NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft CIP Standards Version 5

Technical Webinar – Part 2

Project 2008-06 Cyber Security Order 706 Standards Drafting Team
November 29, 2011

RELIABILITY | ACCOUNTABILITY




NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda

- Opening Remarks – John Lim, Consolidated Edison, Chair
- V5 Schedule Update – Philip Huff, AECC, Vice Chair
- V5 Standards Format – Sharon Edwards, Duke Energy
- Definitions – William Winters, Arizona Public Service
- CIP-003-5 through CIP-011-1 – SDT Members
- Q&A – Steven Noess, NERC

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Version 5 Schedule Update

Philip Huff, Arkansas Electric Cooperative Corporation

RELIABILITY | ACCOUNTABILITY

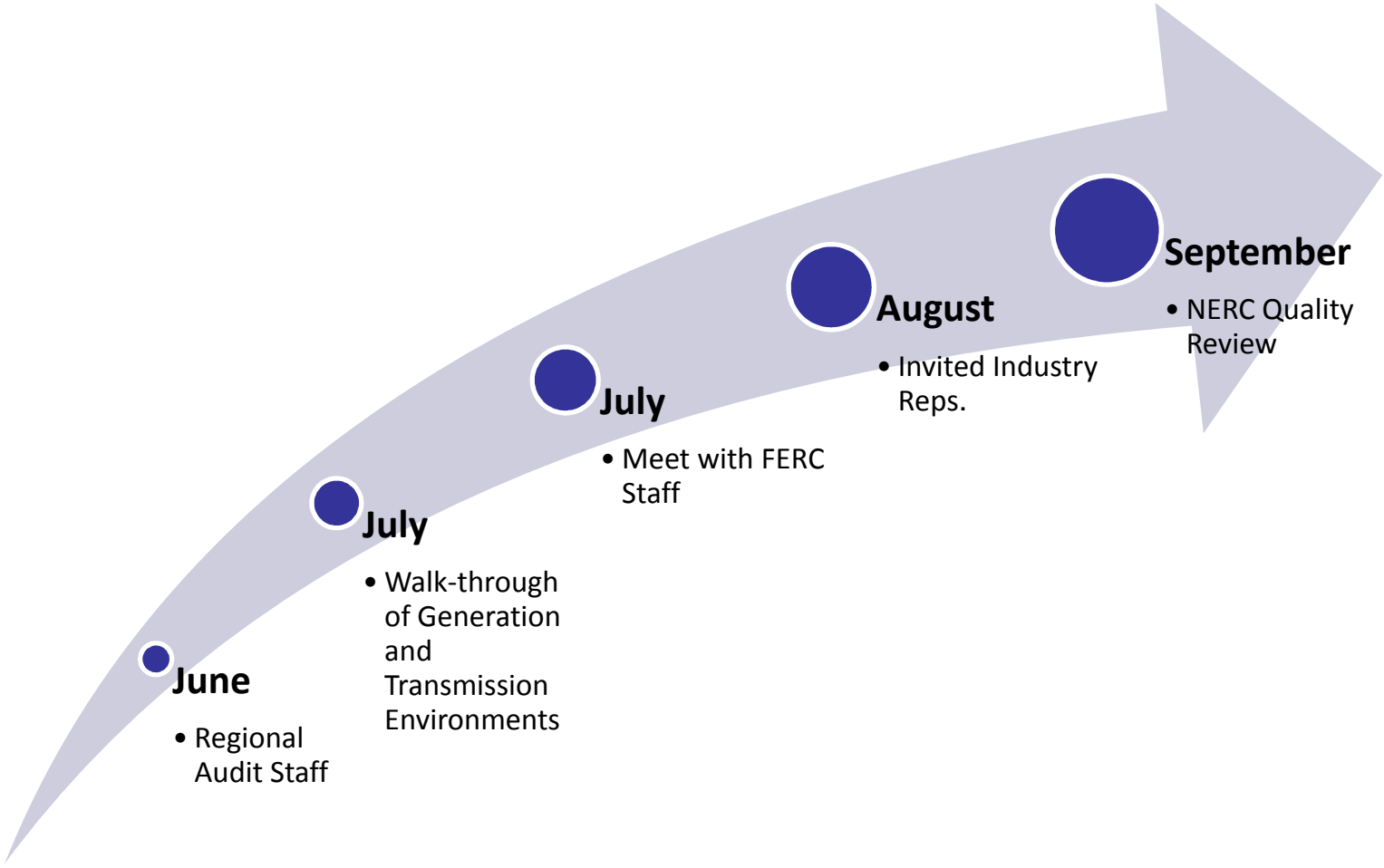



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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.	

Development Schedule



Comment and Ballot Period

- November 7, 2011 – January 6, 2012
  - Formal 60-day comment period
- December 16, 2011 – January 6, 2012
  - Initial Ballot

Long Term Schedule 2012

January 6 – March 26	• Consideration of comments
March 26 – April 27	• 30-day posting for comment and successive ballot
June 6–22	• Possible Recirculation ballot

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Version 5 Standards Format

Sharon Edwards, Duke Energy

RELIABILITY | ACCOUNTABILITY




Format Components – CIP 005

Rationale for R1: The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks ….

Summary of Changes: CIP-005 R1 has taken more of a focus on the discrete Electronic Access points rather than the logical "perimeter".

CIP-005 R1.2 has been deleted. This requirement was definitional in nature and used to bring dialup modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists, therefore there is no need for this requirement.

CIP-005 R1.1 and 1.3 were also definitional in nature and have been deleted as separate requirements but the concepts were integrated into the definitions of ESP and EAP.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter. [Violation Risk Factor: Medium]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

	CIP-005-5 Table R1 – Electronic Security Perimeter		
Part	**Applicability**	**Requirements**	**Measures**
1.1	Low Impact BES Cyber Systems with External Routable Connectivity	Define technical or procedural controls to restrict unauthorized electronic access.	Evidence may include, but is not limited to, documented technical and procedural controls that exist and have been implemented.
Reference to prior version: *CIP-005 R1*		**Change Rationale:** *Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones and to prevent access to an aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Protected Cyber Assets	Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	Evidence may include, but is not limited to: • Network diagrams showing EAP identification or • A list of uniquely identifiable Cyber Assets within the BES Cyber System and assoc. EAPs.

- **Rationale for the requirement**
- **Summary of changes from previous version**
- **Main requirement and measure**
- **Requirement rows**
  - **Applicability**

    (low, medium, high)
  - **Sub-requirements**
  - **Measures for sub-requirements**
  - **Reference to prior versions**
  - **Change rationale for sub-requirement**

Format – Rationale and Summary of Changes Sections

Rationale for R1: The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005 R1 has taken more of a focus on the discrete Electronic Access points rather than the logical "perimeter".

CIP-005 R1.2 has been deleted. This requirement was definitional in nature and used to bring dialup modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists, therefore there is no need for this requirement.

CIP-005 R1.1 and 1.3 were also definitional in nature and have been deleted as separate requirements but the concepts were integrated into definitions.

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

Format – Main Requirement and Measure

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

- **Requirement** specifies what is needed for compliance
- **Measure** explains the type of evidence that must be included to demonstrate compliance
- Most requirements reference a **table** immediately below

Format – Requirement Rows

	CIP-005-5 Table R1 – Electronic Security Perimeter		
Part	**Applicability**	**Requirements**	**Measures**
1.1	Low Impact BES Cyber Systems with External Routable Connectivity	Define technical or procedural controls to restrict unauthorized electronic access.	Evidence may include, but is not limited to, documented technical and procedural controls that exist and have been implemented.
Reference to prior version: *CIP-005 R1*		**Change Rationale:** *Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones and to prevent access to an aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES.*	

- **Requirement row specifics – Low Impact - CIP 005**
  - Sub requirement number
  - Applicability – Identifies the groups of assets which must comply with requirement
  - Requirement – Specifies what is needed for compliance with sub requirement
  - Measures – Explains how compliance with sub requirement may be demonstrated
    - Documented and implemented technical or procedural controls
  - Reference to prior to version – Identifies where the requirement was previously found in CIP
  - Change rationale related to the sub requirement

Format – Requirement Rows

	CIP-005-5 Table R1 – Electronic Security Perimeter		
Part	**Applicability**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Protected Cyber Assets	Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	Evidence may include, but is not limited to: • Network diagrams showing EAP identification or • A list of uniquely identifiable Cyber Assets within the BES Cyber System and associated EAPs.
Reference to prior version: *CIP-005 R1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and BES Cyber System*	

- **Requirement row specifics – High and Medium Impact – CIP 005**
  - Sub requirement number
  - Applicability – Identifies the groups of assets which must comply with requirement
  - Requirement – Specifies what is needed for compliance
    - Controls apply to identified Electronic Access Points
  - Measures – Explains how compliance with sub requirement may be demonstrated
  - Reference to prior to version – Identifies where the requirement was previously found in CIP

Format – Applicability

- **All Responsible Entities**
- **BES Cyber System :** One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services.
  - High Impact BES Cyber Systems
  - Medium Impact BES Cyber Systems
  - Low Impact BES Cyber Systems
- **Electronic Access Control or Monitoring Systems :** Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems.
- **Physical Access Control Systems :** Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers.
- **Protected Cyber Asset:** A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the BES Cyber System. A Transient Cyber Asset is not considered a Protected Cyber Asset.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Version 5 Definitions

William Winters, Arizona Public Service

RELIABILITY | ACCOUNTABILITY




Definitions

- Consolidated in a single document, which is referenced in the Definitions section of each standard
- Terms already defined in the Glossary of Terms used in NERC Reliability Standards are not repeated here
- New or revised definitions become approved when the proposed standard is approved
- **When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary**
- New defined terms are underscored
- For existing glossary terms, new language is shown as underscored, while deleted language is shown as stricken

Definitions Retired and Replaced

- Critical assets
  - Replaced by CIP-002 Attachment 1 and BES Reliability Operating Services definition
- Critical cyber assets
  - Replaced by BES Cyber Asset and BES Cyber System
- Physical security perimeter
  - Replaced by Defined Physical Boundary
  - No more “six-wall” specification

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Definitions
18 New, 3 Revised

	CIP002	CIP003	CIP004	CIP005	CIP006	CIP007	CIP008	CIP009	CIP010	CIP011
BES Cyber Asset	x					x			x	x
BES Cyber Security Incident						x	x		x	
BES Cyber System	x	x	x	x	x	x		x		
BES Cyber System Information										x
BES Reliability Operating Services	att 1									
CIP Exceptional Circumstance			x			x			x	
CIP Senior Manager	x	x	x			x			x	
Control Center	att 1									
Cyber Assets				x					x	
Defined Physical Boundary (“DPB”)					x					
Electronic Access Control or Monitoring Systems					x	x			x	
Electronic Access Point (“EAP”)				x		x				
Electronic Security Perimeter (“ESP”)				x						
External Connectivity										
External Routable Connectivity				applicability						
Interactive Remote Access				x						
Intermediate Device				x						
Physical Access Control Systems					x	x				
Protected Cyber Asset				x		x				
Reportable BES Cyber Security Incident							x			
Transient Cyber Asset						x				

Definitions
Core Applicable Assets

- **Cyber Assets** – Programmable electronic devices including the hardware, software, and data in those devices
- **BES Cyber Asset** – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services
- **BES Cyber System** – One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services
  - Largely replaces Critical Cyber Asset
  - Provides an opportunity for controls to be applied at a system level

Definitions
Related Applicable Assets

- **Electronic Access Control or Monitoring Systems** – Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems
- **Electronic Access Point** – An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets
- **Intermediate Device** – A Cyber Asset that 1) may be used to provide the required multi-factor authentication for the interactive remote access; 2) may be a termination point for required encrypted communication; and 3) may restrict the interactive remote access to only authorized users
- **Physical Access Control Systems** – Cyber Assets that control, alert, or log access to the Defined Physical Boundary exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers

Definitions
Related Applicable Assets

- **Protected Cyber Asset** – A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the BES Cyber System
- **Transient Cyber Asset** – A Cyber Asset that is; 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset, 2) used for data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System

Definitions Boundaries

- **Electronic Security Perimeter ("ESP")** – A collection of Electronic Access Points that protect one or more BES Cyber Systems
  - Asset based definition
  - Physical not logical
- **Defined Physical Boundary ("DPB")** – The physical border surrounding locations in which BES Cyber Assets, BES cyber Systems, or Electronic Access Control Systems reside and for which access is controlled
  - Replaces PSP definition
  - Provides for flexibility in physical boundary access controls
  - Not limited to "six-wall" perimeter
  - Does not exclude "six-wall" perimeter

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-003-5: Security Management Controls

David Revill, Georgia Transmission Corporation

RELIABILITY | ACCOUNTABILITY




CIP-003-5 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-010-1
  - Elements that addressed Information Protection were moved to CIP-011-1

CIP-003-5 Summary of Modifications

- Leadership – R1
- Policy – R2
  - Removed reference to policy addressing all “requirements”
  - Introduction of 10 topics based on the titles of each of the CIP standards with the addition of Remote Access and CIP Exceptional Circumstances
  - Remote Access policy elements from past CIP-005 Urgent Action process
- Exceptions to Policy
  - Requirement removed
- Policy Approval – R3

CIP-003-5 Summary of Modifications

- Awareness of the Policy – R4
  - Allows additional flexibility from previous requirement to make the policy “readily available”
- Delegation Authority – R5
  - Establishes a framework to clearly address FERC Order 706 and the 2003 Blackout Report
  - Attempt to add clarity to the expectation of the requirement allowing for delegations
  - Explicitly allows for delegation of the delegation authority
  - Delegations may be established by position
- CIP Senior Manager and Delegation Updates – R6
  - Footnote: Delegations remain in effect after a change in the CIP Senior Manager

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-004-5: Summary of Modifications

Jerry Freese, American Electric Power

RELIABILITY | ACCOUNTABILITY




CIP-004-5 Summary of Modifications

- Security Awareness – R1
  - Continues with awareness and quarterly reinforcement – Applicable to all responsible (functional) entities but those with authorized access not singled out
- Training – Role-based – R2
  - Identification of roles and specific role-based training
  - Addition of visitor control program
  - Electronic interconnectivity supporting the interoperability of BES Cyber Systems with other cyber assets
  - Storage media as part of the handling of BES Cyber Systems information
- Training Documentation and Implementation – R3
  - Differentiates training provisions to cover both the “program” requirements and “implementation” requirements

CIP-004-5 Summary of Modifications

- Training Documentation and Implementation – R3 Continued
  - Training prior to granting authorized access modified for CIP Exceptional Circumstances
  - Further defines ‘Annual’ as calendar year not to exceed 15 months

CIP-004-5 Summary of Modifications

- Personnel Risk Assessment – R4
  - Identity verification limited to initial PRA only
  - Seven-year criminal history checks add all locations of 6 month or more duration where the subject resided, was employed or attended school
  - Provides for partial criminal history checks with documented reasons for any omissions
  - Includes documenting the processes used to determine when to deny access
  - Differentiates training provisions to cover both the “program” requirements and “implementation” requirements
  - Separates contractors and service vendors into different table (R5)

CIP-004-5 Summary of Modifications

- R5 Verifying Individuals with access to BES Cyber Systems have been assessed for risk (Includes Contractors, Vendors) prior to authorization
  - Primary change – Measure allows vendor attestations verifying PRAs were completed prior to access being authorized
  - Other measure includes dated records verifying that PRAs were completed prior to authorizing access
  - Seven-year update removed the “for cause” renewal

CIP-004-5 Summary of Modifications

- Access Authorization – R6
  - Consolidated authorization and review requirements from CIP-003-4, CIP-004-4, CIP-006-4 and CIP-007-4
  - Enable quarterly and annual reviews to find and fix problems rather than self-report everything as a violation
  - Substitutes “provisioning-to-authorization” comparison for individual account listings on all BES cyber assets
  - List of authorized personnel no longer required
  - The CIP Senior Manager or delegate must authorize electronic and physical access to BES Cyber Systems and access to BES Cyber System Information

CIP-004-5 Summary of Modifications

- Authorization – R6 Continued
  - Quarterly verification that those individuals provisioned for unescorted physical or electronic access are authorized
  - Annual verification that all account groups or role categories and associated privileges are correct and the minimum required
  - Annual verification that access privileges to BES Cyber System Information are correct and the minimum required

CIP-004-5 Summary of Modifications

- Revocation – R7
- Addresses "immediate" access revocation when the need for access no longer exists, job changes, or end of employment (FERC Order 706, Paragraph 460)
  - Resignations/Terminations: revoke concurrent with time of resignation or termination (Physical and Interactive Remote Access)
  - Reassignments/Transfers: End of next calendar day (Electronic and Physical Access)

CIP-004-5 Summary of Modifications

- Access Revocation Continued
  - Revoke Access to BES Cyber System Information (end of next calendar day)
  - Revoke user accounts within 30 days of initial access revocation
  - Transfers, reassignments, resignations, terminations
    - Change passwords for shared accounts within 30 days, or if there are extenuating circumstances, within 10 days of the end of extenuating circumstances

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-005-5: Electronic Security Perimeter(s)

Christine Hasha, Electric Reliability Council of Texas

RELIABILITY | ACCOUNTABILITY




CIP-005 Summary of Modifications

- Define ‘External Routable Connectivity’ for scope modification
- Focus on ‘Electronic Access Points’ of the ESP
- Require IDS at Control Centers
- Add clarity to ‘secure’ dialups
- Inclusion of Remote Access requirements

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-006-5: Physical Security

Kevin Sherlin, Sacramento Municipal Utility District

RELIABILITY | ACCOUNTABILITY




CIP-006-5 Summary of Modifications

- Physical Security of BES Cyber Systems
  - Defined Physical Boundary replaces Physical Security Perimeter ("six-wall border")
- R1 – One or More Physical Security Plans
  - Low Impact – Operational or procedural controls to restrict physical access
  - Medium Impact – Establish one or more Defined Physical Boundaries with at least one physical access control; issue real-time alerts; log of physical entry
  - High Impact – Establish one or more Defined Physical Boundaries with two or more different and complementary physical access controls; issue real-time alerts; log of physical entry

CIP-006-5 Summary of Modifications

- R1 – One or More Physical Security Plans Continued
  - Physical Access Control System – Issue real-time alerts
- R2 – Visitor Control Program
  - High/Medium Impact – Continuous escorted access within Defined Physical Boundary; log entry/exit on a 24 hour basis to each Defined Physical Boundary
- R3 – Maintenance and Testing
  - Physical Access Control System - Testing changed to a 24 month cycle to include locally mounted devices
  - Physical Access Control System – Log failures and outages

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-5: Systems Security Management

Jay Cribb, Southern Company

RELIABILITY | ACCOUNTABILITY




CIP-007 Summary of Modifications

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-008-5: Incident Reporting and Response Planning

Thomas Stevenson, Constellation Energy

RELIABILITY | ACCOUNTABILITY



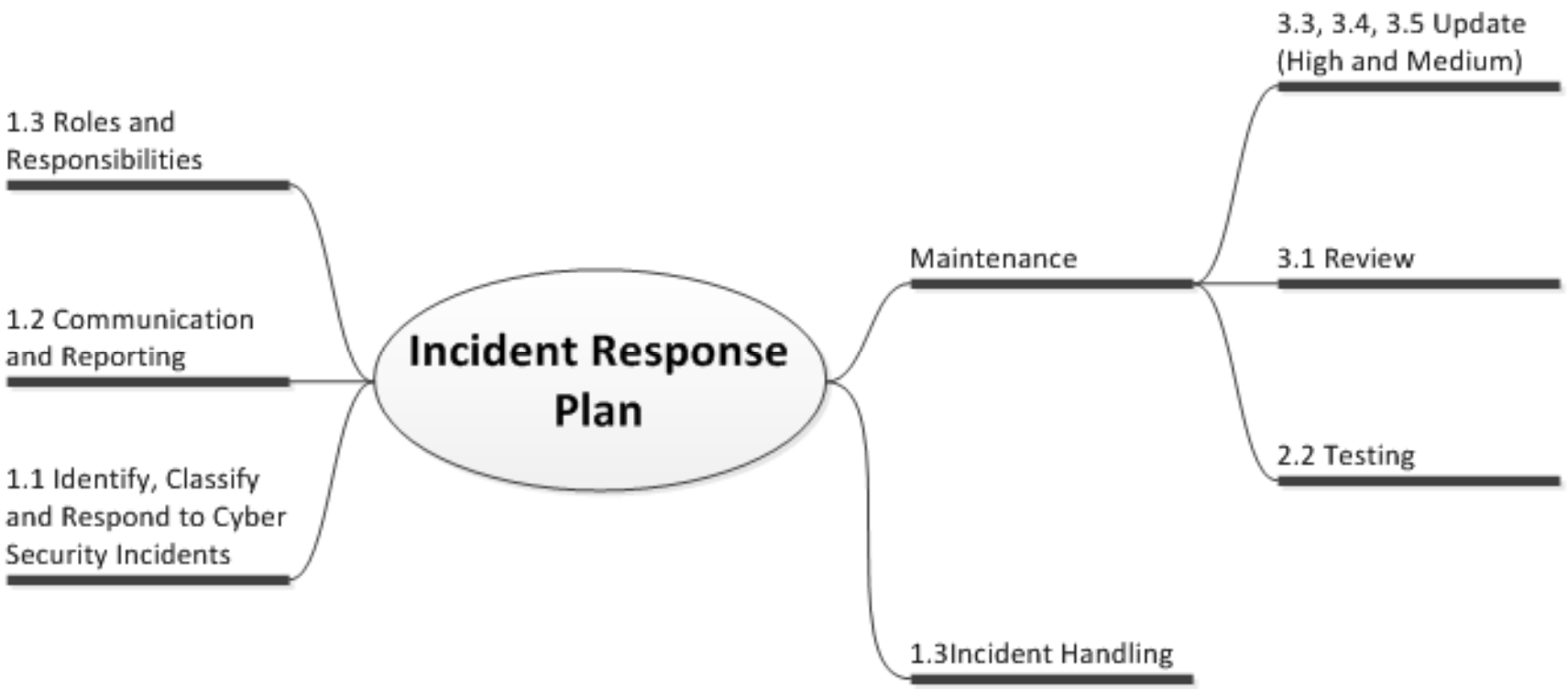

CIP-008-5 Summary of Modifications

- Defined Reportable Cyber Security Incident for clarity
- Harmonized with EOP-004-2 regarding specific reporting requirements
- Included additional specification on update and lessons learned associated with the response plan

Applying to All Responsible Entities

- CIP-008 R1, R2 and 3.1 apply to all Responsible Entities
- Possible to have a single plan – Not per Cyber System
- Rationale
  - Increases the ability of the industry to coordinate a response in a multi-site cyber attack. Every entity has a plan and knows who to contact.
  - High return for minor effort. Not the same degree of maintenance required for preventative controls (i.e. access control, patch management).
  - Key part of a basic security program.

Incident Response Plans



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-009-5: Recovery Plans for BES Cyber Systems

Thomas Stevenson, Constellation Energy

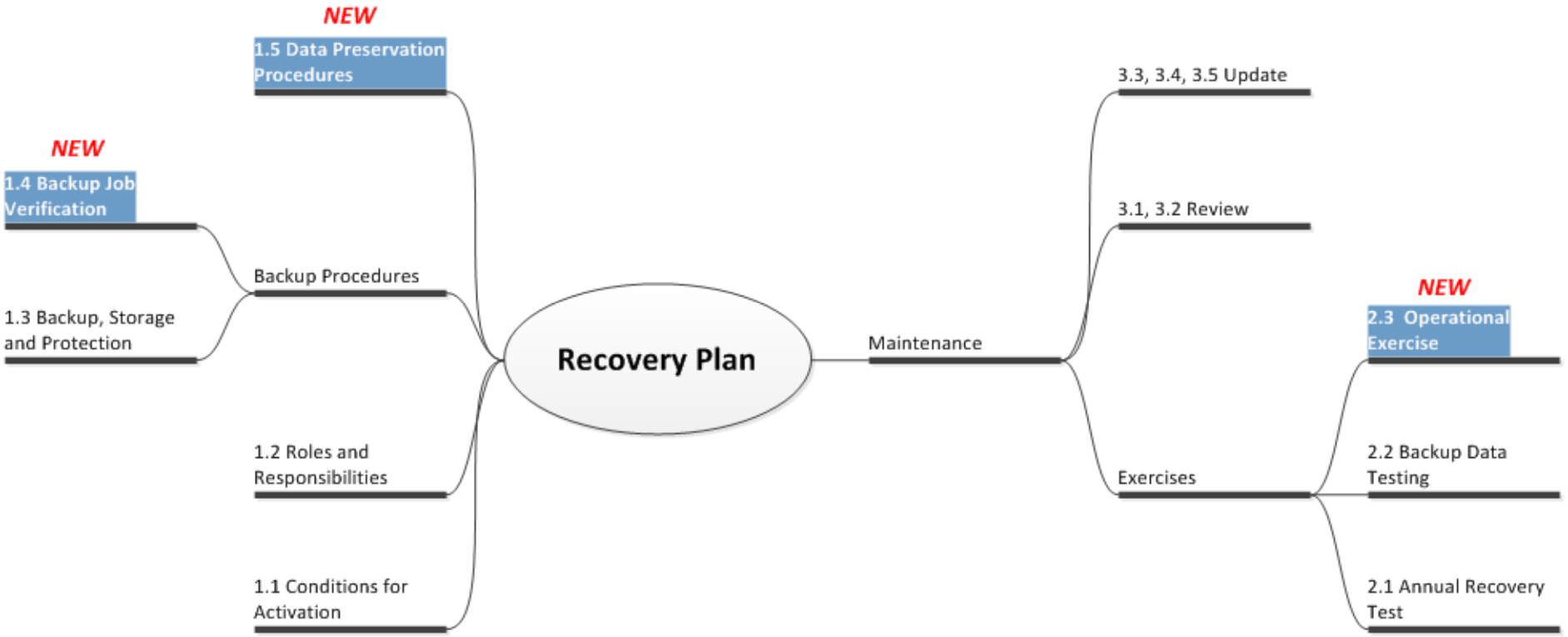
RELIABILITY | ACCOUNTABILITY




CIP-009-5 Summary of Modifications

- Added requirement to implement the recovery plan
- Verification of backup media information prior to storage
- Preservation of data for analysis
- Requirements Similar to CIP-008 structure
  - (R1) Plan, (R2) Exercise, (R3) Maintain

Recovery Plans



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-010-1: Configuration Change Management

David Revill, Georgia Transmission Corporation

RELIABILITY | ACCOUNTABILITY




CIP-010-1 Summary of Modifications

- Configuration Change Management – R1
  - Previously these requirements were dispersed throughout CIP-003-4, CIP-005-4, and CIP-007-4

CIP-010-1 Summary of Modifications

- The SDT proposes the development of a new Standard CIP-010-1 that consolidates all references to Configuration Change Management and Vulnerability Assessments
  - Use of a baseline to add clarity on when the change management process should be invoked
  - Explicit requirement for authorization of changes
  - Tied update of documentation to the change process
  - Clarified testing requirements
    - Testing in a test environment prior to implementation for High Impact BES Cyber Systems
    - Verification of security controls after a change is implemented for High and Medium Impact BES Cyber Systems (and other associated systems)

CIP-010-1 Summary of Modifications

- Configuration Monitoring – R2
  - New requirement for High Impact BES Cyber Systems
  - Responsive to FERC Order 706 ¶ 397 to address potential malicious actions in the change process
- Vulnerability Assessments – R3
  - Paper vs. active vulnerability assessment
    - Additional detail provided in guidance
  - Active vulnerability assessment required every 3 years for High Impact BES Cyber Systems (FERC Order 706 ¶ 541, 542, 544, 547)
  - Mitigation plan now included "planned date of completion" as per FERC Order 706 ¶ 643

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-011-1: Information Protection

David Revill, Georgia Transmission Corporation

RELIABILITY | ACCOUNTABILITY




CIP-011-1 Summary of Modifications

- The SDT proposes the development of a new Standard CIP-011-1 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-011-1 Summary of Modifications

- Information Protection – R1
  - Requirement for classification removed as there was no requirement to on how to protect different classifications
  - Types of information requiring protection moved to a glossary definition – “BES Cyber System Information”
  - Replaced requirement to “protect” information with a requirement to implement “access control and handling procedures”

CIP-011-1 Summary of Modifications

- Media Reuse and Disposal – R2
  - Very similar to previous requirements
  - Requirements focused on outcome and specific methods removed (which in some cases may not have achieved the desired outcome)
  - Attempted to allow for scenario where equipment must be shipped back to vendor for support
    - BES Cyber System has not yet been disposed of or released for reuse

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

- Please submit your questions via the ReadyTalk chat window
- Point of Contact: Steven Noess, NERC
  - steven.noess@nerc.net
- Slides and recording of Webinar will be posted to the NERC website
- Key Dates:
  - CIP Version 5 Balloting Update Webinar: December 13, 2011
  - Ballot Period Begins: December 16, 2011
  - Balloting and Comment Period Ends: January 6, 2012