NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP Standards Development Overview

CSSDTO706

Meeting with Industry Representative

August 16 – 18 – NERC Atlanta Office

to ensure
the reliability of the
bulk power system

Objectives

- Historical Timeline
- CIP-002-4
- CIP-005-4
- CIP Version 5

Project 2008-06 Overview

- **FERC Order 706**
- SDT appointed – August 2008
- CIP Version 2 – September 2009
- CIP Version 3 – March 2010
- CIP Version 4 – Ongoing Effort

CSO706 SDT Members

- 17 members – almost all asset owners
- Representation from IOUs, US and Canadian Government, Cooperatives, Municipals, Independent Power Producers, and ISO/RTO
- Worked together for 3 years
- Monthly face-to-face meetings, several interim conference calls and multiple webinars/workshops
- Worked through 3 successful ballots

CIP-002-4 Overview

- Version 4 of the CIP Standards
- Approved by Industry December 30, 2010
- Submitted to FERC February 10, 2011
  - 2,232 page filing
  - http://www.nerc.com/files/Final_Final_CIP_V4_Petition_20110210.pdf
  - Filing included CIP-002-4 through CIP-009-4, but only changes in CIP-002-4

CIP-002-4 Overview (cont.)

- Replaces "risk-based assessment methodology" with "bright-line criteria"
  - Still maintains the concept of Critical Asset and Critical Cyber Asset
  - Uniform application across all entities and regions
  - Eliminates subjectivity by entities over what is "critical"
  - 17 defined criteria
  - To the greatest extent possible, bright line criteria tied to operational standards

CIP-002-4 Applicability

4.2. The following are exempt from Standard CIP-002-4:

- 4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.
- 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
- 4.2.3 Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.

CIP-002-4 Effective Date

Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

CIP-002-4 Requirement R1

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall update this list as necessary, and review it at least annually.

CIP-002-4 Requirement R2

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1

CIP-002-4 Requirement R3

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)’s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

Remote Access UA

- Implements requirements on “Cyber Assets” used for “monitoring or support” of Critical Cyber Assets when communication is initiated from outside an Electronic Security Perimeter
  - i.e., remote laptop or desktop systems accessing Critical Cyber Assets, but *not* for the purpose of control
  - Remote access for the purpose of control is the subject of CAN-0005
- Development now integrated into CIP Version 5

CIP V5

- The Drafting Team continues to work to address the remaining issues in Order 706
  - Using the “CIP-002 to CIP-009 +” organization
  - Monthly meetings and many conference calls
  - Initial ballot by December 2011
- The Drafting Team developed a set of development goals

Development Goals

Goal 1: To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements.

Goal 2: To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES.

Goal 3: To provide guidance and context for each Standard Requirement

Goal 4: To leverage current stakeholder investments used for complying with existing CIP requirements.

Goal 5: To minimize technical feasibility exceptions.

Goal 6: To develop requirements that foster a “culture of security” and due diligence in the industry to complement a “culture of compliance”.

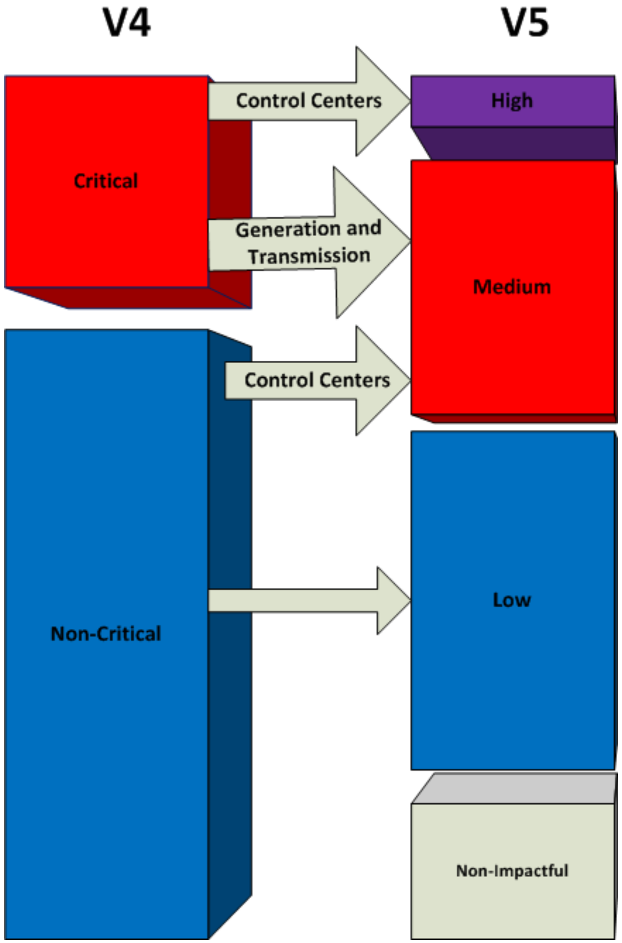
Goal 7: To develop a realistic and comprehensible implementation plan for the industry.

Requirement Filters

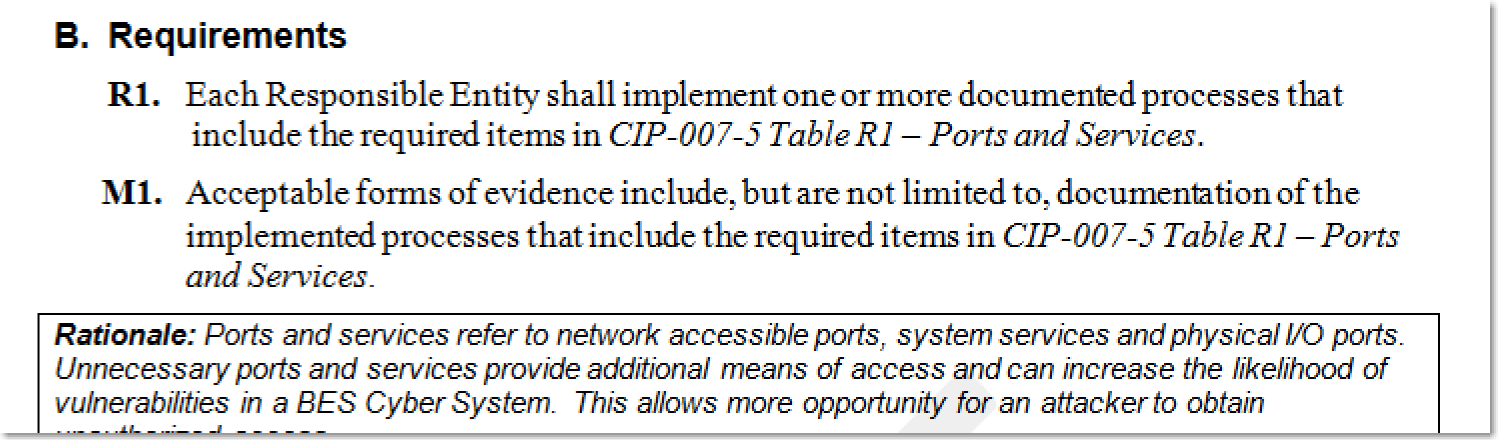
- Why are we doing this? What do we hope to accomplish? What security concept are we trying to implement? If these questions cannot be answered, is the requirement necessary?
- Is it absolutely necessary to be done only this way to protect the BES? Are there other ways of accomplishing this requirement? If so, the requirement may be too specific.
- Is the timeframe arbitrary?
- Is the desired outcome clear and unambiguous? Can the measure clarify the desired outcome?

Levels of impact

- High Impact
  - Large Control Centers
  - CIP-003 through 009+
- Medium Impact
  - Generation and Transmission
  - Other Control Centers
  - Similar to CIP-003 to 009 v4
- All other BES Cyber Systems
  - Security Policy
  - Security Awareness
  - Incident Response
  - Boundary Protection



Format (1/4) – Introductory Requirement



B. Requirements

R1. Each Responsible Entity shall implement one or more documented processes that include the required items in *CIP-007-5 Table R1 – Ports and Services.*

M1. Acceptable forms of evidence include, but are not limited to, documentation of the implemented processes that include the required items in *CIP-007-5 Table R1 – Ports and Services.*

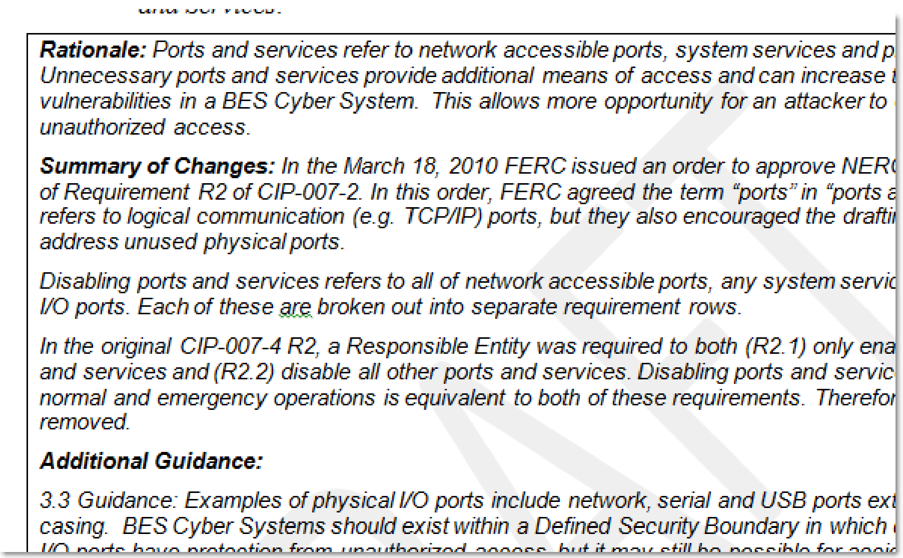
Rationale: *Ports and services refer to network accessible ports, system services and physical I/O ports. Unnecessary ports and services provide additional means of access and can increase the likelihood of vulnerabilities in a BES Cyber System. This allows more opportunity for an attacker to obtain unauthorized access*

- Requirement/measures for implemented procedures in most requirements
- Most requirements reference a table immediately below

Format (2/4) – Contextual Boxes

- **Rationale –** Purpose of requirement and any assumptions made about the requirement
- **Summary of Changes –** High level overview of changes in this requirement
- **Guidance –** Additional guidance in applying the requirement

Work in Progress



and services.

Rationale: *Ports and services refer to network accessible ports, system services and p*
Unnecessary ports and services provide additional means of access and can increase t
vulnerabilities in a BES Cyber System. This allows more opportunity for an attacker to
unauthorized access.

Summary of Changes: *In the March 18, 2010 FERC issued an order to approve NER*
of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports a
refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafti
address unused physical ports.

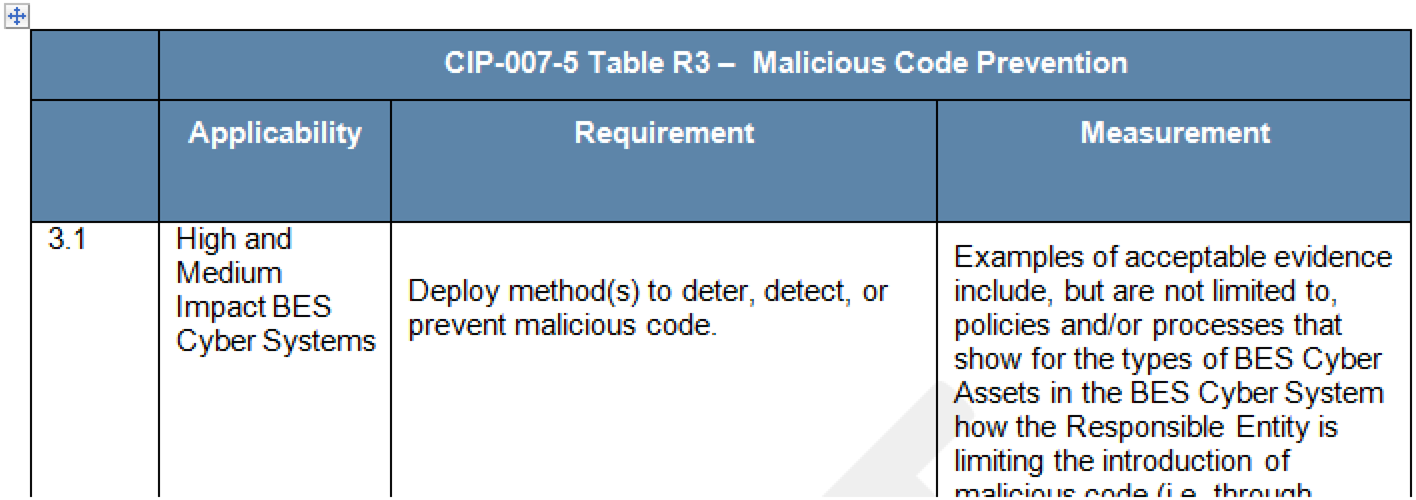
Disabling ports and services refers to all of network accessible ports, any system servic
I/O ports. Each of these are broken out into separate requirement rows.

In the original CIP-007-4 R2, a Responsible Entity was required to both (R2.1) only ena
and services and (R2.2) disable all other ports and services. Disabling ports and servic
normal and emergency operations is equivalent to both of these requirements. Therefor
removed.

Additional Guidance:

3.3 Guidance: Examples of physical I/O ports include network, serial and USB ports ext
casing. BES Cyber Systems should exist within a Defined Security Boundary in which
I/O ports have protection from unauthorized access, but it may still be possible for acci

Format (3/4) – Requirement Row



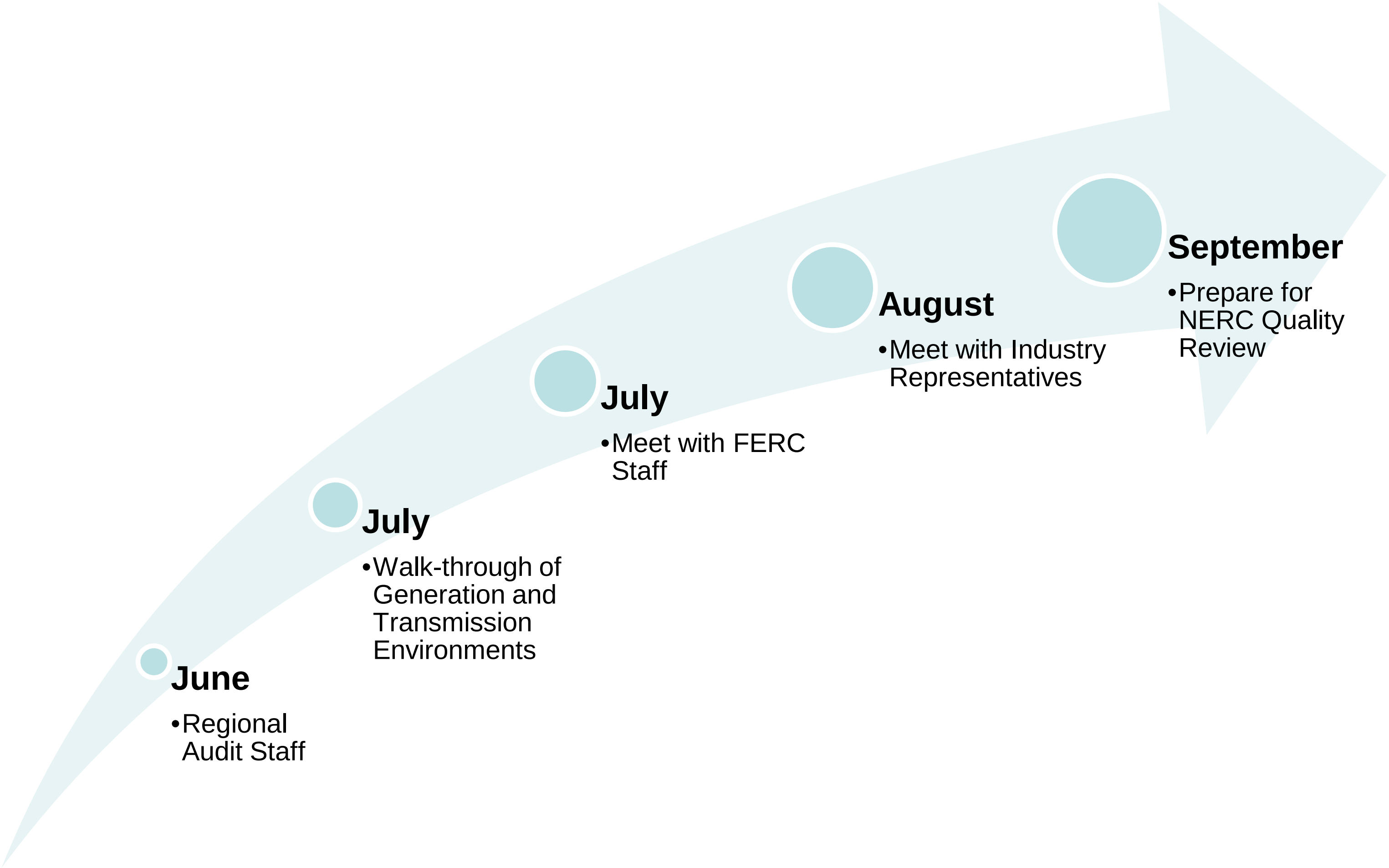
	CIP-007-5 Table R3 – Malicious Code Prevention		
	Applicability	Requirement	Measurement
3.1	High and Medium Impact BES Cyber Systems	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of acceptable evidence include, but are not limited to, policies and/or processes that show for the types of BES Cyber Assets in the BES Cyber System how the Responsible Entity is limiting the introduction of malicious code (i.e. through

- Measurement specifies acceptable evidence of **implementing** procedures associated with the requirement row.
- Measurements still a work in progress.

Format (4/4) – Applicability

- All Responsible Entities
- High Impact BES Cyber Systems
- Medium Impact BES Cyber Systems
- External Connectivity Attributes – Routable or Dial-up connectivity
- Associated Electronic Access Control Systems – CIP-005-4 R1.5
- Associated Physical Access Control Systems – CIP-006-4 R2
- Associated Protected Cyber Systems – Non-Critical Cyber Assets within an ESP

Schedule to Date – 2011



June

- Regional Audit Staff

July

- Walk-through of Generation and Transmission Environments

July

- Meet with FERC Staff

August

- Meet with Industry Representatives

September

- Prepare for NERC Quality Review

Key Dates Moving Forward

- **November 3rd –** First Posting for Comment and Ballot
  - Webinar – November 15th and 29th
  - December 9th – Ballot Opens
  - December 19th – Ballot Closing
- **March 26th –** Second Posting

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Questions?

to ensure
the reliability of the
bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-002-5

Definitions

- **BES Reliability Operating Services**

  BES Reliability Operating Services are those services contributing to the real-time reliable operation of the Bulk Electric System (BES). They include the following Operating Services:…

- **BES Cyber Asset**

  A Cyber Asset that if rendered unavailable, degraded, or misused could, within 15 minutes cause a Disturbance to the BES and adversely impact one or more BES Reliability Operating Services.

- **BES Cyber Systems**

  One or more BES Cyber Assets grouped together for the application of common cyber security controls. These are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services.

Summary of Requirements

- Categorized list of High and Medium Impact
  - Attachment 1 criteria
- Other BES Cyber Systems deemed to be Low Impact by default
- Update for significant changes to BES that affect High/Medium categorization
- Senior manager or delegate annual review and approval

Impact Criteria (Attachment 1)

- High: Large Control Centers (e.g. RC, BA, TOP)
- Medium: Based significant impact field assets, other Control Centers
- Other BES Cyber Systems deemed to be Low Impact by default
- Based on V4 criteria
    - Review of Transmission voltage threshold by SDT for V5
    - Use of MVA bright-line under consideration

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-003-5 Modifications

Summary of Modifications

- CIP-003-5 was reorganized to only include elements of policy and cyber security program governance.
  - Elements that addressed Change Control and Configuration Management were moved to CIP-010-5
  - Elements that address Information Protection were moved to CIP-011-5

Summary of Modifications

- Additional flexibility was added to the Cyber Security Policy requirement by explicitly allowing for multiple policies and specifying the topical areas (as opposed to all requirements) that the policy must address.
- The SDT has removed the requirement to document exceptions to the policy, although discussions of this approach with FERC staff are ongoing.

Addressing FERC Directives

FERC Order 706 Para. 376

"the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards."

- The SDT considers this a general management issue that is not within the scope of a compliance requirement.
- The SDT found no reliability basis in this requirement.
- The SDT has proposed removing the requirement for documented exceptions to the Cyber Security Policy.

Cyber Security Policy Changes

- Required elements of Cyber Security Policy
  - V4 - “The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.”
    - The SDT believes that this languages has caused the industry to develop Cyber Security Policies to the least common denominator, i.e. a restatement of the CIP standards.
  - V5 – “…articulates the Responsible Entity’s commitment to the protection of its BES Cyber Systems and addresses the following topics:
    - 1. Personnel Security
    - 2. Electronic Security Perimeters
    - 3. Remote Access
    - 4. Physical Security
    - 5. System Security
    - 6. Incident Response
    - 7. Recovery Plans
    - 8. Configuration Change Management
    - 9. Information Protection
    - 10. Provisions for emergency situations (Specified Exceptional Circumstances)

Access to the Cyber Security Policy

- Version 4 required that the Cyber Security Policy be "readily accessible to all personnel who have access to, or are responsible for, Critical Cyber Assets"
- Numerous concerns were raised as to the specific meaning of "readily accessible"
- The SDT proposes to modify this requirement by more directly stating its objective:
  - "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function."

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Questions?

to ensure
the reliability of the
bulk power system

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-004-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications (1/3)

- Security Awareness
  - Continues to be general awareness that is refreshed quarterly and not formal tracked training
- Training
  - Addition of visitor control program
  - electronic interconnectivity supporting the operation and control of BES Cyber Systems
  - storage media as part of the handling of BES Cyber Systems information
  - Reorganization of requirements into the respective requirements for “program” and “implementation” of the training.

Summary of Modifications (2/3)

- Personnel Risk Assessment
  - Changed to only initial identity verification
  - Now includes documenting the processes used to determine when to deny access
  - Reorganization of requirements into the respective requirements for “program” and “implementation”

Summary of Modifications (3/3)

- Authorization
  - Consolidated authorization and review requirements from CIP-003-4, CIP-004-4, CIP-006-4 and CIP-007-4
  - Allow quarterly and annual reviews to find and fix problems rather than self-report everything as a violation
- Revocation
  - Remove ability to access BES Cyber System when access no longer needed

Addressing FERC Directives

- FERC Order 706 P433 “we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard.”
  - The SDT addressed this by identifying the training topics that should be provided in the Training Program.
- FERC Order 706 P434 “The Commission adopts the CIP NOPR’s proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets.”
  - The SDT added this as a topic for role specific training.

Addressing FERC Directives

- FERC Order 706 P435 “Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves.”
  - The SDT does not feel security trainers need to be specially trained or certified.

Addressing FERC Directives (Immediate Revocation)

FERC Order 706 Para. 460

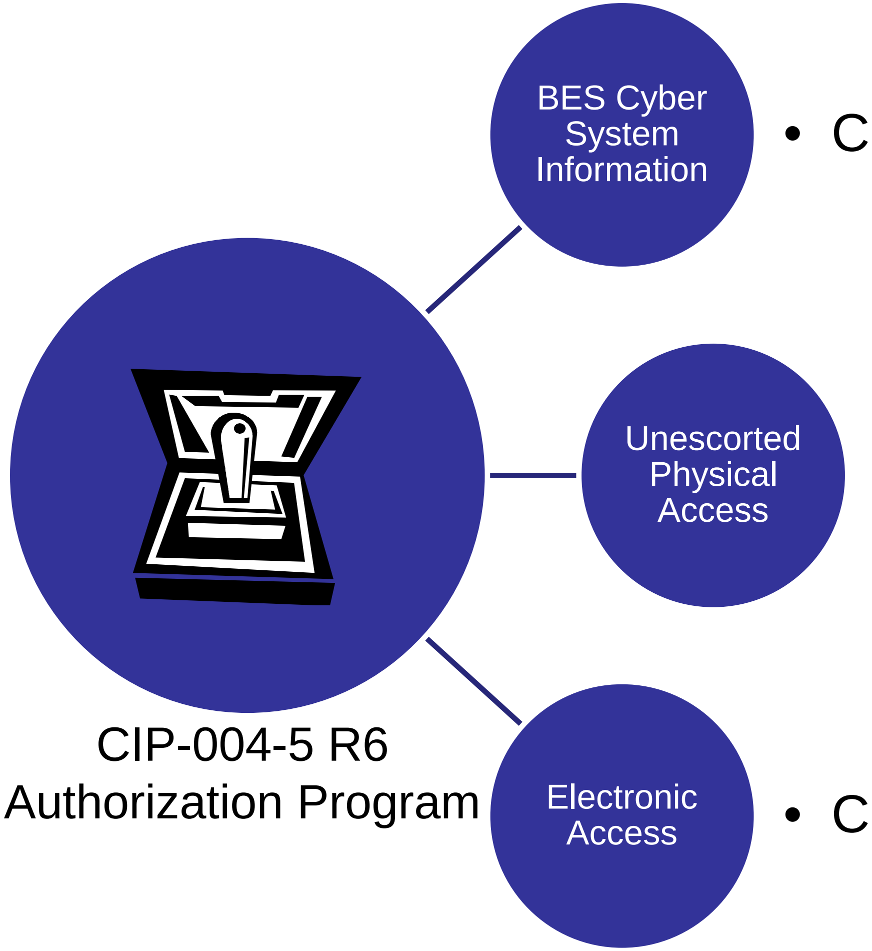
"The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."

- Take actions to remove the ability to access the BES Cyber System when access is no longer required

Requirements applicable to Low Impact

- Security Awareness – A security practice program that conveys the security awareness concepts, and provides on-going reinforcement of such concepts on at least a quarterly basis.

Access Authorization Program (1/2)



CIP-004-5 R6
Authorization Program

BES Cyber System Information

- CIP-003-4 R5

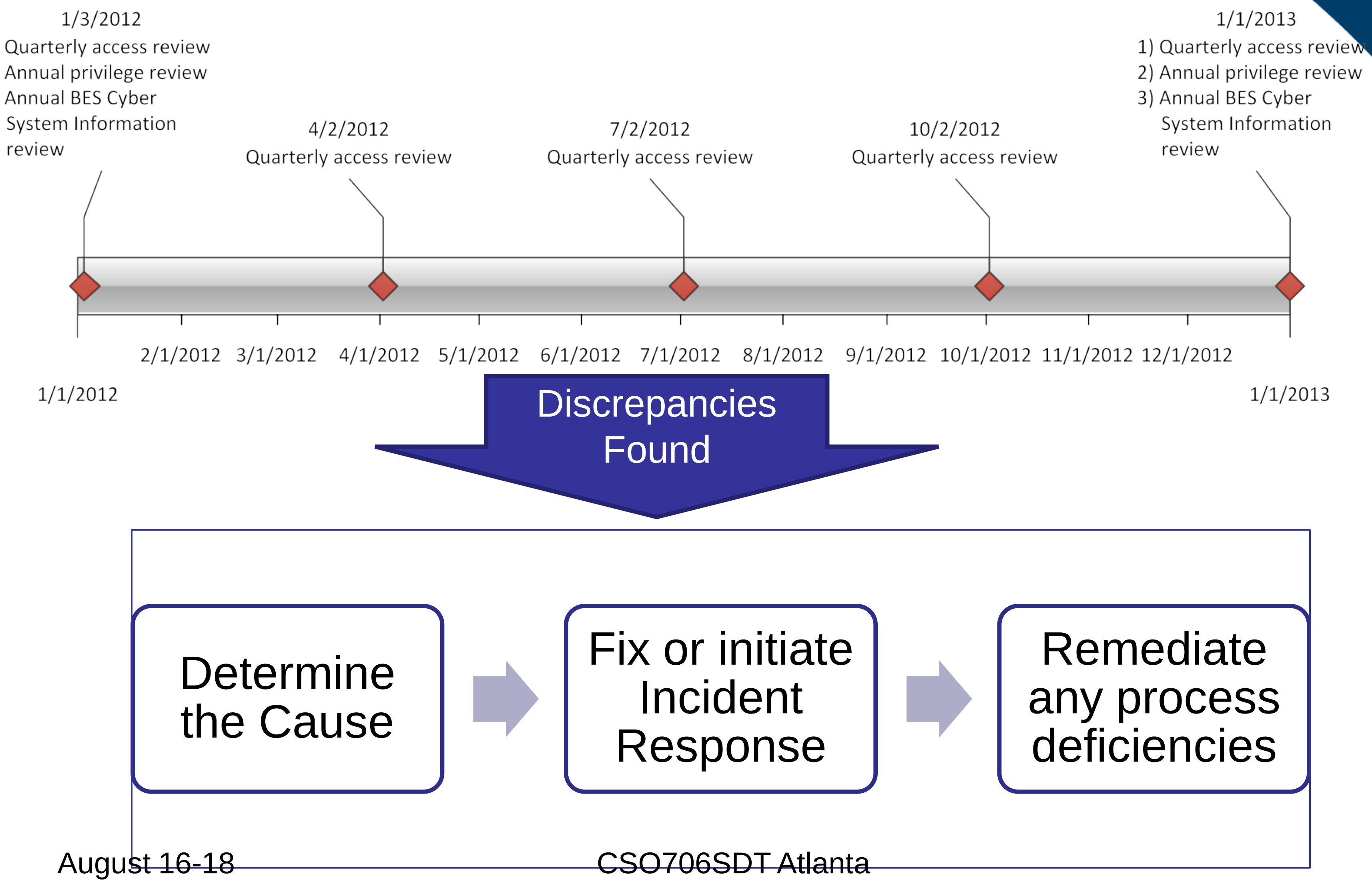
Unescorted Physical Access

- CIP-004-4 R4

Electronic Access

- CIP-007-4 R4

Access Authorization (2/2)



1/3/2012
Quarterly access review
Annual privilege review
Annual BES Cyber System Information review

4/2/2012
Quarterly access review

7/2/2012
Quarterly access review

10/2/2012
Quarterly access review

1/1/2013
1) Quarterly access review
2) Annual privilege review
3) Annual BES Cyber System Information review

Discrepancies Found

Determine the Cause

Fix or initiate Incident Response

Remediate any process deficiencies

Revocation of Access

- When access is no longer needed
  - Involuntary dismissals
  - Voluntary terminations
  - Retirements
  - Deaths
  - Transfers – Date determined by the entity
- Revoke ability to access
  - Physical access
  - Remote Access
- Complete the revocation process
  - Revoke individual user accounts within 30 days

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-005-5 Modifications

to ensure
the reliability of the
bulk power system

Summary of Modifications

- Define ‘External Connectivity’ for scope modification
- Focus on ‘Electronic Access Points’ vs. ESP
- Require IDS at Control Centers
- Add clarity to ‘secure’ dialups
- Consolidated Monitoring and Vulnerability Assessment Requirements in CIP-007 and CIP-011 respectively
- Removed Appropriate Use Banner
- Incorporated CIP-005-4 Urgent Action revisions

Trimmed Requirements

- R1.1 – 1.6 and 2.5 – New measures, rationale and guidance allow the removal of explanatory text in the Standard
- R2.6 (Appropriate Use Banner) – Not necessary for meeting the reliability objective
- R3 (Monitoring) – Consolidated in CIP-007-5 R4 to ensure consistency
- R4 (Vulnerability Assessment) – Consolidated and moved to CIP-010-5 R3
- R5 (Documentation Review and Maintenance) – Largely administrative requirement

Addressing FERC Directives (2 Security Measures – Defense in Depth)

FERC Order 706 Para. 496

“Commission adopts the CIP NOPR’s proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter.”

- Deploy methods to inspect communications and detect potential malicious communications for all External Connectivity (Intrusion Detection)

Requirements applicable to Low Impact

- R1. Electronic Security Perimeter
  - 1.1 Identify and secure Electronic Access Points
  - 1.2 Firewall controls
  - 1.3 Dial-up controls

Requirements Applicable to High Impact Only

- R1 Table 1.6
  - Deploy intrusion detection for all Electronic Access Points

Dial-Up

- Add clarity to ‘secure’ dialup
    - Secure each Electronic Access Point that utilizes dial-up access such that authentication occurs before establishing connectivity with the BES Cyber System

CIP-005-4 Urgent Action Revisions

- Addressing NERC Alert regarding remote access VPN vulnerabilities
- Creates basic requirements to protect critical systems from untrusted networks.
- Identifies protective measures that provide secure access to critical systems.
- Helps ensure secure practices by employees, contractors, and service vendors to minimize exploitation of vulnerabilities.

CIP-005-4 Urgent Action Revisions

- Addresses questions regarding ability to audit or enforce the requirement through the design of clear measures.
- Significant guidance to be provided to address implementation options for organizations of differing sizes, capabilities, and complexity.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Questions?

to ensure
the reliability of the
bulk power system

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-006-5 Modifications

Summary of Modifications

- Physical Security Program
  - Must define the operational or procedural controls to restrict physical access
  - Removed current “6 wall” wording to instead require Defined Physical Boundary
  - For High Impact, added the need to utilize two or more different and complementary physical access controls to restrict physical access
  - Testing changed to a 24 month cycle with ongoing discussions of different cycles based on environment.

Requirements applicable to Low Impact

- Define the operational or procedural controls to restrict physical access.

Addressing FERC Directives

- FERC Order 706 P572 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."
    - The SDT added this for High Impact BES Cyber Assets
- FERC Order 706 P581 "The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years,."
    - The SDT changed to a 24 month testing cycle but is also still discussing different cycles based on environment

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-007-5 Modifications

to ensure
the reliability of the
bulk power system

Summary of Modifications (1/2)

- Addition of physical I/O port requirement
- Security Patch mgt source requirement
- Non-prescriptive malware requirement
- Security Event Monitoring failure handling
- Bi-weekly log summary/sampling reviews

Summary of Modifications (2/2)

- Simplified access-control requirements, removed TFE language while strengthening password requirements
- Added requirement for maintenance devices
- Consolidated vulnerability assessment in CIP-010-5
- Disposal requirement moved to CIP-011-5

Requirements applicable to Low Impact

- Change or have unique default passwords on production BES Cyber Assets, Electronic Access Control Systems, Physical Access Control Systems and Protected Cyber Assets, where technically feasible.

Requirements Applicable to High Impact Only

- Bi-weekly log reviews - Review a summarization or sampling of logged events every two weeks to identify unanticipated Cyber Security Incidents and potential event logging failures. Activate a response to rectify any event logging failure identified from the review before the end of the next calendar day.

Addressing FERC Directives (Log Review)

FERC Order 706 Para. 525

"The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily…"

FERC Order 706 Para. 628

"Requirement R6 of CIP-007-1 does not address the frequency with which log should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly…"

- The SDT Proposes the performance of a review of log summaries or samples every two weeks.

Addressing FERC Directives (Malware)

FERC Order 706 Para. 620

"The Commission will not adopt Consumers' recommendation that every system in an electronic security perimeter does not need antivirus software. Critical cyber assets must be protected, regardless of the operating system being used. Consumers has not provided convincing evidence that any specific operating system is not directly vulnerable to virus attacks. Virus technology changes every day. Therefore we believe it is in the public interest to protect all cyber assets within an electronic security perimeter, regardless of the operating system being used…"

FERC Order 706 Para. 622

"The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above.

- Rewrote the requirement as a competency based requirement that does not prescribe technology.
- Added Maintenance to cover malware on removable media.

Addressing FERC Directives (Ports & Services)

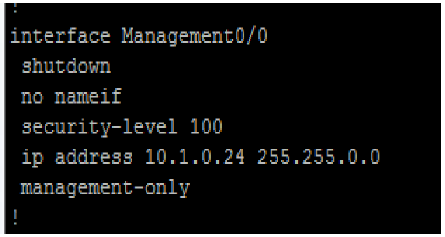
March 18th Order on ports/services

"The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."

- The SDT proposes to address this directive by having a requirement to disable or restrict use of physical I/O ports

Ports and Services

Acceptable ways to disable or restrict access.



```
!
interface Management0/0
 shutdown
 no nameif
 security-level 100
 ip address 10.1.0.24 255.255.0.0
 management-only
!
```

Configuration

Logically Disable

USB Lock

Restrict

Epoxy Glue

Permanently Disable

Security Event Monitoring

- Combines all monitoring requirements (CIP-005-4 R3, CIP-007-4 R5 and R6)
- Industry commented – What is monitoring? What are security events
  - Entity determines which events to **log** and which events necessitate **alerts**
- Draft CAN – Are logging system failures a violation?
  - Generate alerts for event logging failures

Access Control

- Moved access privilege review to CIP-004-5
- Simplified the requirement wording in controlling shared, administrative and generic accounts
- Minimize the need for TFEs for passwords
    - Password length is the minimum of 8 characters or maximum supported by the device
    - Strengthened the requirement by limiting or alerting on unsuccessful login attempts

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Questions?

to ensure
the reliability of the
bulk power system

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-008-5 Modifications

to ensure
the reliability of the
bulk power system

Summary of Modifications

- CIP-008-5 was primarily modified to satisfy the FERC 706 directives as follows:

Addressing FERC Directives

FERC Order 706 Para. 661

"the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."

1. Added: Reportable Cyber Security Incidents are either:

- Any malicious act or suspicious event or events that compromise, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a BES Cyber System.

  or

- Any event or events which have either impacted or have the potential to impact the reliability of the Bulk Electric System (Reliability Function CIP-002-5).

2. Retired R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in EOP-004-2, Requirement 1, Part 1.3. Will need to give instruction to report as a "Reportable Cyber Security Event" in EOP-004 space.

3. See R1.1 above

4. Guidance and measurements are being developed accordingly

Addressing FERC Directives

FERC Order 706 Para. 673

“The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report..”

Cyber Security - Incident Reporting and Response Planning: Retired R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in EOP-004-2, Requirement 1, Part 1.3 and Attachment 1

Addressing FERC Directives

FERC Order 706 Para. 676

“the Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report..”

– Cyber Security - Incident Reporting and Response Planning: Retired R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in EOP-004-2, Requirement 1, Part 1.3.

Addressing FERC Directives

FERC Order 706 Para. 686

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.."

R3.3 and R3.4 Includes additional specification on update of response plan Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-009-5 Modifications

Summary of Modifications

- CIP-009-5 was primarily modified to satisfy the FERC 706 directives as follows:

Addressing FERC Directives

FERC Order 706 Para. 694

"For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan..We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard"

Added specific R1 requirement to implement recovery plan

Addressing FERC Directives

FERC Order 706 Para. 739

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."

R1.5 Added requirements related to restoration processes based on review of the DHS Controls

Addressing FERC Directives

FERC
Order 706
Para. 748

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."

R1.5 : Processes for the restoration of BES Cyber Systems to the most current baseline configuration

Addressing FERC Directives

FERC
Order 706
Para. 706

“Preserve data for analysis”

CIP-009-5 1.6
Requires process to preserve data for analysis

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-010-5 Modifications

to ensure
the reliability of the
bulk power system

Summary of Modifications

- The SDT proposes the development of a new Standard CIP-010-5 that consolidates all references to Configuration Change Management and Vulnerability Assessments.
  - Previously these requirements were dispersed throughout CIP-003-4, CIP-005-4, and CIP-007-4

Summary of Modifications

- The SDT has made changes the Vulnerability Assessment requirements to
  - Consolidate the previous requirements in CIP-005-4 and CIP-007-4 into a single requirement
  - Make provisions for differences between Control Centers and field assets
  - Respond to FERC Order 706 regarding the performance of “active vulnerability assessments”

Addressing FERC Directives

FERC Order 706 Para. 397

"The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes."

- The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System.
- Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment prior to their implementation in the production environment to aid in identifying any accidental consequences of the change.

Addressing FERC Directives

FERC Order 706 Para. 609	“We therefore direct the ERO to develop requirements addressing what constitutes a “representative system” and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.”
FERC Order 706 Para. 610	“we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above.”
FERC Order 706 Para. 611	“the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production.”

- The SDT proposes to require a “representative system” or test system for those High Impact Control Centers to use for the purposes of testing proposed changes and performing active vulnerability assessments.
- The SDT proposes using the defined baseline configuration of a BES Cyber System for the measuring stick as to whether a test system is truly representative of the production system.
- To account for any additional differences between the two systems, the SDT proposes using the words directly from FERC Order 706 “Document 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.”

Addressing FERC Directives

FERC Order 706 Para. 541	“we adopt the ERO’s proposal to provide for active vulnerability assessments rather than full live vulnerability assessments.”
FERC Order 706. Para 542	“the Commission adopts the ERO’s recommendation of requiring active vulnerability assessments of test systems.”
FERC Order 706 Para. 547	“we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years”

- The SDT has added requirements for an “active vulnerability” assessment to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System.

Addressing FERC Directives

FERC Order 706 Para. 544

"the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification."

FERC Order 706 Para. 544

"we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment"

- The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new cyber asset undergo an active vulnerability assessment.
  - An exception is made for specified exceptional circumstances such as an emergency.

Baseline Configurations

- The SDT proposes the introduction of a requirement for a baseline configuration that would be used to determine when the Configuration Change Process is invoked as well as what constitutes a representative system.
  - “Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified in CIP-002-5:
    - Physical location
    - Operating System (including version)
    - Commercially available application software (including version) intentionally installed on the BES Cyber Asset
    - Any software/scripts developed for the entity
    - Logical network accessible ports
    - Enabled system services
    - Security patch levels”

Testing of Changes

- In additional to the current requirement to verify that a change does not impact the existing cyber security controls, the SDT proposes to expand this requirement to ensure that the availability of the BES Cyber System is not affected.
- For High Impact Control Centers, the SDT proposes that the change be tested in a test environment prior to implementation in the production environment.

Vulnerability Assessments

- The Vulnerability Assessment requirement now consists of the following components
  - Conduct a review for Low Impact BES Cyber Systems
  - Conduct passive vulnerability assessments for High and Medium Impact BES Cyber Systems every 12 months
  - Conduct active vulnerability assessments in a test environment for High Impact BES Cyber Systems every 36 months
  - Conduct active vulnerability assessments on new Cyber Assets in a High Impact BES Cyber System prior to placing the Cyber Asset into production.
  - Document and implement a remediation plan to correct any deficiencies found.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Questions?

to ensure
the reliability of the
bulk power system

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-011-5 Modifications

Summary of Modifications

- The SDT proposes the development of a new Standard CIP-011-5 that consolidates all references to Information Protection and Media Sanitization.
  - Previously these requirements were dispersed throughout CIP-003-4 and CIP-007-4
- The SDT has also moved the requirements regarding the authorization and revocation of access to BES Cyber System Information to CIP-004-5, consolidating these requirements with those for electronic and physical access.

Summary of Modifications

- The SDT has introduced a definition of a glossary term “BES Cyber System Information” which defines what needs to be protected.
  - Previously, this list was a requirement itself.

Summary of Modifications

- The SDT has shifted the focus of the requirements for media sanitization from the Cyber Asset to the information itself.
  - In version 4, these requirements are invoked when the Critical Cyber Asset is to be disposed of or redeployed.
  - In version 5, the requirement is triggered when either
    - BES Cyber System Information no longer needs to be stored on specific media, or
    - Media containing BES Cyber System Information is designated for disposal

Addressing FERC Directives

FERC Order 706 Para. 633

"The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it."

FERC Order 706 Para 635

"the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."

- The SDT has proposed that preventing unauthorized retrieval of data means to "render the data unrecoverable."
- The SDT understands that this may be too high of a bar and is continuing discussions in this area.

Information Protection

- Previous versions of the CIP Standards required that information be identified, classified, and protected.
- The SDT noted that while previous standards required that information be classified based upon its sensitivity, it did not require a difference in the protection pursuant to the information's sensitivity.
  - The SDT has thus removed the requirement to classify information without preventing an entity from performing this function if it so chooses.
- The SDT proposes for version 5 that the requirements to "protect" and manage access to information be replaced with a requirement for "labeling, handling (including storage, transit, and usage), and access control procedures."

Media Sanitization

- As previously mentioned, the SDT has shifted the focus of the media sanitization requirements from the Critical Cyber Asset to the information itself.
- The SDT has proposed the language that media be “erased, using a method to render the data unrecoverable.”
    - However, we believe that this would be difficult to audit and could be a constantly changing requirement due to the evolution of techniques to recover data, including some that are of a classified nature.

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Thank you