

- Clarity for serial to IP conversion scenarios
  - Serial, non-routable protocol Cyber Asset that has no ESP
  - Serial converted to IP upstream
- Proposed changes to IRA definition so it is NOT dependent on ERC
- Conforming changes to ERC only

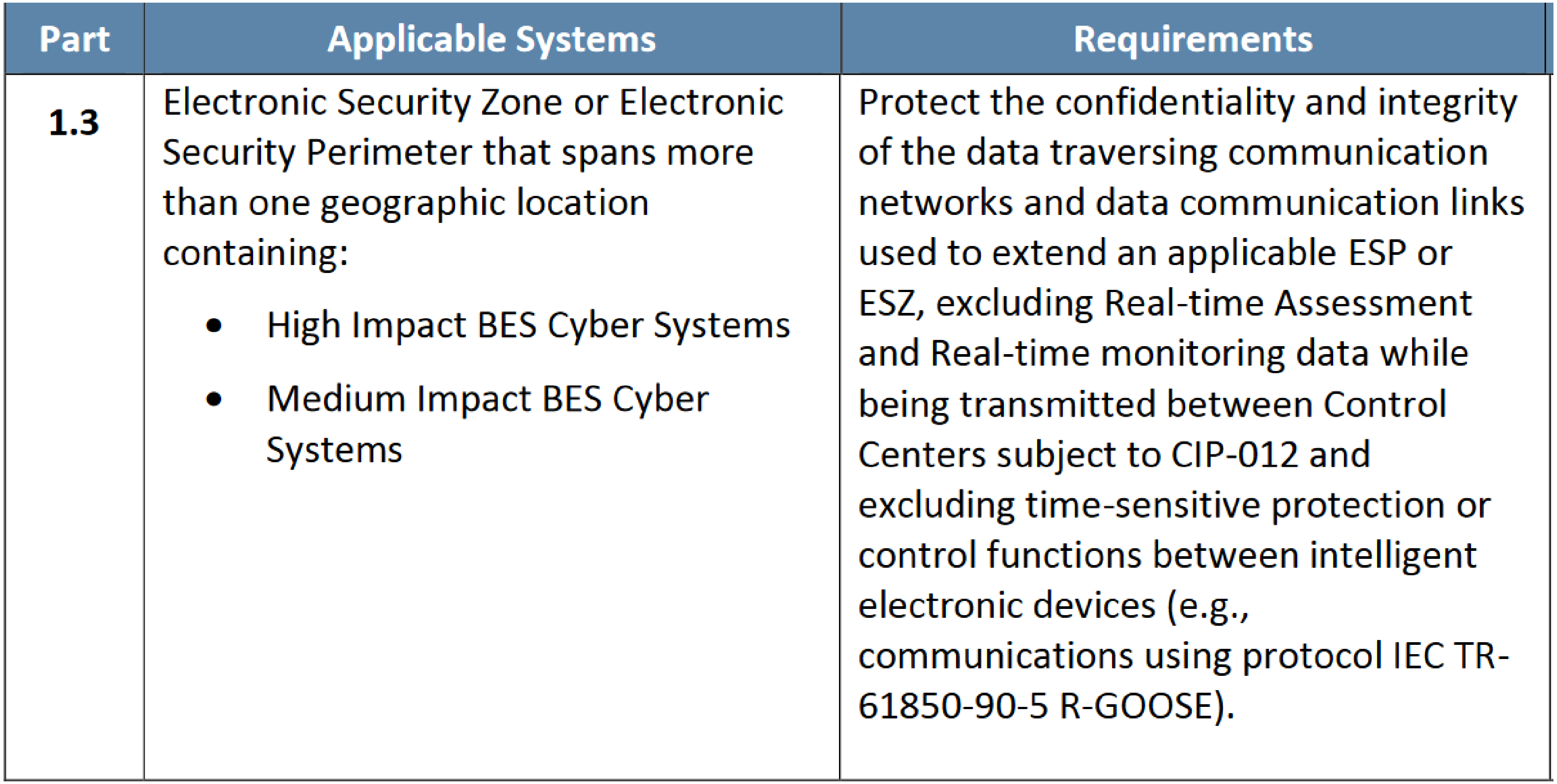
Proposed CIP-005-7

Part	Applicable Systems	Requirements
1.1	High Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems connected to a network via routable protocol and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	All applicable systems shall reside within one or more defined ESPs or ESZs.

Proposed CIP-005-7

Part	Applicable Systems	Requirements
1.2	Electronic Security Perimeters and Electronic Security Zones created in Part 1.1.	Require inbound and outbound logical access permissions, including the reason for granting access, and deny all other logical access by default. Excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Proposed CIP-005-7

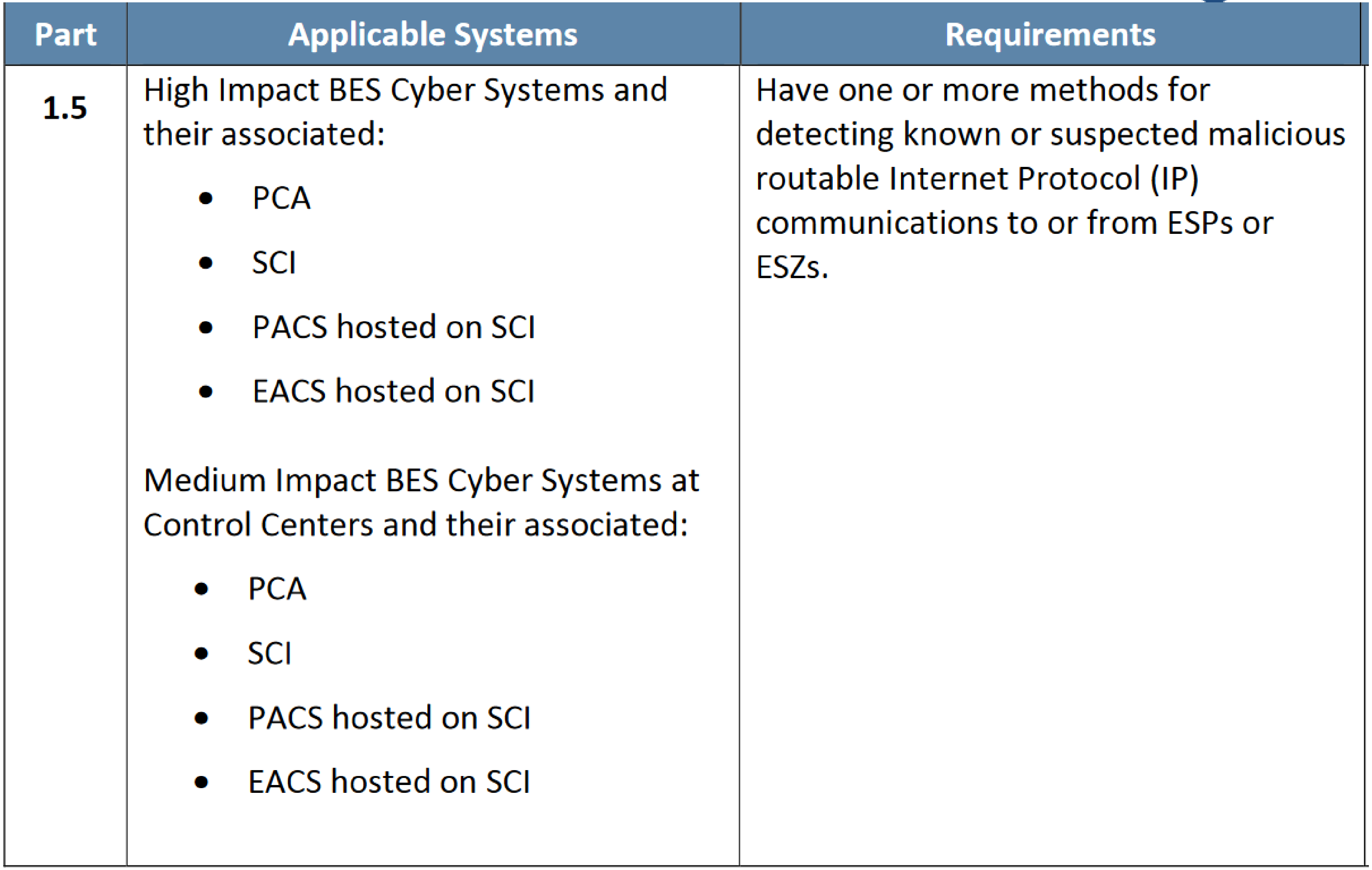


Part	Applicable Systems	Requirements
1.3	Electronic Security Zone or Electronic Security Perimeter that spans more than one geographic location containing: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems	Protect the confidentiality and integrity of the data traversing communication networks and data communication links used to extend an applicable ESP or ESZ, 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).

Proposed CIP-005-7

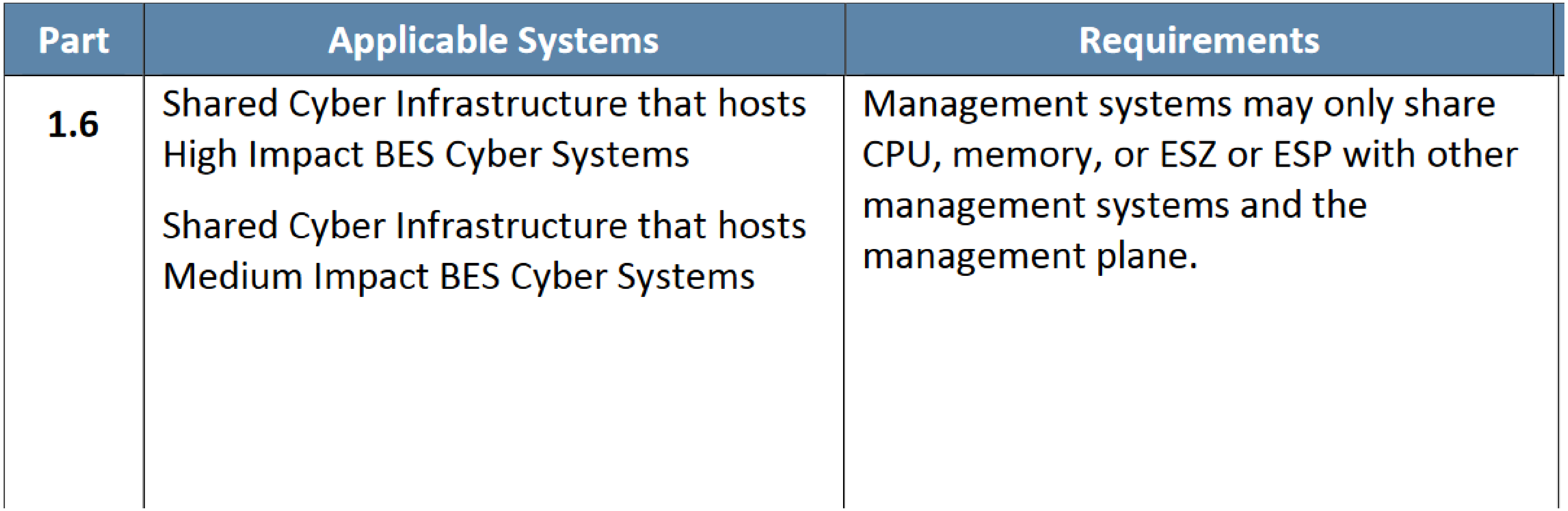
Part	Applicable Systems	Requirements
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	Perform authentication when establishing Dial-up Connectivity with applicable systems, per system capability.

Proposed CIP-005-7



Part	Applicable Systems	Requirements
1.5	High Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	Have one or more methods for detecting known or suspected malicious routable Internet Protocol (IP) communications to or from ESPs or ESZs.

Proposed CIP-005-7



Part	Applicable Systems	Requirements
1.6	Shared Cyber Infrastructure that hosts High Impact BES Cyber Systems Shared Cyber Infrastructure that hosts Medium Impact BES Cyber Systems	Management systems may only share CPU, memory, or ESZ or ESP with other management systems and the management plane.

Requirement R2

R2 Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in CIP-005-7 Table R2 –Remote Access Management for all remote access that originates from outside of any of the entities’ ESP’s or ESZ’s containing high or medium impact BES Cyber Systems or associated SCI. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]

Proposed CIP-005-7

CIP-005-7 Table R2 - Remote Access Management		
Part	**Applicable Systems**	**Requirements**
2.1	High Impact BES Cyber Systems and their associated: • PCA • SCI Medium Impact BES Cyber Systems with IRA and their associated: • PCA • SCI	Ensure that Interactive Remote Access is through an Intermediate System that is not inside an applicable ESP or ESZ.

Proposed CIP-005-7

CIP-005-7 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements
2.2	Intermediate Systems associated with High Impact BES Cyber Systems. Intermediate Systems associated with Medium Impact BES Cyber Systems.	Protect the confidentiality and integrity of Interactive Remote Access between the client and the Intermediate System.

Proposed CIP-005-7

CIP-005-7 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements
2.3	Intermediate Systems associated with High Impact BES Cyber Systems. Intermediate Systems associated with Medium Impact BES Cyber Systems.	Require multi-factor authentication to IS.

Proposed CIP-005-7

CIP-005-7 Table R2 – Remote Access Management		
Part	**Applicable Systems**	**Requirements**
2.4	High Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).

Proposed CIP-005-7

CIP-005-7 Table R2 – Remote Access Management		
Part	**Applicable Systems**	**Requirements**
2.5	High Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).

Proposed CIP-005-7

CIP-005-7 Table R2 – Remote Access Management		
Part	**Applicable Systems**	**Requirements**
2.6	Intermediate Systems that are hosted on SCI and are associated with High Impact BES Cyber Systems. Intermediate Systems that are hosted on SCI and are associated with Medium Impact BES Cyber Systems.	IS may only share CPU, memory, or ESZ or ESP with other IS.

EACMS and PACS split

- Different Risks
  - Access CONTROL Systems – Unauthorized access
  - Access LOGGING/MONITORING Systems – Information Leakage
- Coordinate with other CIP SDT's that may require these definitions

Backwards Compatibility

- Create virtualization specific controls for:
  - ESZ, SCI, Virtualized BCAs, EACMS, PACS, PCAs etc.
- Objective Requirements
  - Logically isolate vs. create an EAP at a cyber asset interface
- Be aware of traditional firewalls as SCI

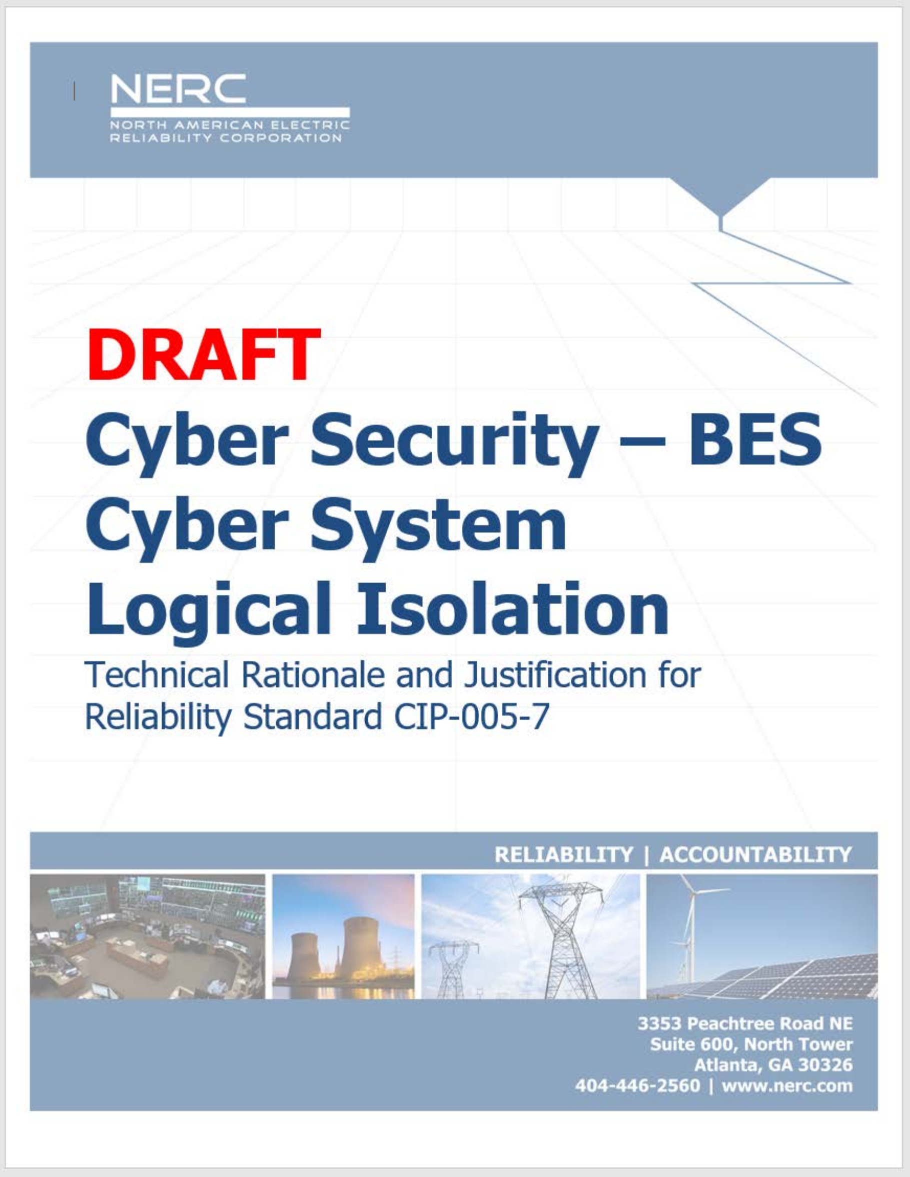
Concepts - Unchanged

- Cyber Asset (CA)
- BES Cyber Asset (BCA)
- BES Cyber System (BCS)
- Electronic Security Perimeter (ESP)
- External Routable Connectivity (ERC)

Path Forward

- Virtualization specific changes within CIP-007/CIP-010
  - Dormant VMs
  - Parent images/VDI
  - Remediation VLANs for vulnerability assessments, etc.
- Technology agnostic requirements

Technical Rationale Document



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security – BES
Cyber System
Logical Isolation

Technical Rationale and Justification for
Reliability Standard CIP-005-7

RELIABILITY | ACCOUNTABILITY

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

Resources

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

Questions and Answers