

# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

## CIP Standards Version 5 Requirements & Status

Philip Huff – Arkansas Electric Cooperative Corporation  
Doug Johnson – Commonwealth Edison Company  
David Revill – Georgia Transmission Corporation

CS0706 SDT Webinar  
August 24, 2011

to ensure  
the reliability of the  
bulk power system

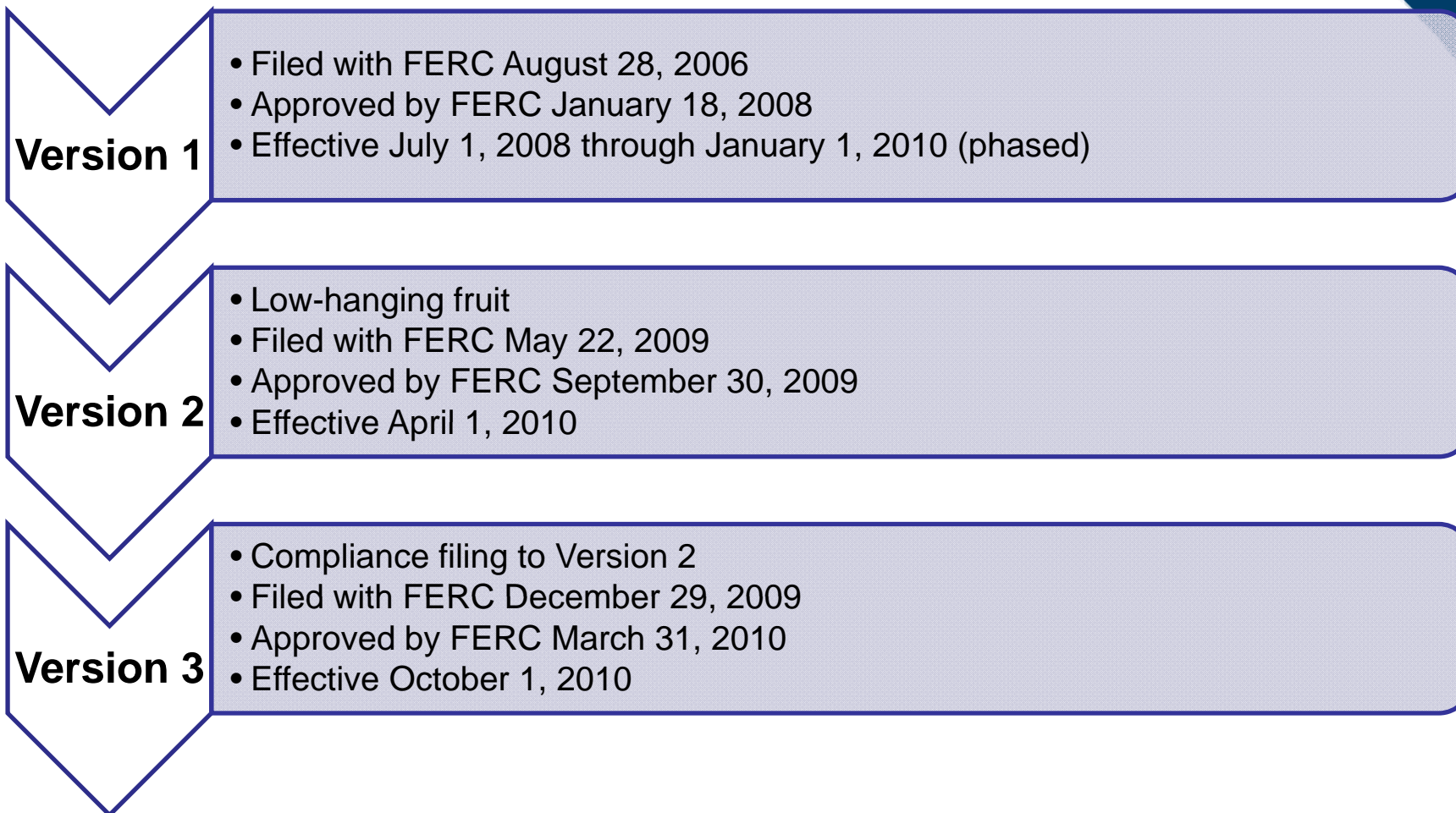
Background

Version 4 - Overview

Version 5 – Requirements Summary

Schedule and Implementation Plan

# Project Background



- **Version 4** of the CIP Standards
- Approved by Industry **December 30, 2010**
- Submitted to FERC **February 10, 2011**
  - 2,232 page filing
  - Filing included CIP-002-4 through CIP-009-4, but only changes in CIP-002-4

# Looking Ahead to Version 5

- The SDT continues work to address the remaining 50+ issues in Order 706
  - Version 5 builds on CIP-002-4 and previous drafts of CIP-010 & 011
  - Use similar content structure and terminology as previous CIP Standards (CIP-002 through CIP-009)



# 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 5:** To minimize technical feasibility exceptions

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

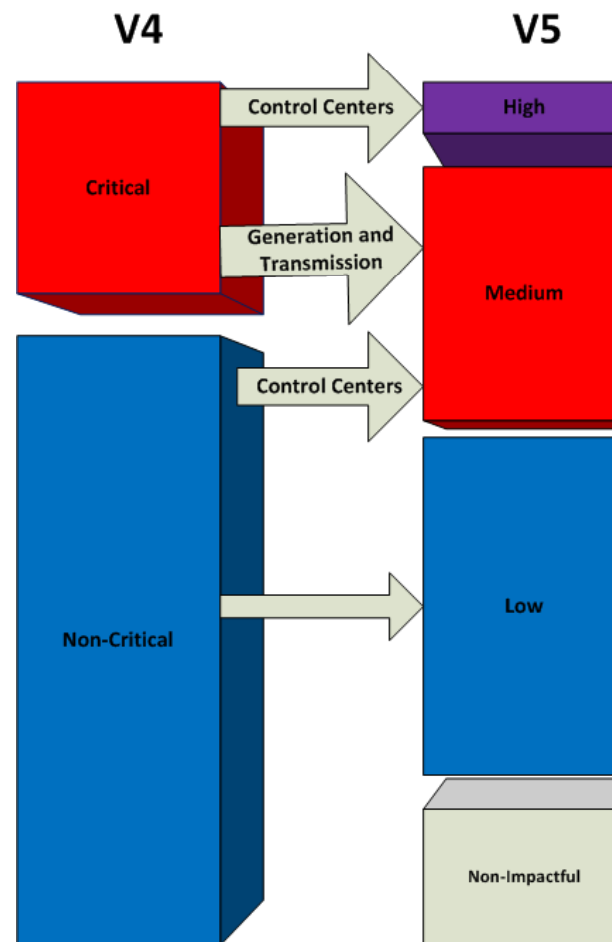
**Goal 3:** To provide guidance and context for each Standard Requirement

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

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

# 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



## **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

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

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

Disabling ports and services refers to all of network accessible ports, any system services and 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 enable ports and services and (R2.2) disable all other ports and services. Disabling ports and services in normal and emergency operations is equivalent to both of these requirements. Therefore, the original R2.2 was removed.

**Additional Guidance:**

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

## 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 compliance associated with the requirement row

## 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

# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

---

## CIP-002-5 – CIP-011-5

---

to ensure  
the reliability of the  
bulk power system



# CIP-002-5 Summary of Modifications

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

# CIP-002-5 Impact Criteria (Attachment 1)

- High: Large Control Centers (e.g. RC, BA, TOP)
- Medium: 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



# CIP-003-5 Summary of Modifications (1/2)

- 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

- 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

## 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.

- 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.

- 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”

## ■ 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



# CIP-004-5 Addressing FERC Directives (Training)

## FERC Order 706 Para. 433

“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.”

## FERC Order 706 Para. 434

“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.”

## FERC Order 706 Para. 435

“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 addressed this by identifying the training topics that should be provided in the Training Program.
- The SDT added this as a topic for role specific training.
- Take actions to remove the ability to access the BES Cyber System when access is no longer required

# CIP-004-5 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

## CIP-005-5 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

# CIP-005-5 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)

# CIP-006-5 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

# CIP-006-5 Addressing FERC Directives

## FERC Order 706 Para. 572

“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 Para. 581

“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



# CIP-007-5 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

# CIP-007-5 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

# CIP-007-5 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.

# CIP-007-5 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.

# CIP-007-5 Addressing FERC Directives (Ports & Services)

March 18<sup>th</sup>  
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

## CIP-008-5 Summary of Modifications

- Defined Reportable Cyber Security Incident
- Working to harmonize with EOP-004-2
- Includes additional specification on update and lessons learned associated with the response plan



# CIP-008-5 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.”

A1

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

## Slide 33

---

A1

Rework text format to be consistent with other slide formats (bullets and fonts).Applied to tother slides in CIP-008 and CIP-009 as well.

Author, 8/19/2011

# CIP-008-5 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

# CIP-008-5 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.

# CIP-008-5 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

# CIP-009-5 Summary of Modifications

- Added requirement to implement the response plan
- Verification of backup media information prior to storage
- Preservation of data for analysis

# CIP-009-5 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

# CIP-009-5 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



# CIP-009-5 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

# CIP-009-5 Addressing FERC Directives

**FERC  
Order 706  
Para. 706**

**“Preserve data for analysis”**

CIP-009-5 1.6

Requires process to preserve data for analysis

# CIP-010-5 Requirements Summary

- 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

# CIP-010-5 Requirements Summary

- 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”

## 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.

# CIP-010-5 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.”

# CIP-010-5 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.

# CIP-010-5 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.



# CIP-011-5 Requirements Summary

- 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

# CIP-011-5 Requirements Summary

- 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

- 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

# CIP-011-5 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

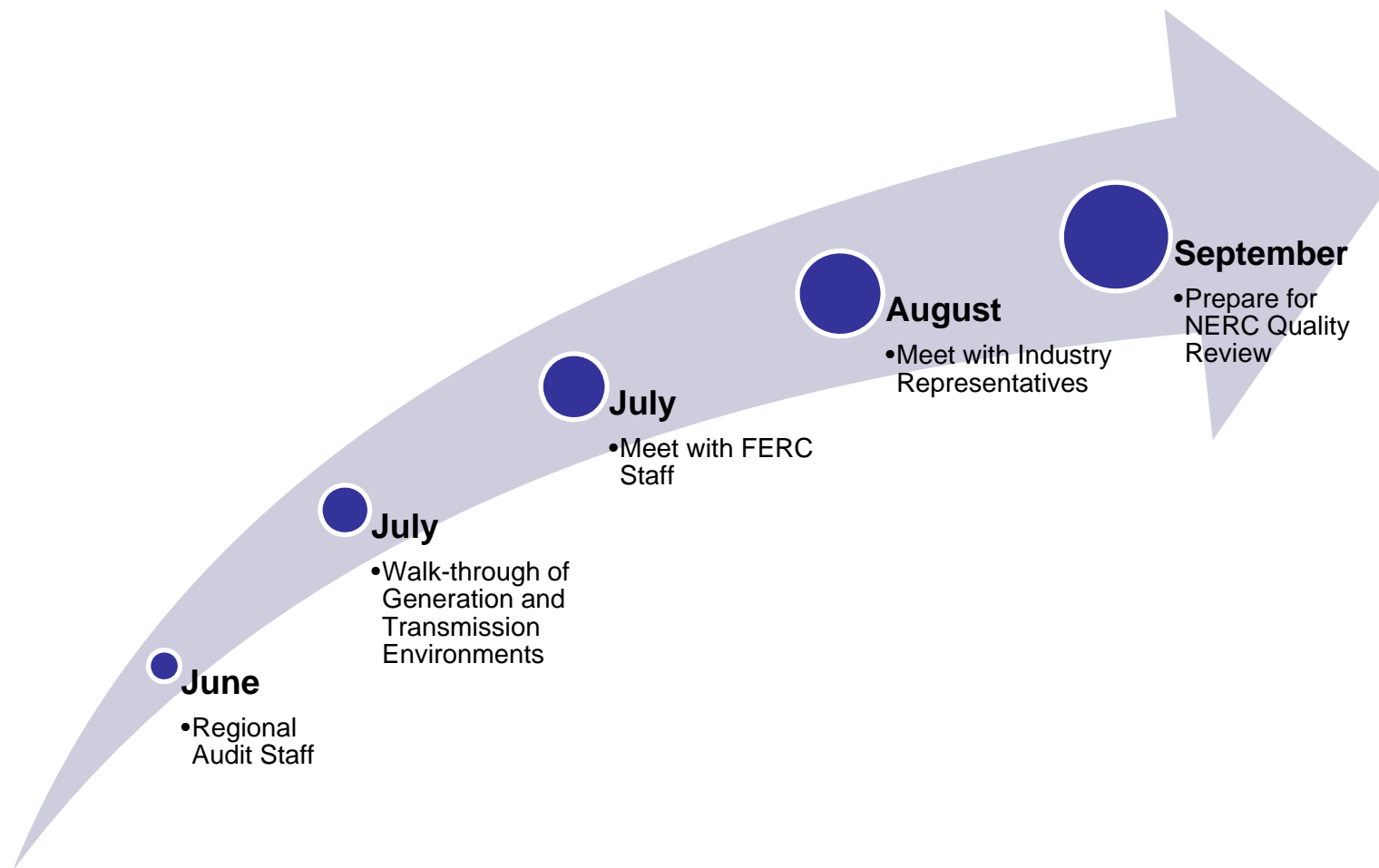
“the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data.”

- 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.

- Implementation plan is in the very early phases of development
- Current concepts include staggered Effective Dates for:
  - CIP-002-5
  - Organizational Requirements (CIP-003-5, CIP-008-5)
  - Technical Requirements (CIP-005-5, CIP-006-5, etc.)
- Technical Requirements would be further staggered by:
  - High Impact BES Cyber Systems
  - Medium Impact BES Cyber Systems
  - Low Impact Cyber Systems

- Currently evaluating a single implementation plan that would include compliance timelines for future newly identified BES Cyber Systems and those BES Cyber Systems that change categories
  - Eliminates the separate Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (IPFNICCANRE)

# Schedule to Date – 2011



August 24, 2011

CSO706 SDT Webinar

# Key Dates Moving Forward

- **November 3<sup>rd</sup>, 2011** –  
*First Posting for Comment and Ballot*
  - Webinars – November 15<sup>th</sup> and 29<sup>th</sup>, 2011
  - Ballot Opens – December 9<sup>th</sup>, 2011
  - Ballot Closing – December 19<sup>th</sup>, 2011



# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

## Questions?

---

*Points of Contact:*

Philip Huff – [philip.huff@aecc.com](mailto:philip.huff@aecc.com)

Doug Johnson – [douglas.johnson@comed.com](mailto:douglas.johnson@comed.com)

David Revill – [david.revill@gatrans.com](mailto:david.revill@gatrans.com)

---

Slides and Recording of Webinar will be Posted  
(on NERC Website)

to ensure  
the reliability of the  
bulk power system