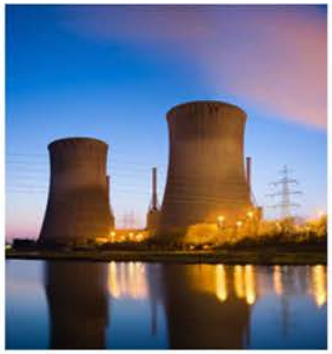
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Critical Infrastructure Protection (CIP) Version 5 Revisions

Standard Drafting Team Update
Industry Webinar
September 19, 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 call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

FERC Order 791 Highlights

- Directed changes to four main areas:
  - Identify, Assess, and Correct (IAC) – Filing deadline Feb. 3, 2015
    - Remove or modify the IAC language, retain the substantive provisions, and clarify the obligations for compliance
  - Communication Networks – Filing deadline Feb. 3, 2015
    - Define communication networks and create new or modified Reliability Standards to protect the nonprogrammable components of communication networks (e.g. cables and wires)
  - Low Impact Assets – 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
- CIP-003-6 Revisions
  - Attachments 1 and 2
  - Two New Definitions
- CIP-010-2 Revisions
  - Attachments 1 and 2
  - Revised Definitions
- -X Posting
- Implementation Plan

Development Steps

Directive Area	Standard	Weighted Segment Vote
Communication Networks	CIP-006-6	76.20%
	CIP-007-6	78.35%
Identify, Assess, Correct	CIP-009-6	85.29%
Lows Impact Assets	CIP-003-6	**35.72%**
Transient Devices	CIP-004-6	80.71%
	CIP-010-2	**49.48%**
	CIP-011-2	82.51%
	Definitions	78.52%

- Initial comment period and ballot ended July 16, 2014
- Standard drafting team (SDT) received over 200 pages of comments
- SDT met July 29-31, 2014 and August 19-21, 2014 to revise the standards based on stakeholder comments
- Latest revisions and consideration of comments posted for additional comment and ballot period Sept 3-Oct 17, 2014

CIP-003-6 Comment Themes

- Define *external routable protocol path*
- Security awareness timeframes
- More guidance
- Inventory implications
- Requirement placement

CIP-003-6, Requirement R1

- Requirement R1 addresses policies for all impact levels
- Part 1.1 includes high and medium

R1. Each Responsible Entity~~, for its high impact and medium impact BES Cyber Systems~~ shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and~~&~~ training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

CIP-003-6, Requirement R1 *(continued)*

- Requirement R1, Part 1.2 now includes lows topics in policies

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls for Low Impact External Routable Connectivity and Dial-up Connectivity; and

~~**1.1.9.**~~**1.2.4.** Cyber Security Incident Response

CIP-003-6, Requirement R2 *(continued)*

R2. Each Responsible Entity ~~for its assets~~with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall ~~perform each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets*~~implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the elements in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the elements in Attachment 1 and additional evidence to demonstrate implementation of cyber security plan(s). Additional examples of evidence per element are located in Attachment 2. ~~Evidence must include each of the applicable documented policies and processes that collectively include each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets* and any additional evidence to demonstrate implementation as described in the Measures column of the table~~

- Attachment 1 – Required Elements for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems
- Attachment 2 – Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

CIP-003-6 Attachments, Element 1

- Cyber Security Awareness

1. Cyber security awareness: Each Responsible Entity shall reinforce, once every 15 calendar months, its cyber security practices, using one or a combination of the following methods:
    - Direct communications (for example, e-mails, memos, computer-based training);
    - Indirect communications (for example, posters, intranet, or brochures); or
    - Management support and reinforcement (for example, presentations or meetings).

Element 1: An example of evidence for element 1 may include, but is not limited to documentation that the reinforcement of cyber security practices once every 15 months has been provided through dated copies of the information used to reinforce security awareness via direct communications, indirect communications or management support and reinforcement.

CIP-003-6 New Definitions

- Low Impact BES Cyber System Electronic Access Point (LEAP)
  - A Cyber Asset interface that allows Low Impact External Routable Connectivity. The Cyber Asset 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)
  - 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). Communication protocols created for Intelligent Electronic Device (IED) to IED communication for protection and/or control functions from assets containing low impact BES Cyber Systems are excluded (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

CIP-003-6 Attachments, Element 2

- Physical Access Controls

2. Physical access controls: Each Responsible Entity shall implement controls to restrict physical access to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Low Impact BES Cyber System Electronic Access Point, if any, based on need as determined by the Responsible Entity, through one or more of the following:

- Access controls;
- Monitoring controls; or
- Other operational, procedural, or technical physical security controls.

Element 2: Examples of evidence for element 2 may include, but are not limited to:

1. Documentation of one or more access controls (e.g. card key, special locks), monitoring controls (e.g. alarm systems, human observation), or other operational, procedural or technical physical security controls to restrict physical access to both:
   a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
   b. The Cyber Asset, if any, containing the Low Impact BES Cyber System Electronic Access Point.
2. Documentation showing that the physical access restrictions cited above are based on need, which may include, but is not limited to, a policy describing the high level operational or business need(s) for physical access.

CIP-003-6 Attachments, Element 3

- Electronic Access Controls

3. Electronic access controls: Each Responsible Entity shall implement controls to restrict electronic access for Low Impact External Routable Connectivity and Dial-up Connectivity, which shall include the following, or other electronic access controls that provide an equal or greater level of protection:

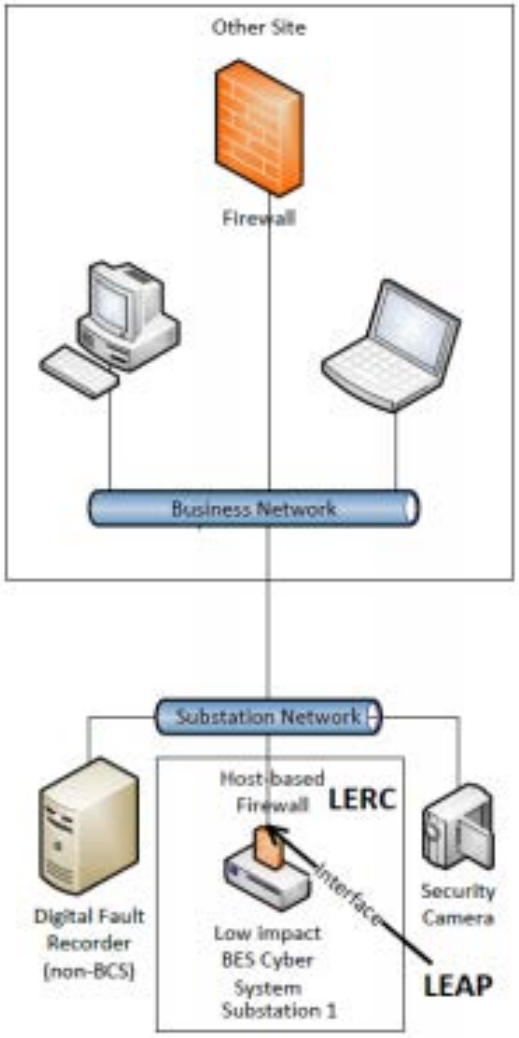
3.1 For any Low Impact External Routable Connectivity, establish a Low Impact BES Cyber System Electronic Access Point that permits only necessary inbound and outbound access and denies all other access; and

3.2 Authentication of all Dial-up Connectivity that provides access to low impact BES Cyber Systems, per Cyber Asset capability.

Element 3: Examples of evidence for element 3 may include, but are not limited to:

- Documentation showing that inbound and outbound connections (e.g. IP addresses, ports, services) for any Low Impact BES Cyber System Electronic Access Point are confined to only those the Responsible Entity deems necessary; and documentation of authentication for Dial-up Connectivity (e.g. dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, access control on the BES Cyber System); or
- Documentation of other electronic access controls that provide an equal or greater level of protection.

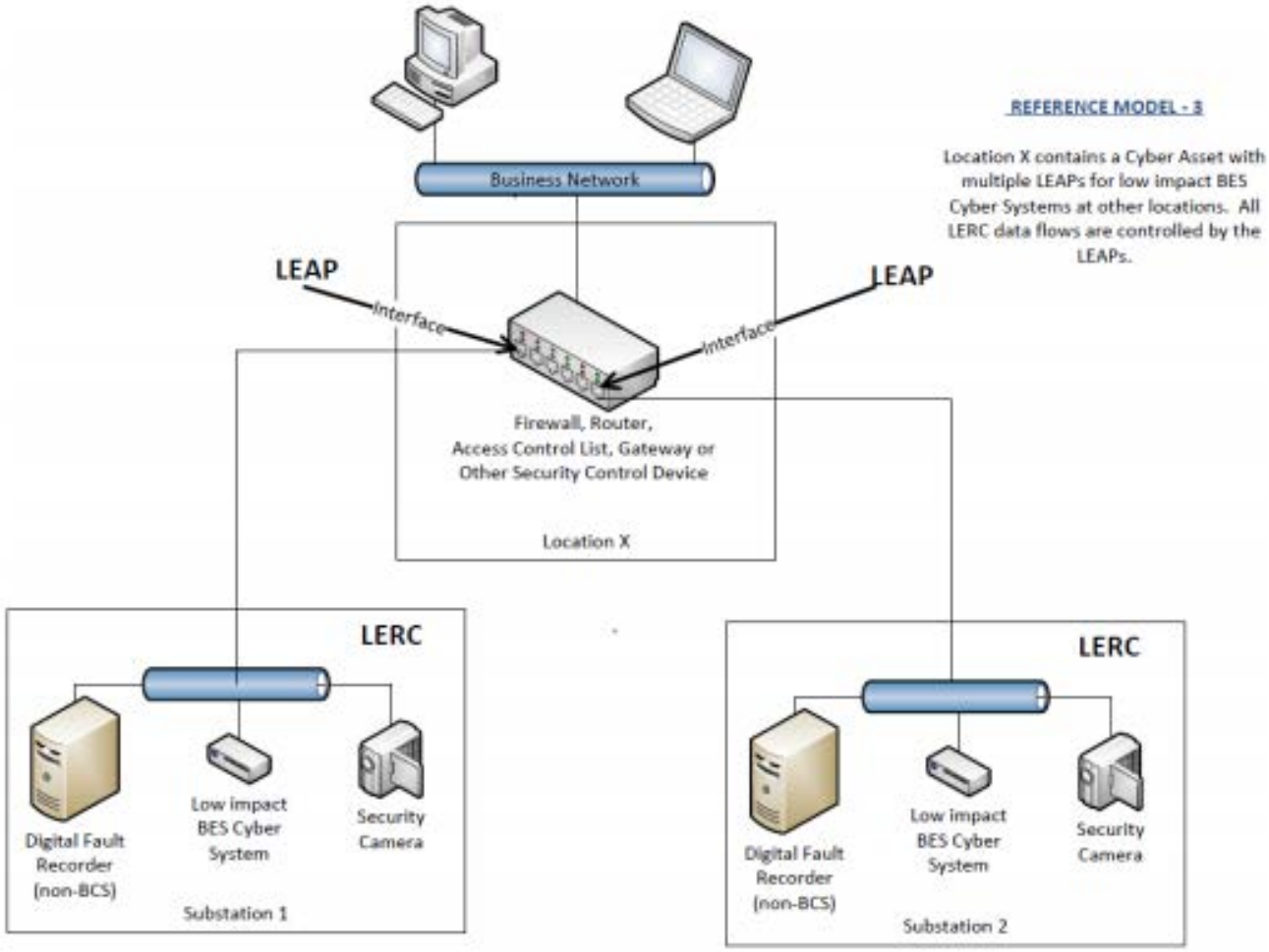
Use Case 1



REFERENCE MODEL - 1

The low impact BES Cyber System is behind a LEAP. In this example, the LEAP is the network interface on the low impact BES Cyber System. The host-based firewall restricts electronic access for Low Impact External Routable Connectivity (LERC).

Use Case 2


REFERENCE MODEL - 3
Location X contains a Cyber Asset with multiple LEAPs for low impact BES Cyber Systems at other locations. All LERC data flows are controlled by the LEAPs.
Business Network
LEAP
Interface
LEAP
Interface
Firewall, Router, Access Control List, Gateway or Other Security Control Device
Location X
LERC
Digital Fault Recorder (non-BCS)
Low impact BES Cyber System
Security Camera
Substation 1
LERC
Digital Fault Recorder (non-BCS)
Low impact BES Cyber System
Security Camera
Substation 2

CIP-003-6 Attachments, Element 4

- Cyber Security Incident Response

4. Cyber Security Incident response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents.

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law.

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals.

4.4 Incident handling for Cyber Security Incidents.

4.5 Testing the Cyber Security Incident response plan at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident.

4.6 Record retention related to Reportable Cyber Security Incidents.

4.7 Updating the Cyber Security Incident response plan within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

CIP-003-6 Attachments, Element 4 *(continued)*

- Cyber Security Incident Response

Element 4: An example of evidence for element 4 may include, but is not limited to, dated documentation such as policies, procedures or process documents of one or more Cyber Security Incident response plan(s); either by asset or group of assets that include the following processes:

1. to identify, classify and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security incident and for notifying the Electricity Sector Information Sharing and Analysis Center (ES-ISAC);
2. the identification and documentation of the roles and responsibilities for Cyber Security Incident response by groups of individuals (e.g. initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g. containment, eradication, recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to retain records related to Reportable Cyber Security Incidents (e.g. security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes).

Also include dated revised Cyber Security Incident response plan(s) that identify that the plan(s) were updated within 180 calendar days after a completion of a test or actual Reportable Cyber Security Incident.

CIP-003-6 Implementation Plan

- Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 1 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.
- Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 2 until the later of April 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

CIP-003-6 Implementation Plan

- Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 3 until the later of September 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.
- Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 4 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

CIP-003-6 Implementation Plan

Standard/Req.	Revision	Compliance Date
CIP-003-6		1-Apr-16
CIP-003-6, R1, P1.2	Policy	1-Apr-17
CIP-003-6, R2	Plan	1-Apr-17
CIP-003-6, A1, E1	Sec Awareness	1-Apr-17
CIP-003-6, A1, E2	Phys Access	1-Apr-18
CIP-003-6, A1, E3	Elec. Access	1-Sep-18
CIP-003-6, A1, E4	Incident Resp	1-Apr-17

CIP-010-2 Comment Themes

- Authorization
- Inspection
- Vendor-managed devices
- “Prior to use”
- More guidance

CIP-010-2 Revised Definitions

- BES Cyber Asset (BCA): A Cyber Asset 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. ~~A Transient Cyber Asset is not a BES Cyber Asset.~~

CIP-010-2 Revised Definitions *(continued)*

- Protected Cyber Assets (PCA): One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. ~~A Transient Cyber Asset is not a Protected Cyber Asset.~~

CIP-010-2 Revised Definitions *(continued)*

- Removable Media: ~~Portable media~~Media, directly connected for 30 consecutive calendar days or less, capable of transmitting executable code 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, ~~and/~~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. ~~A Cyber Asset is not Removable Media.~~

CIP-010-2 Revised Definitions *(continued)*

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

CIP-010-2, Requirement R4

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement one or more documented ~~process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media* Protection~~ plan(s) for Transient Cyber Assets and Removable Media that include the elements in Attachment 1, except under CIP Exceptional Circumstances. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable elements in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per element are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media~~Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table~~.

- Attachment 1 – Required Elements for Plans for Transient Cyber Assets and Removable Media
- Attachment 2 – Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

CIP-010-2 Attachments, Element 1

- Transient Cyber Asset(s) Owned or Managed by the Responsible Entity
  - 1.1 – Transient Cyber Asset management
  - 1.2 – Transient Cyber Asset authorization
  - 1.3 – Security vulnerability mitigation
  - 1.4 – Introduction of malicious code mitigation
  - 1.5 – Risk of unauthorized use mitigation
- Measures
  - Important to note if an entity does not use Transient Cyber Asset(s), examples of evidence include, but are not limited to a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s).

CIP-010-2 Attachments, Element 2

- Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors
  - 2.1 – Security vulnerability mitigation
  - 2.2 – Malicious code mitigation
  - 2.3 – Additional mitigation actions necessary?
- Measures
  - Important to note if a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

CIP-010-2 Attachments, Element 3

- Removable Media
  - 3.1 – Removable Media authorization
  - 3.2 – Malicious code mitigation
- Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Role of Guidance

- In response to comments, SDT expanded Guidelines and Technical Basis
- Stakeholders are encouraged to thoroughly consider the Guidelines and Technical Basis sections
- Guidance is to help clarify the requirement language, but not change the scope or intent of the requirement

Implementation Timeline

Standard/Requirement	Revision	Targeted NERC BOT Approval	If FERC approves CIPV5R in: 3Q15	4Q15	1Q16	V5 E-Date
CIP-002-5	not up for revision	November 13, 2014 - NERC BOT Meeting, Atlanta	1-Apr-16	1-Apr-16	1-Apr-16	April 1, 2016 - CIP V5 Approved Effective Date
CIP-003-6			1-Apr-16	1-Apr-16	1-Jul-16	
CIP-003-6, R1, part 1.2	LIA - Policy		1-Apr-17	1-Apr-17	1-Apr-17	
CIP-003-6, R2	LIA - Plan		1-Apr-17	1-Apr-17	1-Apr-17	
CIP-003-6, Att 1, Item 1	LIA - Sec Awareness		1-Apr-17	1-Apr-17	1-Apr-17	
CIP-003-6, Att 1, Item 2	LIA - Phys Access		1-Apr-18	1-Apr-18	1-Apr-18	
CIP-003-6, Att 1, Item 3	LIA - Elec. Access		1-Sep-18	1-Sep-18	1-Sep-18	
CIP-003-6, Att 1, Item 4	LIA - Incident Resp		1-Apr-17	1-Apr-17	1-Apr-17	
CIP-004-6	TCA & RM added to Training		1-Apr-16	1-Apr-16	1-Oct-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-007-6			1-Apr-16	1-Apr-16	1-Jul-16	
CIP-007-6, R1, part 1.2*	CN		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-010-2			1-Apr-16	1-Apr-16	1-Jul-16	
CIP-010-2, R4	TD		1-Jan-17	1-Jan-17	1-Apr-17	
CIP-011-2	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	
LERC, LEAP Glossary Terms	LIA		1-Apr-17	1-Apr-17	1-Apr-17	

-X Posting

- Purpose of the posting is as a practical contingency
- -X decouples the IAC and Communication Network revisions from the Low Impact and Transient Device revisions
- Single ballot for the –X package
- Approval of the –X standards enables the SDT to meet the FERC filing deadline of February 3, 2015 should the Lows or Transient Device revisions fail in the second ballot
- All proposed revisions will be subject to final ballot

BES Cyber Asset Directive

- NERC will no longer pursue Section 1600 to meet directive regarding BES Cyber Asset definition
- NERC will coordinate with implementation study participants, regions, and other entities, as necessary, to answer questions in FERC Order No. 791
- Filing deadline of February 3, 2015

Next Steps

- Additional comment period – September 3-October 17, 2014
- Ballot period – October 8-17, 2014
- SDT meeting October 22-24, 2014 – ERCOT (Austin, TX)
- Targeted final ballot – October 31-November 10, 2014
- Targeted NERC Board of Trustees meeting to approve revisions – November 13, 2014
- The SDT appreciates your support

Questions and Answers