NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Management of Shared Cyber Infrastructure

Project 2016-02 CIP Standards – Management Virtualization

Project 2016-02 CIP Standards Drafting Team
August 6, 2020

RELIABILITY | RESILIENCE | SECURITY




NERC Antitrust

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.

Questions

Please use the Q&A feature in WebEx to ask any relevant questions during the presentation. We will be holding questions until the end of the presentation.

Disclaimer

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

NOT

***REQUIRE** Them*

Agenda

- Management Plane/ Data Plane Concepts
- Protecting the Management of SCI
- SCI Management
- Management Systems, Management Interfaces and Management Modules
- Changes in CIP-005, CIP-007 and CIP-010
- Backwards Compatibility

Management Plane / Data Plane

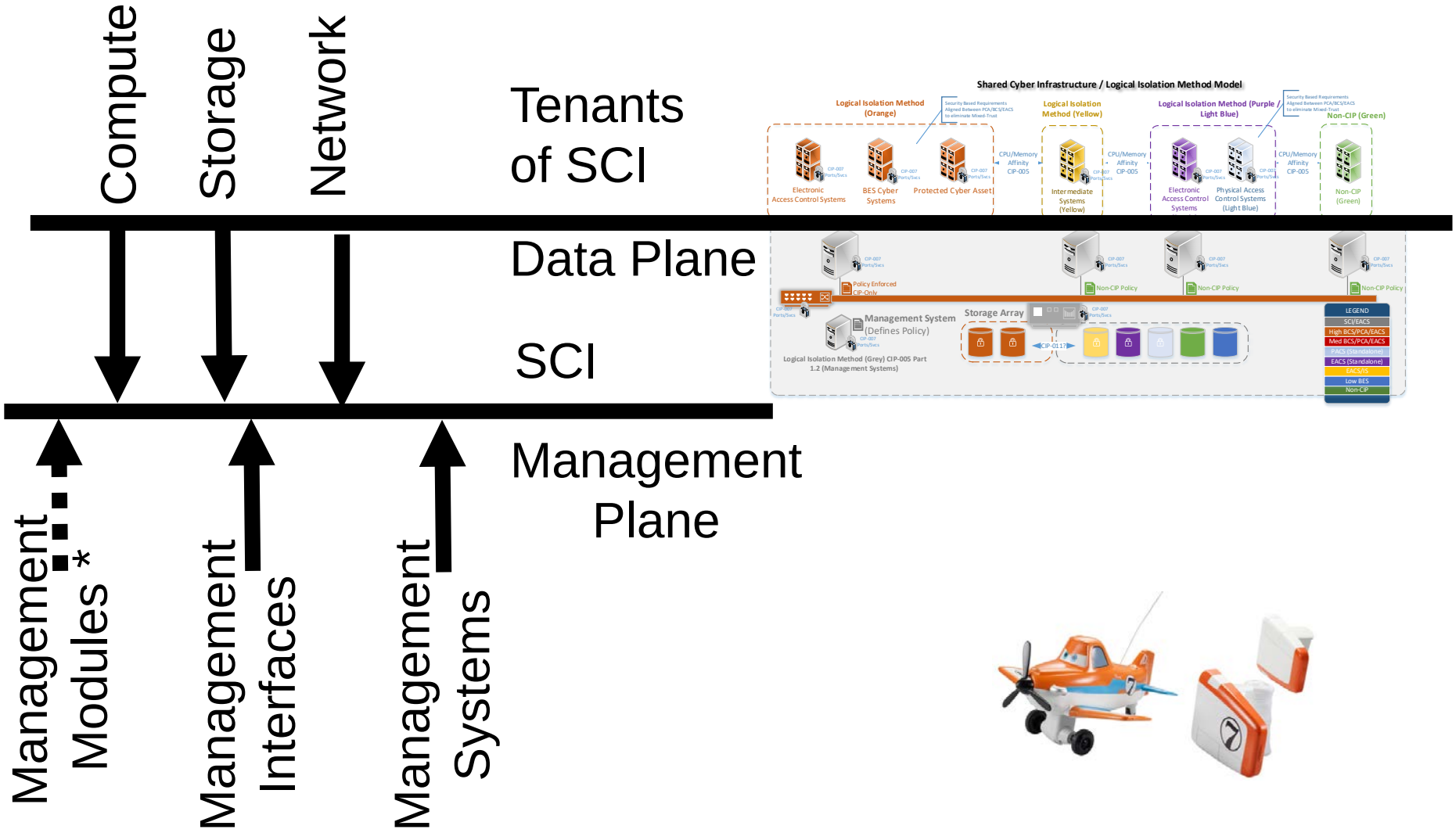
- What is Shared Cyber Infrastructure (SCI)?
  - One or more programmable electronic devices (excluding Management Modules) and their software that share their computer or storage resources with one or more Virtual Cyber Assets or other Cyber Assets; including Management Systems used to initialize, deploy, or configure the SCI.
- The last posting in Aug 2019 introduced the concepts of the SCI Management Plane and SCI Data Plane.

Security Objectives for the Protection of SCI

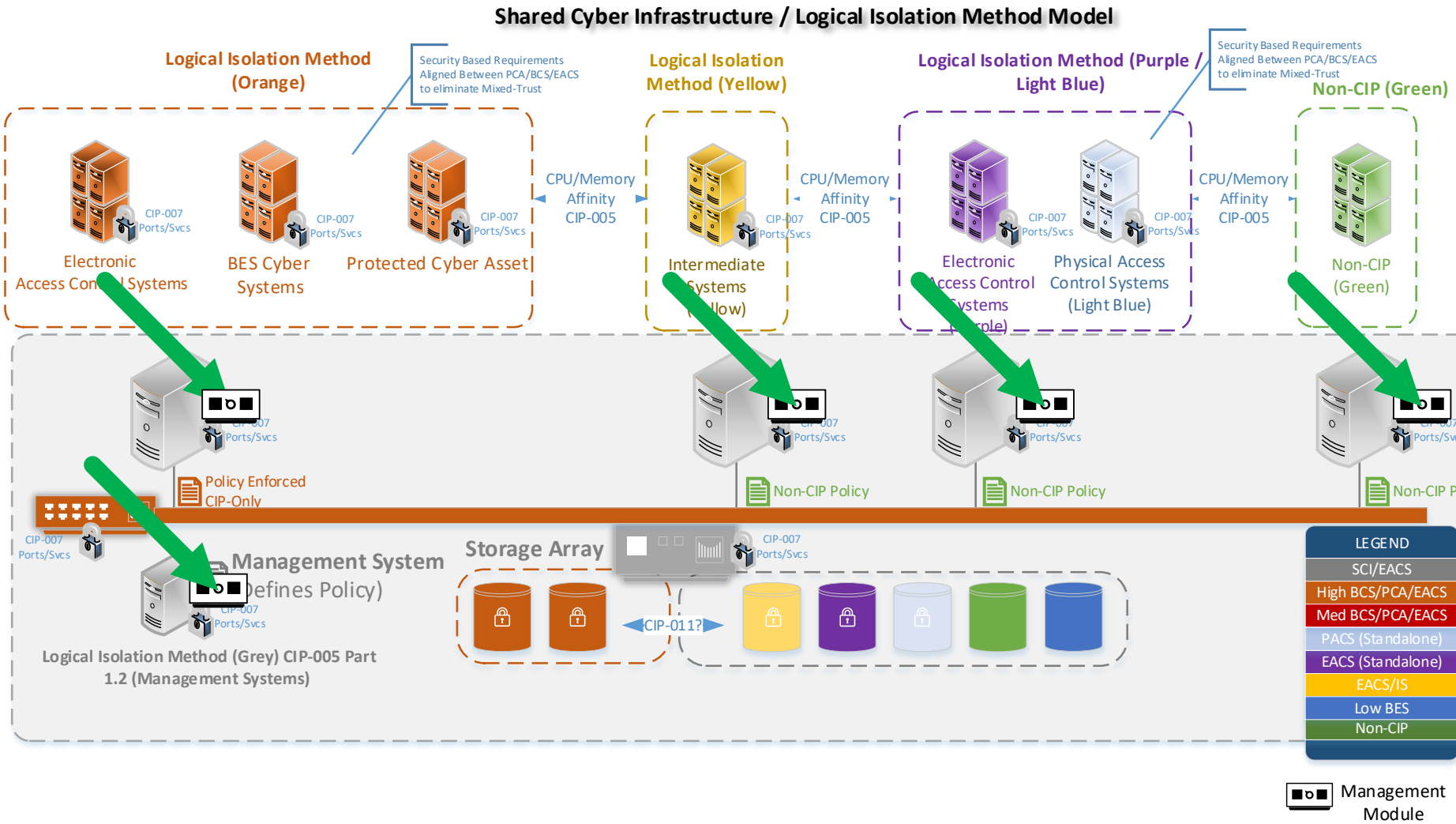
- Protect the SCI at least as well as the highest rated tenants running on that SCI (i.e. BES Cyber Systems)
  - How - The addition of SCI as an Applicable System in the CIP Standards
- Protect the ability to configure or manage SCI from the tenants of that SCI
  - How - The addition of new technical objectives around the concepts expressed in the “Management Plane”

Management Plane / Data Plane

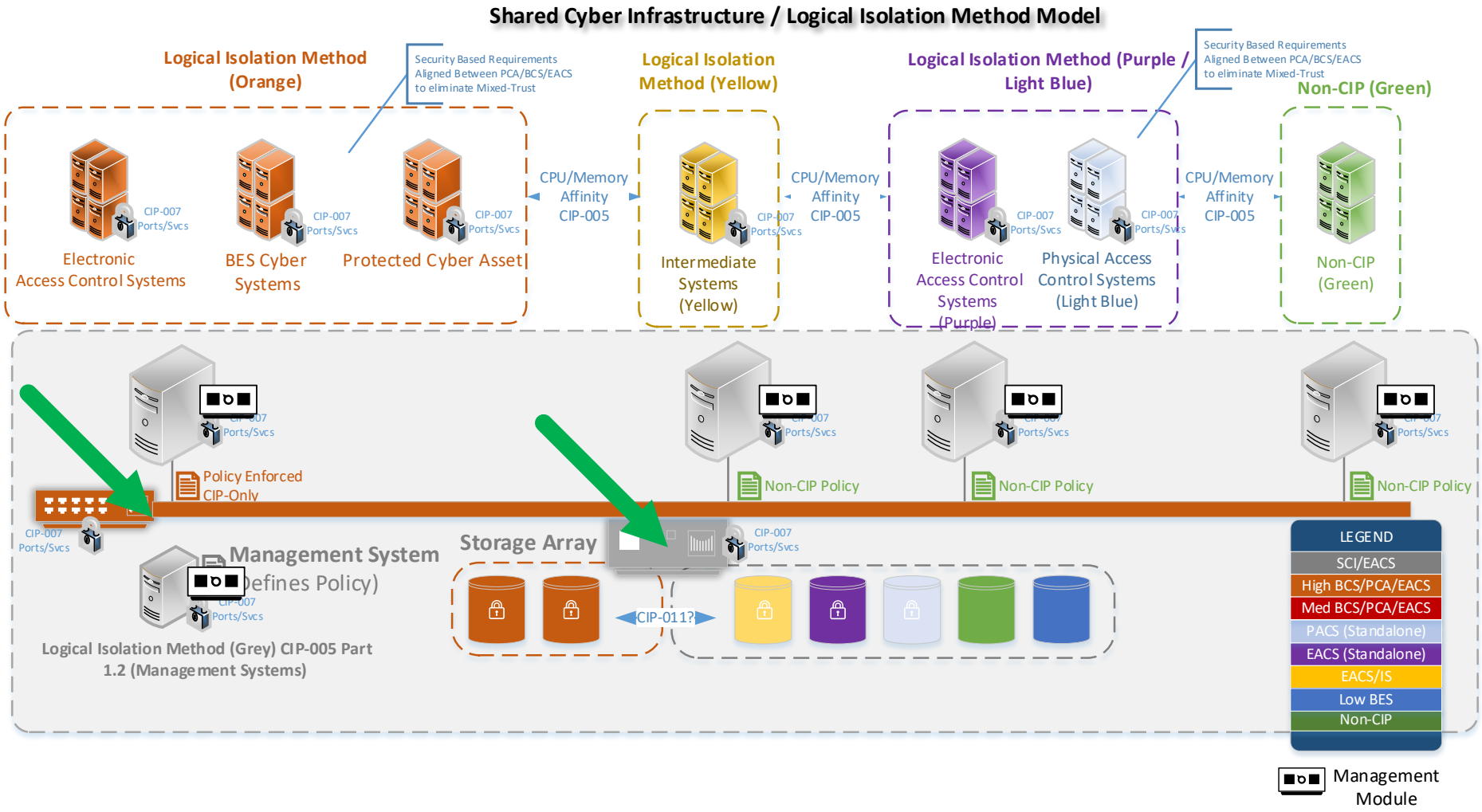
Virtual Cyber Assets or Cyber Assets



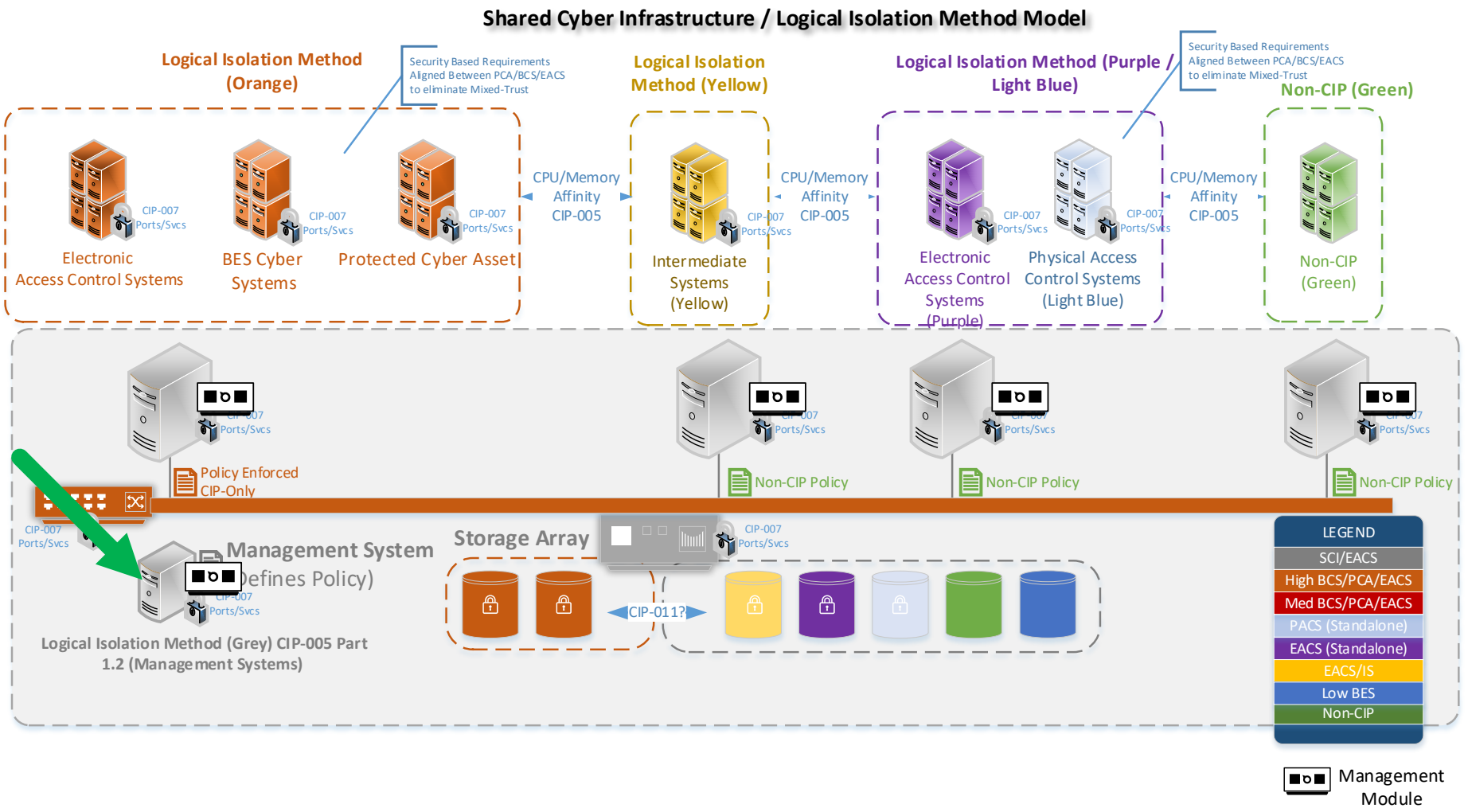
Management Modules



Management Interface



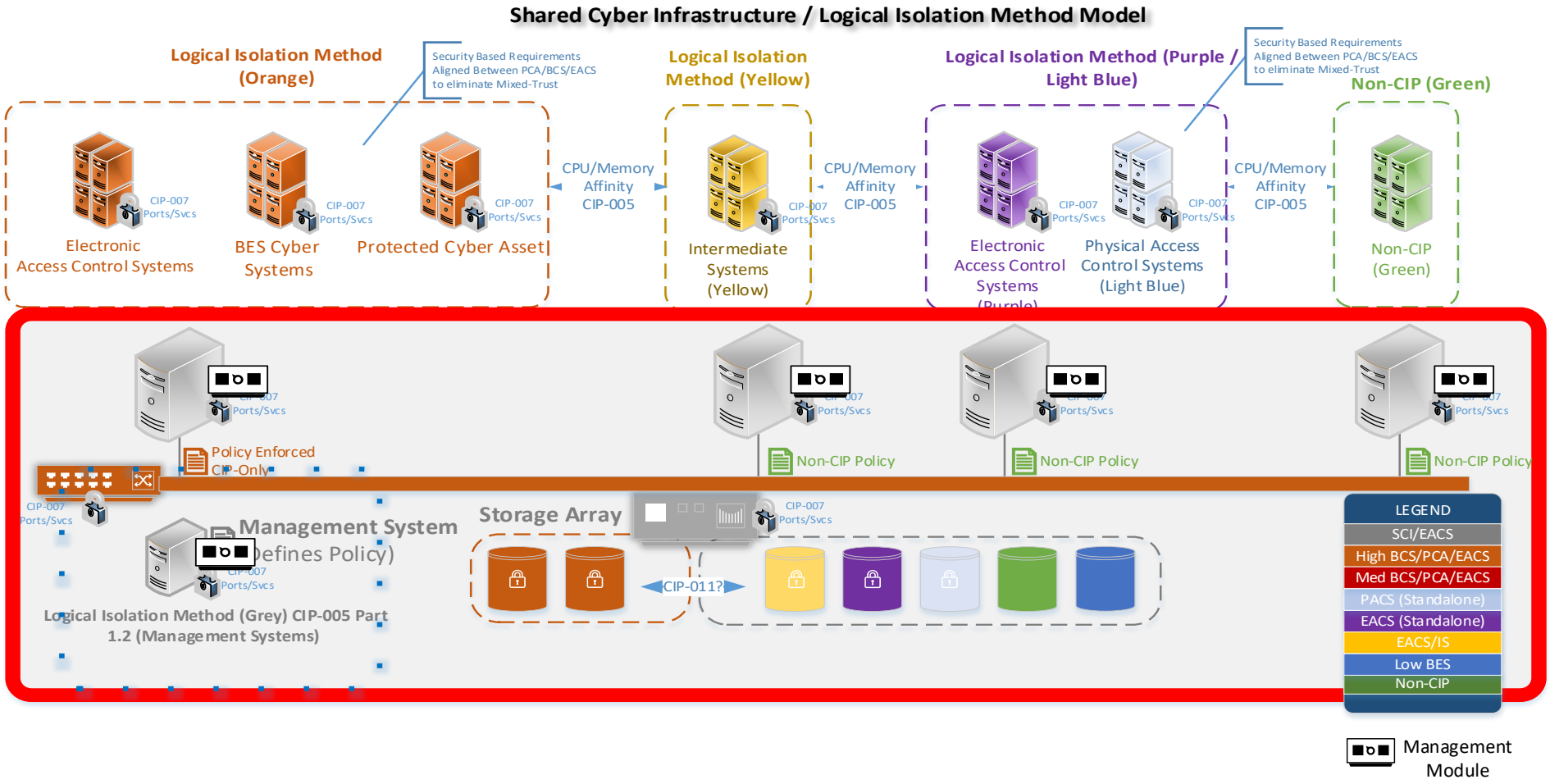
Management System



Changes in CIP-005

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.	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)

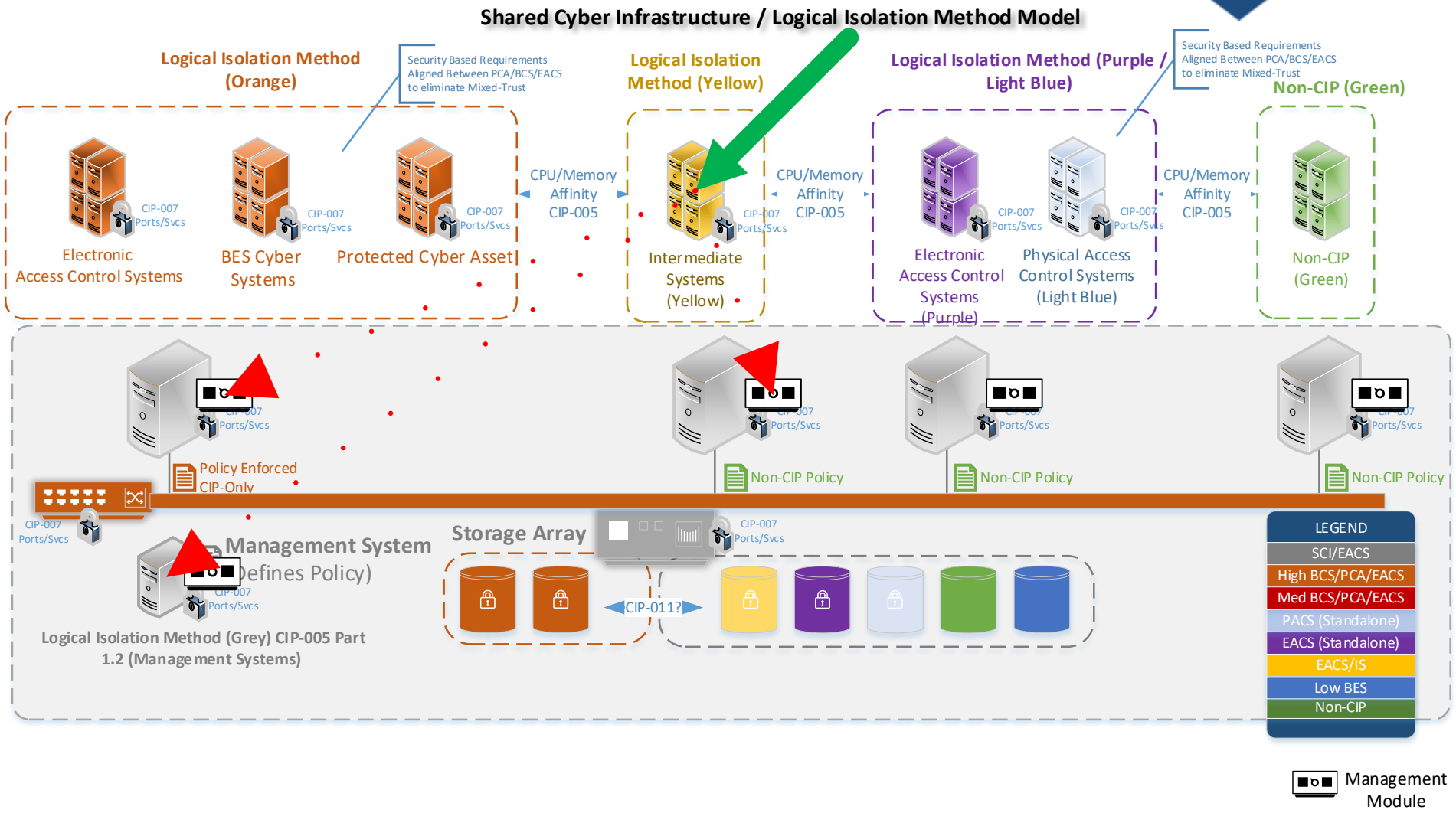
Changes in CIP-005



Changes in CIP-005

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 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	Ensure that authorized Interactive Remote Access is through an Intermediate System.	Examples of evidence may include, but are not limited to, network, diagrams, architecture documents, or Management Systems reports that show all IRA is through an IS.

Changes in CIP-005



Changes in CIP-007

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated PCA. Medium Impact BES Cyber Systems at Control Centers and their associated PCA. SCI at Control Centers hosting High or Medium Impact BCS or their associated PCA. Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA 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.

Changes in CIP-007

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
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

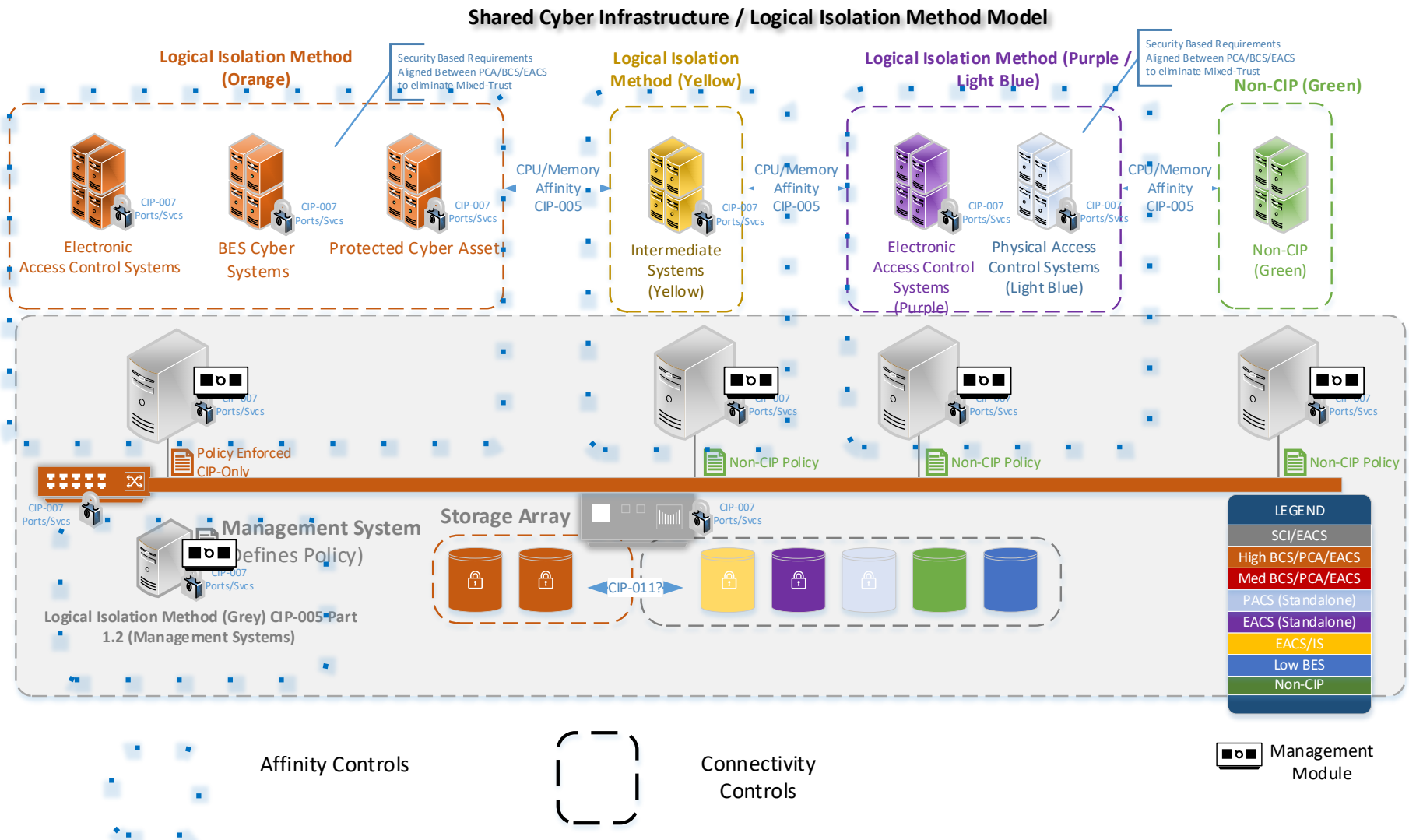
Changes in CIP-007

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
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. 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 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.

Changes in CIP-010

CIP-010-4 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
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. Operating system(s) or firmware or images used to derive operating systems or firmware; 2. Commercially available or open-source application software including Self-Contained Applications ; 3. Custom software installed including Self-Contained Applications; 4. Logical network connectivity; 5. Security patches applied; 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

Changes in CIP-010



Changes in CIP-010

CIP-010-4 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	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.	For each change to the items listed in Part 1.1: 1.2.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.2.2. Following the change, verify that required cyber security controls determined in 1.2.1 are not adversely affected; and 1.2.3. Document the results of the verification.	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.

Changes in CIP-010

CIP-007-7 Table R2 – Security Patch Managementt			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	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 associated with 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: 1.4.1. Verify the identity of the software source; and 1.4.2. 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.

Changes in CIP-010

CIP-010-4 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
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.	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.

Backward Compatibility – Management Modules

- SCI - 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.
- Existing Management Modules: Existing Management Modules remain as they were previously. The new requirements are built around Management Modules of SCI. Where SCI is not used , these particular requirements will not apply

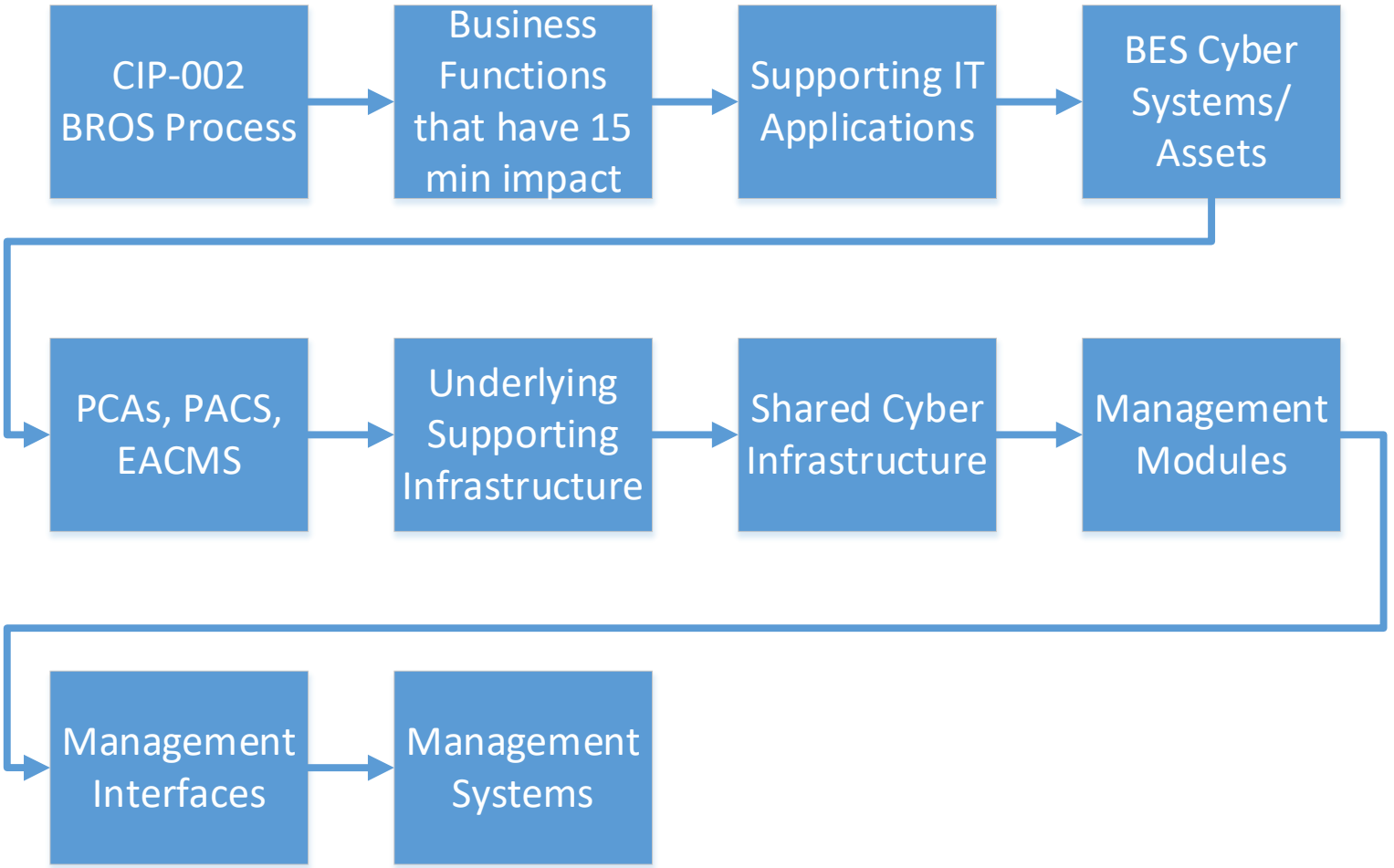
Management Systems of SCI vs. Existing Management Systems

- 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.
- Existing Cyber Assets that are used for the management of systems such as a software distribution system management station or a anti malware management station – but not used to initialize, deploy or configure SCI will remain classified as they were before.
- The exception are existing systems that are also used to manage the logical isolation of SCI such as a centralized firewall management station.

Management Systems of SCI vs. Existing Management Systems

- Example: A software distribution management system that manages software on BCAs - has administrative rights on BCA and is running as Virtual Cyber Asset on SCI
- The software distribution management system is not used to initialize, deploy or configure SCI - Not a Management System of SCI
- However this system, that is running as a VCA, may still be an Applicable System depending on how it is classified (i.e. PCA associated with a BCS, EACMS or Intermediate System)
- There may be logical isolation or affinity requirements for this software distribution management system as it is a VCA, however no requirements as a Management System of SCI

Guidance - Classification Process for the Management of SCI



Q&A Objectives

- 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.

Questions and Answers

Jordan Mallory
Jordan.Mallory@nerc.net