NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Critical Infrastructure Protection (CIP) Version 5 Revisions

Standard Drafting Team Update
Industry Webinar
December 11, 2014

RELIABILITY | ACCOUNTABILITY

Administrative Items

- NERC Antitrust Guidelines
  - It is NERC’s policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.
- Notice of Open Meeting
  - Participants are reminded that this webinar is public. The access number was widely distributed. Speakers on the webinar should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

FERC Order 791 Highlights

- Directed changes to four main areas:
  - Identify, Assess, and Correct (IAC) – FERC-directed filing deadline
    - Remove or modify the IAC language, retain the substantive provisions, and clarify the obligations for compliance
  - Communication Networks – FERC-directed filing deadline
    - Define communication networks and create new or modified Reliability Standards to protect the nonprogrammable components of communication networks (e.g. cables and wires)
  - Low Impacts – No filing deadline
    - Add objective criteria from which to judge the sufficiency of controls
  - Transient Devices – No filing deadline
    - Develop new or modified Reliability Standards for transient devices (e.g. thumb drives and laptops)

Discussion Topics

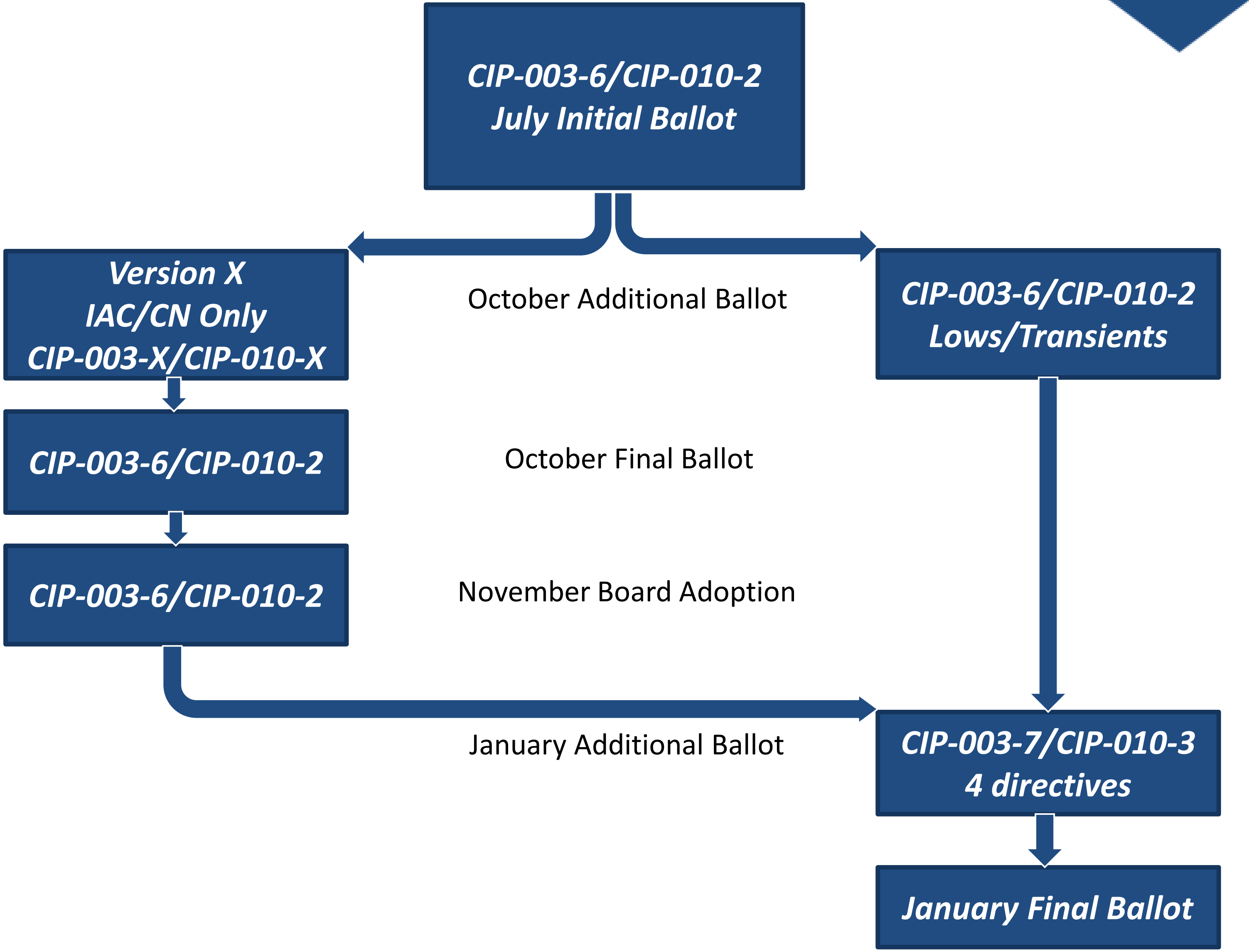
- Development Steps
- Versioning
- Current Comment Period & Ballot
- CIP-003-7 Revisions
  - Attachments 1 and 2
  - Revised Definitions
- CIP-010-3 Revisions
  - Attachments 1 and 2
  - Revised Definitions
- CIP-004-7, CIP-007-7, and CIP-011-3
- Implementation Plan Revisions
- Next Steps

Development Steps

Directive Area	Standard	Weighted Segment Vote
Communication Networks	-X	93.21%
Identify, Assess, Correct		
Lows Impact Assets	CIP-003-6	68.09%
	CIP-003-6 Definitions	74.25%
Transient Devices	CIP-010-2	79.91%
	CIP-010-2 Definitions	85.68%
Implementation Plan	N/A	89.01%

- All ballots ending on October 17, 2014 achieved passage
- SDT met October 22-24 to review comments and consider revisions
- Communication Networks and IAC revisions posted for final ballot October 28-November 6
- SDT met November 18
- Additional revisions for low impact and transient devices posted for additional comment period and ballot November 25-January 9

Versioning



CIP-003-6/CIP-010-2
July Initial Ballot

Version X
IAC/CN Only
CIP-003-X/CIP-010-X

October Additional Ballot

CIP-003-6/CIP-010-2
Lows/Transients

CIP-003-6/CIP-010-2

October Final Ballot

CIP-003-6/CIP-010-2

November Board Adoption

January Additional Ballot

CIP-003-7/CIP-010-3
4 directives

January Final Ballot

Current Additional Comment Period & Ballot

- SDT decided to make further revisions in response to comments and posted the following documents:
  - CIP-003-7, CIP-004-7, CIP-007-7, CIP-010-3, and CIP-011-3
  - Definitions
  - Implementation Plan
- Includes language adopted by NERC Board in November
  - IAC removal
  - Communication networks revisions
- Revisions addressed transient devices and lows directives
  - Focused on clarifying language and intent

CIP-003-7 Comment Themes

- Clarify requirement language and definitions
  - When does LERC exist?
  - Authorizations
  - "Based on need"
- Incident response record retention
- Guidance

CIP-003-7 Revisions

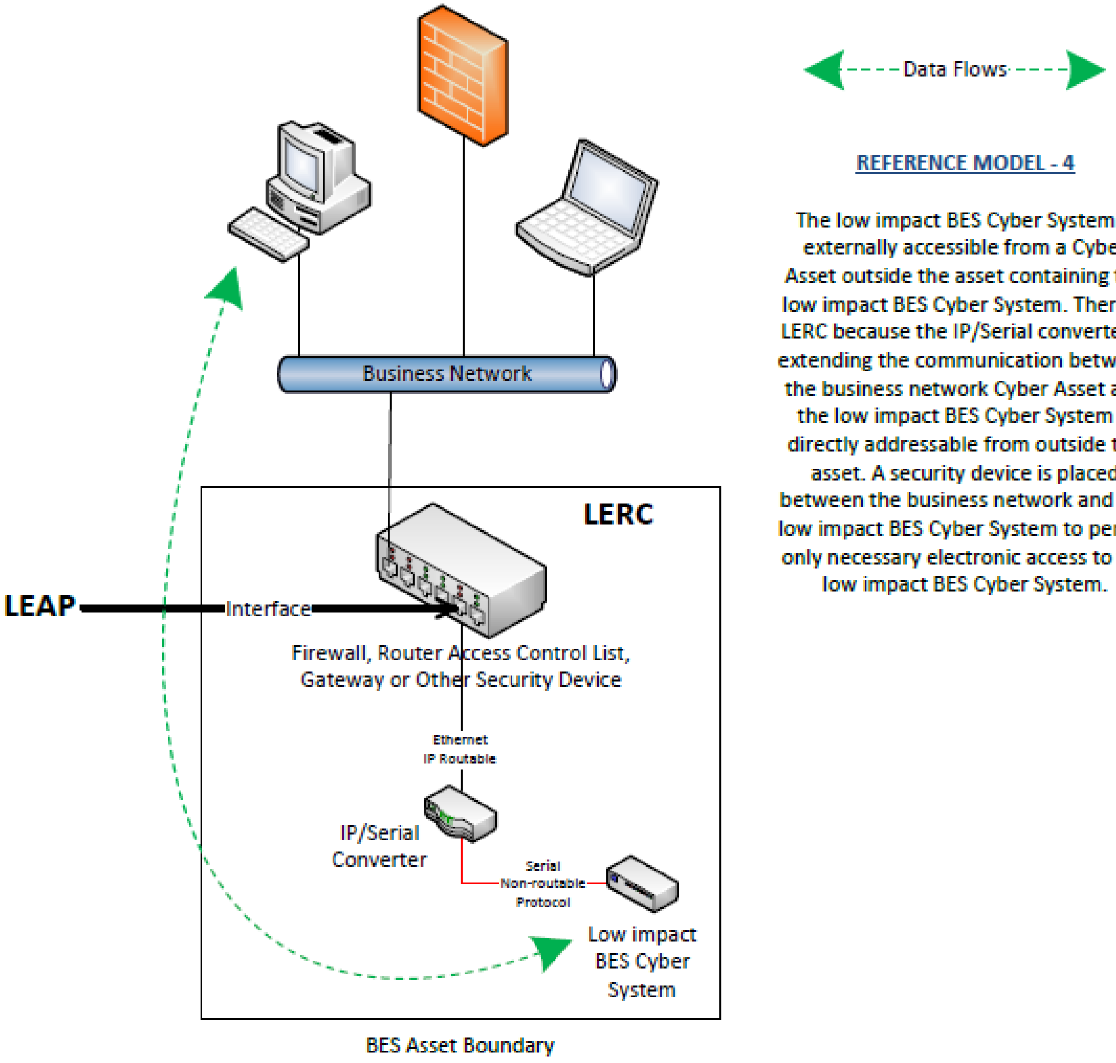
- Section 1 – Cyber security awareness
  - Added reference to physical security practices and bullets moved to guidance
- Section 2 – Physical security controls
  - Changed “restrict” to “control physical access” and moved “based on need” within the section for clarity
- Section 3 – Electronic access controls
  - Clarified language the relationship between LERC and LEAP, and significantly updated guidance
- Section 4 – Cyber Security Incident response
  - Removed record retention and added “if needed” on update obligation

CIP-003-7 Definitions Revisions

Low Impact BES Cyber System Electronic Access Point (LEAP): A Cyber Asset interface that controls~~allows~~ Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems. ~~The Low Impact BES Cyber System Electronic Access Point is not an Electronic Access Control or Monitoring System.~~

Low Impact External Routable Connectivity (LERC): Direct user-initiated interactive access or a direct device-to-device connection to a~~Bi-directional routable communications between~~ -low impact BES Cyber System(s) ~~and~~ from a Cyber Asset~~s~~ outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. ~~Communication protocols created for~~ Point-to-point communications between intelligent electronic devices that use routable communication protocols for time--sensitive protection or control functions between Transmission station or substation ~~Intelligent Electronic Device (IED) to IED communication for protection and/or control functions from~~ assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

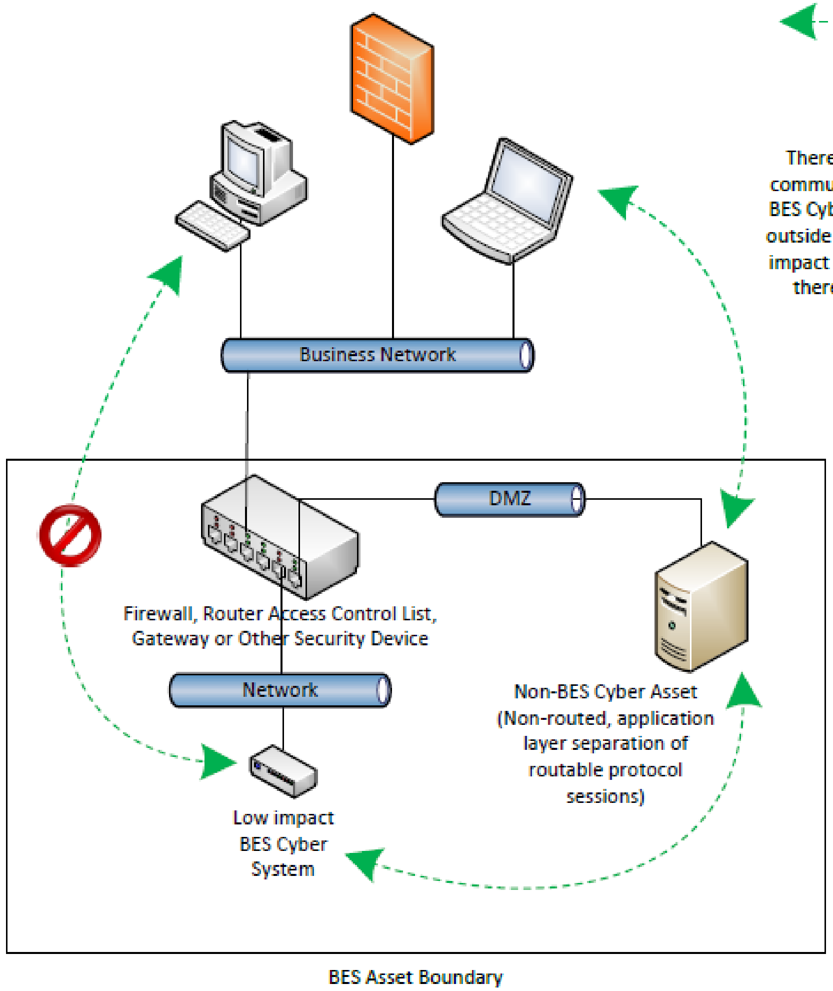
CIP-003-7 Reference Models



REFERENCE MODEL - 4

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System.

CIP-003-7 Reference Models

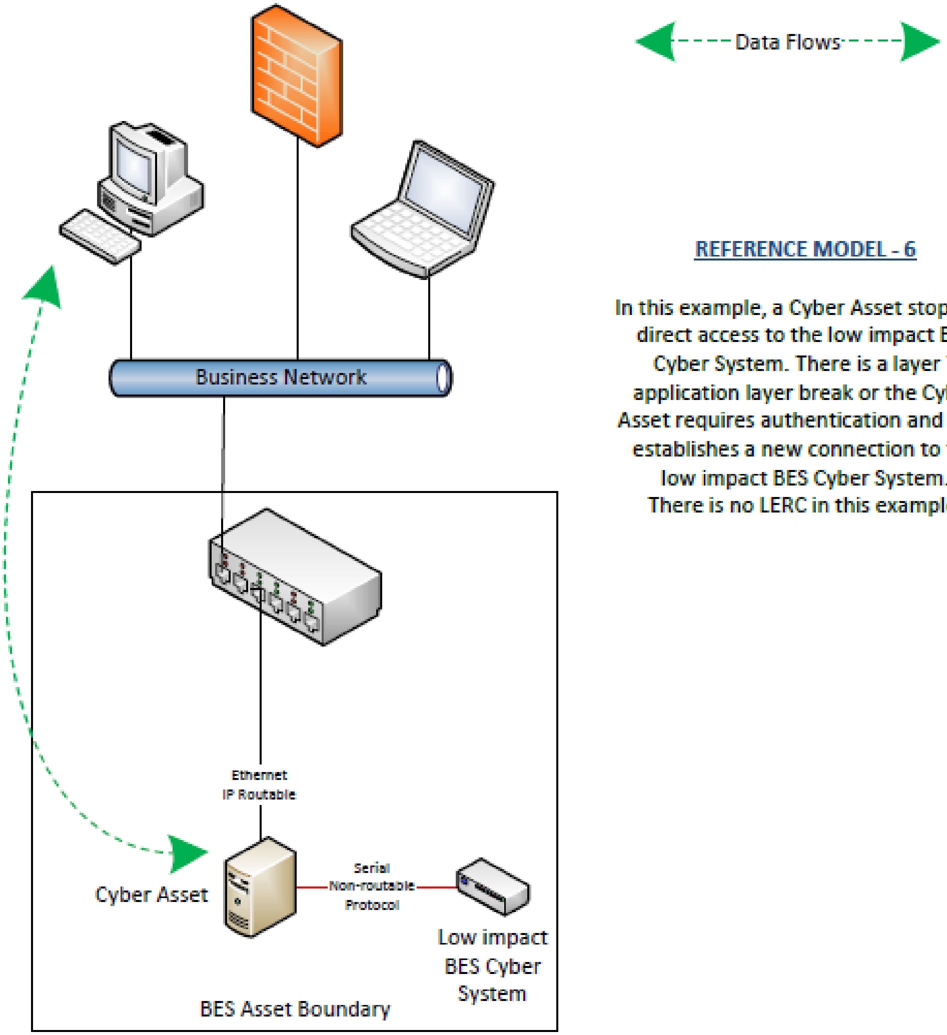

Business Network
DMZ
Firewall, Router Access Control List, Gateway or Other Security Device
Network
Low impact BES Cyber System
Non-BES Cyber Asset (Non-routed, application layer separation of routable protocol sessions)
BES Asset Boundary

Data Flows

REFERENCE MODEL - 5

There is no bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s) therefore there is no LERC in this example.

CIP-003-7 Reference Models

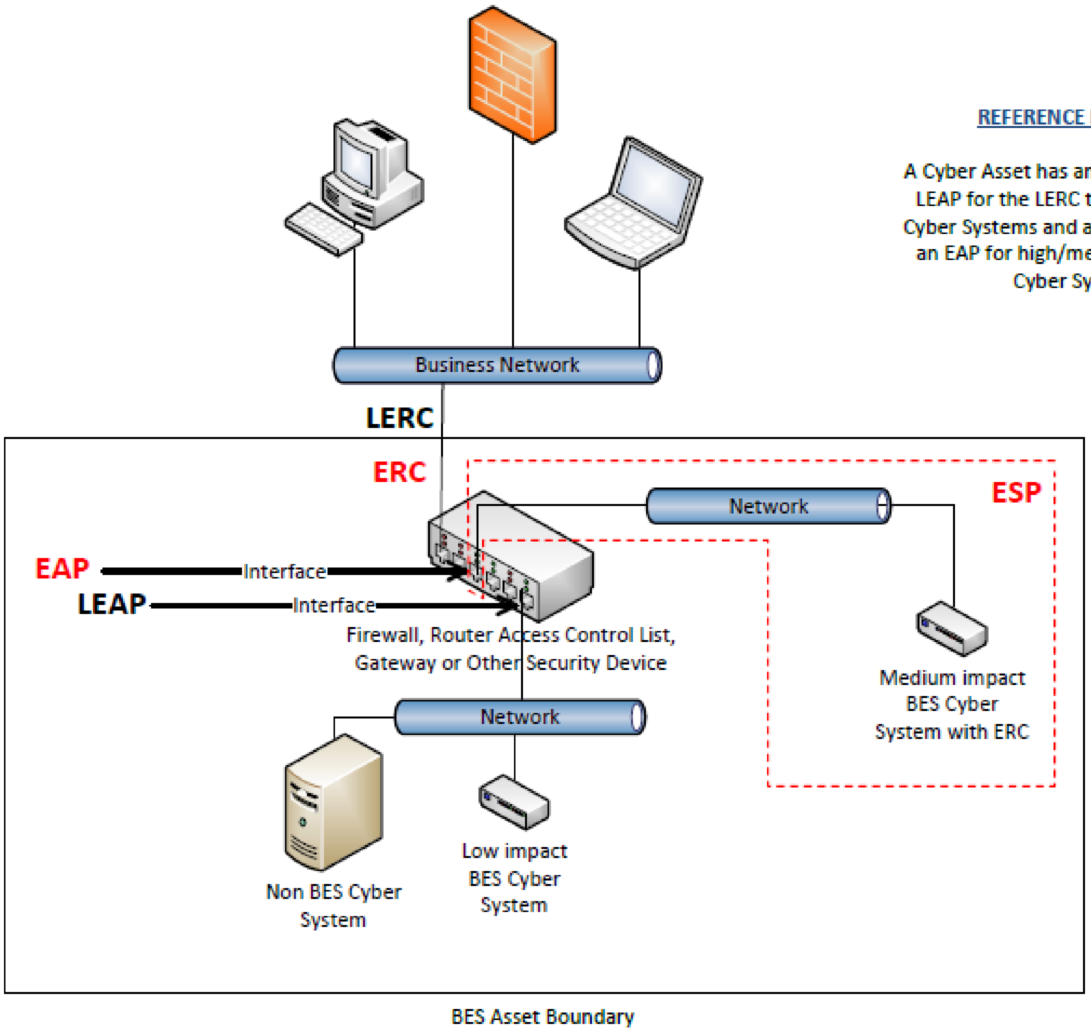


REFERENCE MODEL - 6

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System.
There is no LERC in this example.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-003-7 Reference Models



REFERENCE MODEL - 7

A Cyber Asset has an interface that is a LEAP for the LERC to low impact BES Cyber Systems and another interface is an EAP for high/medium impact BES Cyber Systems.

CIP-010-3 Comment Themes

- Clarify requirement language and definitions
  - “Owned” devices
  - “Vendor or contractor”
  - Authorizations
  - Classification as Transient Cyber Asset or Removable Media
  - Is Media defined term?
- Guidance
  - Authorization based on a group of assets
  - Mitigation of vulnerabilities and malicious code
  - Managing physical access (tampering)

CIP-010-3 Revisions

- Section 1 – Transient Cyber Assets managed by Responsible Entity removed “owned”
  - Section 1.2 – clarified only one authorization needed by moving “authorize” to apply to the sub-sections
  - Section 1.3 – revised “security vulnerability” to “software vulnerability” and added “objective” language
  - Section 1.4 & 1.5 – added “objective” language
- Section 2 – Transient Cyber Assets managed by party other than Responsible Entity removed “owned” and replaced “vendor or contractor”
  - Section 2.1 & 2.2 – added “objective” language

CIP-010-3 Revisions

- Section 3 – Removable Media
  - Section 3.1 – clarified only one authorization needed by moving “authorize” to apply to the sub-sections
  - Section 3.2 – added “objective” language and clarified language in sub-sections

CIP-010-3 Definitions Revisions

Removable Media: Storage ~~Media~~media~~,~~ that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less~~, capable of transmitting executable code to:~~ to ~~(1)~~ a BES Cyber Asset, ~~(2)~~ a network within an ESP, or ~~(3)~~ a Protected Cyber Asset ~~that can be used to store, copy, move, or access data~~. ~~Removable Media are not Cyber Assets.~~ Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Transient Cyber Asset: A Cyber Asset~~,~~ that is (i) capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is ~~(e.g., using Ethernet, serial, Universal Serial Bus, and wireless including near field and Bluetooth communication)~~ directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less~~, capable of transmitting executable code to: (1)~~ to a BES Cyber Asset, ~~(2)~~ a network within an ESP, or ~~(3)~~ a ~~Protected Cyber Asset~~PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

CIP-004-7, CIP-007-7, and CIP-011-3

- Revisions include language related to transient devices
- CIP-004-7 – Training content to include cyber security risks associated with electronic interconnectivity and interoperability with Cyber Assets, including Transient Cyber Assets, and with Removable Media
- CIP-007-7 – capitalized Removable Media in Part 1.2 and added paragraph to guidance
- CIP-011-3 – added guidance that information stored on Transient Cyber Assets or Removable Media could be BES Cyber System Information

Implementation Plan Revisions

		NERC Board Adoption	*If FERC approves CIPV5R in:*			V5 E-Date
Standard/Requirement	**Revision**		3Q15	4Q15	1Q16	
CIP-002-5	**not up for revision**	**IAC, CN revisions - November 13, 2014** **LI, TD revisions -targeted Feb 2015**	1-Apr-16	1-Apr-16	1-Apr-16	**April 1, 2016 - CIP V5 Approved Effective Date**
CIP-003-7			1-Apr-16	1-Apr-16	1-Jul-16	
CIP-003-7, R1, part 1.2	LIA - Policy		1-Apr-17	1-Apr-17	1-Apr-17	
CIP-003-7, R1, part 1.2	LI - Policy		1-Apr-17	1-Apr-17	1-Apr-17	
CIP-003-7, R2	LI - Plan		1-Apr-17	1-Apr-17	1-Apr-17	
CIP-003-7, Att 1, Sect. 1	LI - Sec Awareness		1-Apr-17	1-Apr-17	1-Apr-17	
CIP-003-7, Att 1, Sect. 2	LI - Phys Security		1-Sep-18	1-Sep-18	1-Sep-18	
CIP-003-7, Att 1, Sect. 3	LI - Elec. Access		1-Sep-18	1-Sep-18	1-Sep-18	
CIP-003-7, Att 1, Sect. 4	LI - Incident Resp		1-Apr-17	1-Apr-17	1-Apr-17	
CIP-004-7	TCA & RM added to Training		1-Apr-16	1-Apr-16	1-Jul-16	
CIP-005-5	**not up for revision**		1-Apr-16	1-Apr-16	1-Apr-16	
CIP-006-6			1-Apr-16	1-Apr-16	1-Jul-16	
CIP-006-6, R1, part 1.10*	CN		1-Jan-17	1-Jan-17	1-Apr-17	
CIP-007-7			1-Apr-16	1-Apr-16	1-Jul-16	
CIP-007-7, R1, part 1.2*	CN, RM capitalized		1-Jan-17	1-Jan-17	1-Apr-17	
CIP-008-5	**not up for revision**		1-Apr-16	1-Apr-16	1-Apr-16	
CIP-009-6			1-Apr-16	1-Apr-16	1-Jul-16	
CIP-010-3			1-Apr-16	1-Apr-16	1-Jul-16	
CIP-010-3, R4	TD		1-Jan-17	1-Jan-17	1-Apr-17	
CIP-011-3	TCA & RM added to Guidelines		1-Apr-16	1-Apr-16	1-Jul-16	
TCA, RM Glossary Terms	TD		1-Jan-17	1-Jan-17	1-Apr-17	
BCA, PCA Glossary Terms	TD		1-Jan-17	1-Jan-17	1-Apr-17	
LERC, LEAP Glossary Terms	LIA		1-Apr-17	1-Apr-17	1-Apr-17	

Next Steps

- Additional Ballot concludes January 9
- SDT will meet January 13-14 at NERC in Atlanta
- Final ballot will be conducted soon after SDT meeting
- Request NERC Board adoption
- File at FERC following NERC Board adoption
- RSAW coordination
- Dispersed generation resources coordination

Questions and Answers