NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft CIP Standards Version 5

Technical Webinar – Part 1

Project 2008-06 Cyber Security Order 706 Standards Drafting Team
November 15, 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-002-5 – John Lim, Consolidated Edison
- Implementation Plan – Philip Huff, AECC
- Q&A – Steven Noess, NERC

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Version 5 Schedule Update

Philip Huff, Arkansas Electric Cooperative Corporation

RELIABILITY | ACCOUNTABILITY




Posted Materials

Project 2008-06
Cyber Security Order 706 Version 5 CIP Standards

Activity: Version 5 CIP Standards (Phase III)

Status: Ten CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1 – collectively referred to as the 'Version 5 CIP Standards'), the associated implementation plan, and the associated definitions are posted for a parallel formal comment period and twelve separate initial ballots (ten for the standards, one each for the definitions and implementation pla). In consideration of the volume of documents and the significant changes to the format and substance of the standards, the Standards Committee authorized extending the comment period to 60 days and the initial ballot window to 20 days, through January 6, 2012.

Draft	Action	Dates	Results	Consideration of Comments
Draft 1 - Version 5 CIP Standards CIP-002-5 CIP-003-5 CIP-004-5 CIP-005-5 CIP-006-5 CIP-007-5 CIP-008-5 CIP-009-5 CIP-010-1 CIP-011-1 Implementation Plan Definitions		6/11 - 01/06/12		
Supporting Materials Unofficial Comment Form (Word) Mapping Document	Period Info>> Submit Comments>>	11/07/11 - 01/06/12		
CIP-002-4 CIP-003-4 CIP-004-4 CIP-005-4a CIP-006-4c CIP-007-4 CIP-008-4 CIP-009-4 Consideration of Comments from June 2010 Informal Comment Period	Join Ballot Pool Info>> Join>>	11/07/11 - 12/15/11		
CIP Standards Version 5 Webinar Slides		08/24/2011		

Version 5 Standards, Definitions and Implementation Plan

Posted Materials

Project 2008-06
Cyber Security Order 706 Version 5 CIP Standards

Activity: Version 5 CIP Standards (Phase III)

Status: Ten CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1 – collectively referred to as the 'Version 5 CIP Standards'), the associated implementation plan, and the associated definitions are posted for a parallel formal comment period and twelve separate initial ballots (ten for the standards, one each for the definitions and implementation pla). In consideration of the volume of documents and the significant changes to the format and substance of the standards, the Standards Committee authorized extending the comment period to 60 days and the initial ballot window to 20 days, through January 6, 2012.

Draft	Action	Dates	Results	Consideration of Comments
Draft 1 - Version 5 CIP Standards CIP-002-5 CIP-003-5 CIP-004-5 CIP-005-5 CIP-006-5 CIP-007-5 CIP-008-5 CIP-009-5 CIP-010-1 CIP-011-1 Implementation Plan Definitions **Supporting Materials** Unofficial Comment Form (Word) Mapping Document	Initial Ballot Vote>>	12/16/11 - 01/06/12		
	Formal Comment Period Info>>	11/07/11 - 01/06/12		
CIP-002-4 CIP-003-4 CIP-004-4 CIP-005-4a CIP-006-4c CIP-007-4 CIP-008-4 CIP-009-4 Consideration of Comments from June 2010 Informal Comment Period	Join Ballot Pool Info>> Join>>	11/07/11 - 12/15/11		
CIP Standards Version 5 Webinar Slides		08/24/2011		

Unofficial Comment Form and Mapping Document

Posted Materials

Project 2008-06
Cyber Security Order 706 Version 5 CIP Standards

Activity: Version 5 CIP Standards (Phase III)

Status: Ten CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1 – collectively referred to as the 'Version 5 CIP Standards'), the associated implementation plan, and the associated definitions are posted for a parallel formal comment period and twelve separate initial ballots (ten for the standards, one each for the definitions and implementation pla). In consideration of the volume of documents and the significant changes to the format and substance of the standards, the Standards Committee authorized extending the comment period to 60 days and the initial ballot window to 20 days, through January 6, 2012.

Draft	Action	Dates	Results	Consideration of Comments
Draft 1 - Version 5 CIP Standards CIP-002-5 CIP-003-5 CIP-004-5 CIP-005-5 CIP-006-5 CIP-007-5 CIP-008-5 CIP-009-5 CIP-010-1 CIP-011-1 Implementation Plan Definitions **Supporting Materials** Unofficial Comment Form (Word) Mapping Document	Initial Ballot Vote>>	12/16/11 - 01/06/12		
	Formal Comment Period Info>> Submit Comments>>	11/07/11 - 01/06/12		
CIP-002-4 CIP-003-4 CIP-004-4 CIP-005-4a CIP-006-4c CIP-007-4 CIP-008-4 CIP-009-4 Consideration of Comments from June 2010 Informal Comment Period	oin Ballot Pool Info>> Join>>	11/07/11 - 12/15/11		
CIP Standards Version 5 Webinar Slides		08/24/2011		

Version 4 BOT Approved Standards

Posted Materials

Project 2008-06
Cyber Security Order 706 Version 5 CIP Standards

Activity: Version 5 CIP Standards (Phase III)

Status: Ten CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1 – collectively referred to as the 'Version 5 CIP Standards'), the associated implementation plan, and the associated definitions are posted for a parallel formal comment period and twelve separate initial ballots (ten for the standards, one each for the definitions and implementation pla). In consideration of the volume of documents and the significant changes to the format and substance of the standards, the Standards Committee authorized extending the comment period to 60 days and the initial ballot window to 20 days, through January 6, 2012.

Draft	Action	Dates	Results	Consideration of Comments
Draft 1 - Version 5 CIP Standards CIP-002-5 CIP-003-5 CIP-004-5 CIP-005-5 CIP-006-5 CIP-007-5 CIP-008-5 CIP-009-5 CIP-010-1 CIP-011-1 Implementation Plan Definitions **Supporting Materials** Unofficial Comment Form (Word) Mapping Document	Initial Ballot Vote>>	12/16/11 - 01/06/12		
	Formal Comment Period Info>> Submit Comments>>	11/07/11 - 01/06/12		
CIP-002-4 CIP-003-4 CIP-004-4 CIP-005-4a CIP-006-4c CIP-007-4 CIP-008-4 CIP-009-4 Consideration of Comments from June 2010 Informal Comment Period		5/11		
CIP Standards Version 5 Webinar Slides		08/24/2011		

Consideration of Comments from Informal Posting

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	• Recirculation ballot

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Version 5 Standards Format

Sharon Edwards, Duke Energy

RELIABILITY | ACCOUNTABILITY




Format – Example/Overview

Rationale for R3: *Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable components of a Bulk Electric System (BES) Cyber system. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System. …*

Summary of Changes: *In prior versions, this requirement has arguably been the single greatest generator of TFE's as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. …The drafting team …made… this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component.* ***…****Beginning in paragraph 619-622 of FERC Order 706, …FERC agrees that the standard "does not need to prescribe a single method…"*

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention. [Violation Risk Factor: Medium]

M3. Evidence must include each of the documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevent. and add'l evidence to demonstrate implementation as described in ..Measures in the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicability**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Deploy method(s) to deter, detect, or prevent malicious code.	Evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (i.e. through traditional antivirus, system hardening, policies, etc.).
Reference to prior version: *CIP-007-4 R4*		**Change Rationale:** *See the Summary of Changes.*	

Format – Rationale/ Summary of Changes

Rationale for R3: *Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable components of a BES Cyber system. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System. …*

Summary of Changes: *In prior versions, this requirement has arguably been the single greatest generator of TFE's as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. …The drafting team …made… this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component.* ***…****Beginning in paragraph 619-622 of FERC Order 706, …FERC agrees that the standard "does not need to prescribe a single method…"*

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

Format – High Level/ Requirement and Measure

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention. [Violation Risk Factor: Medium]

M3. Evidence must include each of the documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevent. and add'l evidence to demonstrate implementation as described in ..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-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicability**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Deploy method(s) to deter, detect, or prevent malicious code.	Evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (i.e. through traditional antivirus, system hardening, policies, etc.).
Reference to prior version: *CIP-007-4 R4*		**Change Rationale:** *See the Summary of Changes.*	

- **Requirement row specifies:**
  - 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
  - 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

Format – Applicability

- **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

Additional Format

- The following slide illustrates additional format:
  - Identification of Assets
  - Application of Cyber Security Controls commensurate with risk to the BES

High Level Structure Assets/Controls

High Impact	**Large Control Centers**
Medium Impact	**Generation + Transmission Small Control Centers That meet Criteria** • **Generation- >1500 MW** • **Gen - BlackstartResource** • **Substation - >500 KV** • **Sub - Blackstart Path** • **See additional criteria in posting**
Low Impact	**Everything else**

Additional layer of Controls apply Only to High Impact BES Cyber Systems

CIP 004	CIP 006	CIP 007	CIP 010	CIP 010
Revoke individual user acct access within 30 days	2 or more physical controls	Review a summary or sampling of logged events every 2 weeks	For each change to baseline, test and document CS controls	Perform Active Vulner. Assessment every 3 years (test environment)
Chg. passwords for shared accts within 30 days			Monitor for changes to the baseline	Prior to adding a device perform Vulnerability Assessment

Controls for Medium and High BES Cyber System Controls roughly equate to previous versions of CIP with some modifications:

- FERC Order 706 Directives have been incorporated into requirements
- Access Control requirements previously in CIP 003, 004, 005, and 007 are combined
- Efforts have been made to eliminate the need for TFE's
- New Standards for Info. Protection and Configuration Mgt/Vul. Assessments
- Efforts to remove documentation only based requirements. Performance based std.
- Other modifications for problem areas, i.e., passwords, transient assets, etc.

Requirements that apply to LOW Impact BES Cyber Systems include Governance and non-technical controls

CIP 003	CIP 004	CIP 005	CIP 006	CIP 007	CIP 008
ID Sr. Manger + Maintain CS Policy	Awareness	If routable protocol is used, define technical and procedural controls to restrict access	Define technical and procedural controls to restrict physical access	Initially change default passwords	Incident Response Plan + Testing and Review of Plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Version 5 Definitions

William Winters, Arizona Public Service

RELIABILITY | ACCOUNTABILITY




NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Definitions

- 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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Definitions
21 New or 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 Retired and Replaced

- Critical assets
  - Replaced by CIP002 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

Definitions
New Scoping Concepts

- 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.
  - This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services.
  - The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES.
  - Redundancy shall not be considered when determining availability.
  - A Transient Cyber Asset is not considered a BES Cyber Asset.
- 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.

Definitions Nested for Impact

- **BES Reliability Operating Services**

  BES Reliability Operating Services are those services contributing to the real-time reliable operation of the BES. They include the following Operating Services:

  - Dynamic Response to BES conditions
  - Balancing Load and Generation
  - Controlling Frequency (Real Power)
  - Controlling Voltage (Reactive Power
  - Managing Constraints
  - Monitoring & Control
  - Restoration of BES
  - Situational Awareness
  - Inter-Entity Real-Time Coordination and Communication

- **Integral to CIP002 scoping of BES Cyber System and BES Cyber Asset impact levels**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-002-5: BES Cyber Asset and BES Cyber System Categorization

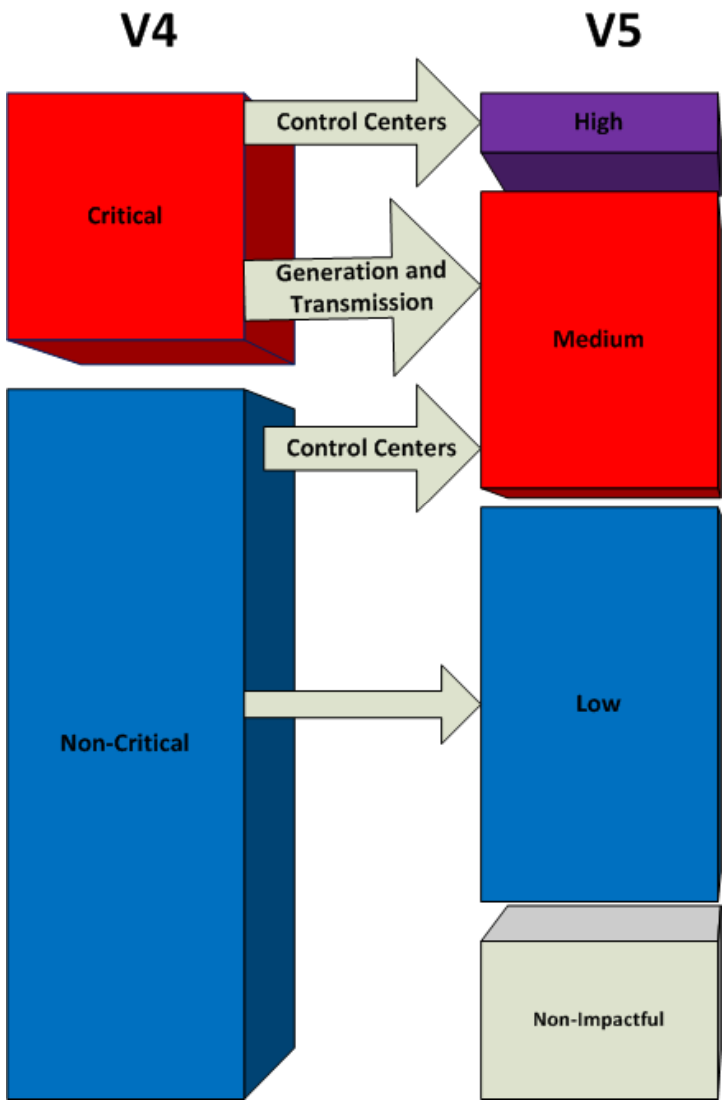
John Lim, Consolidated Edison

RELIABILITY | ACCOUNTABILITY




Levels of Impact

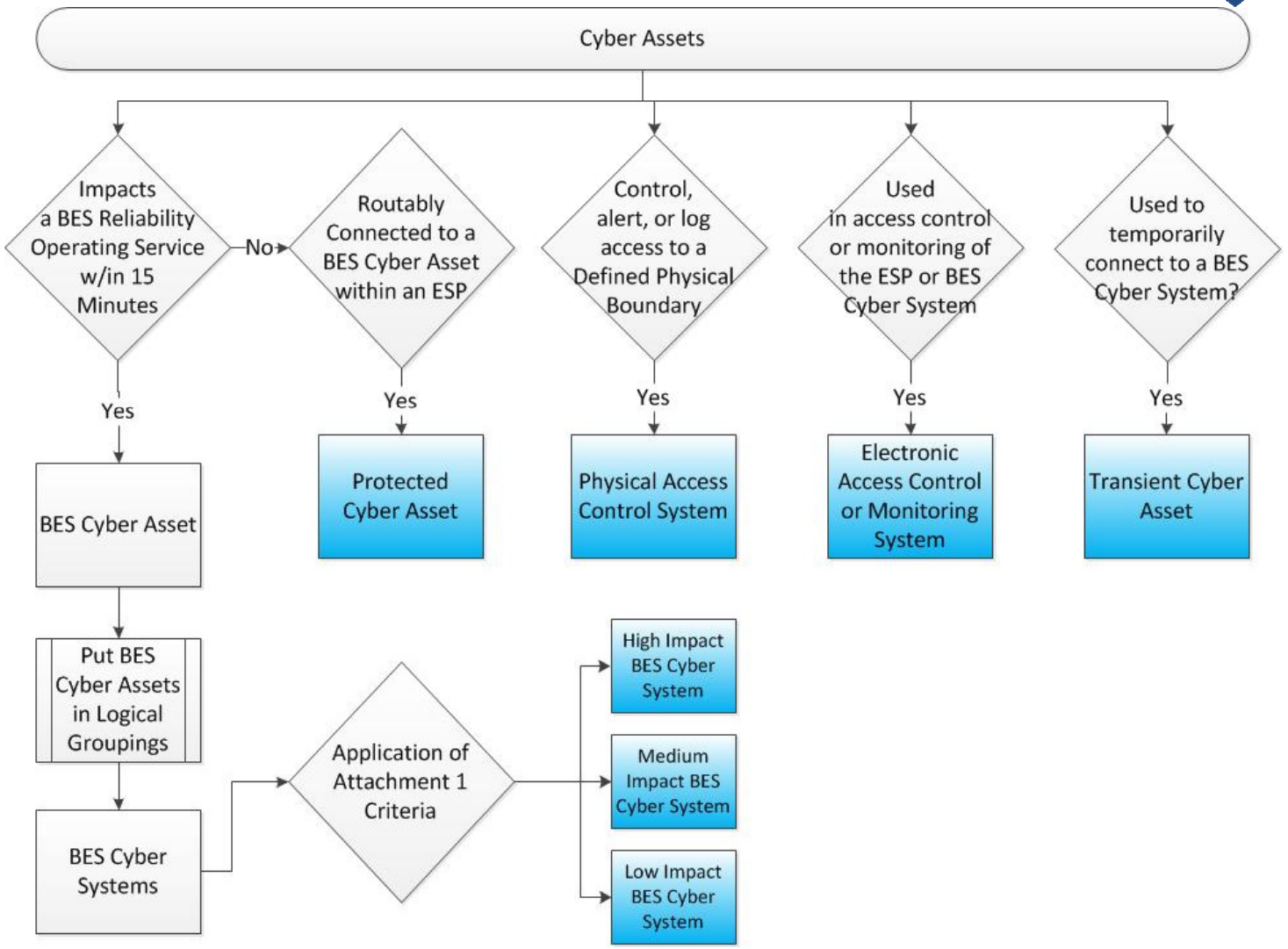
- High Impact
  - Large Control Centers
  - CIP-003 through 009+
- Medium Impact
  - Generation and Transmission
  - Other Control Centers
  - Similar to CIP-003 to 009 v4
- All other BES Cyber Systems
  - Security Policy
  - Security Awareness
  - Incident Response
  - Boundary Protection



Summary of Modifications CIP-002-5

- 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

Categories of Cyber Assets Under CIP v5



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
  - Modification to transmission voltage threshold

CIP-002-5 R1

- Identify and categorize its high and medium impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems*
- All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be low impact and do not require discrete identification
- *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

CIP-002-5 R1 – Part 1.1

- Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities:
  - Intended to be in service for more than 6 calendar months and
  - Causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.

CIP-002-5 R2

- CIP Senior Manager or delegate approve the identification and categorization required by R1:
  - Initially upon the effective date of the standard and
  - At least once each calendar year thereafter, not to exceed 15 calendar months between approvals
- *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

CIP-002-5 Attachment 1 (1 of 9) High Impact

- Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at:
  - 1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.
  - 1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority.
  - 1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator or Transmission Owner that includes control of one or more of the assets identified in criteria 2.2, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11 or 2.12 below.
  - 1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generation Operator that includes control of one or more of the assets identified in criteria 2.1, 2.3, 2.4, or 2.12, below.

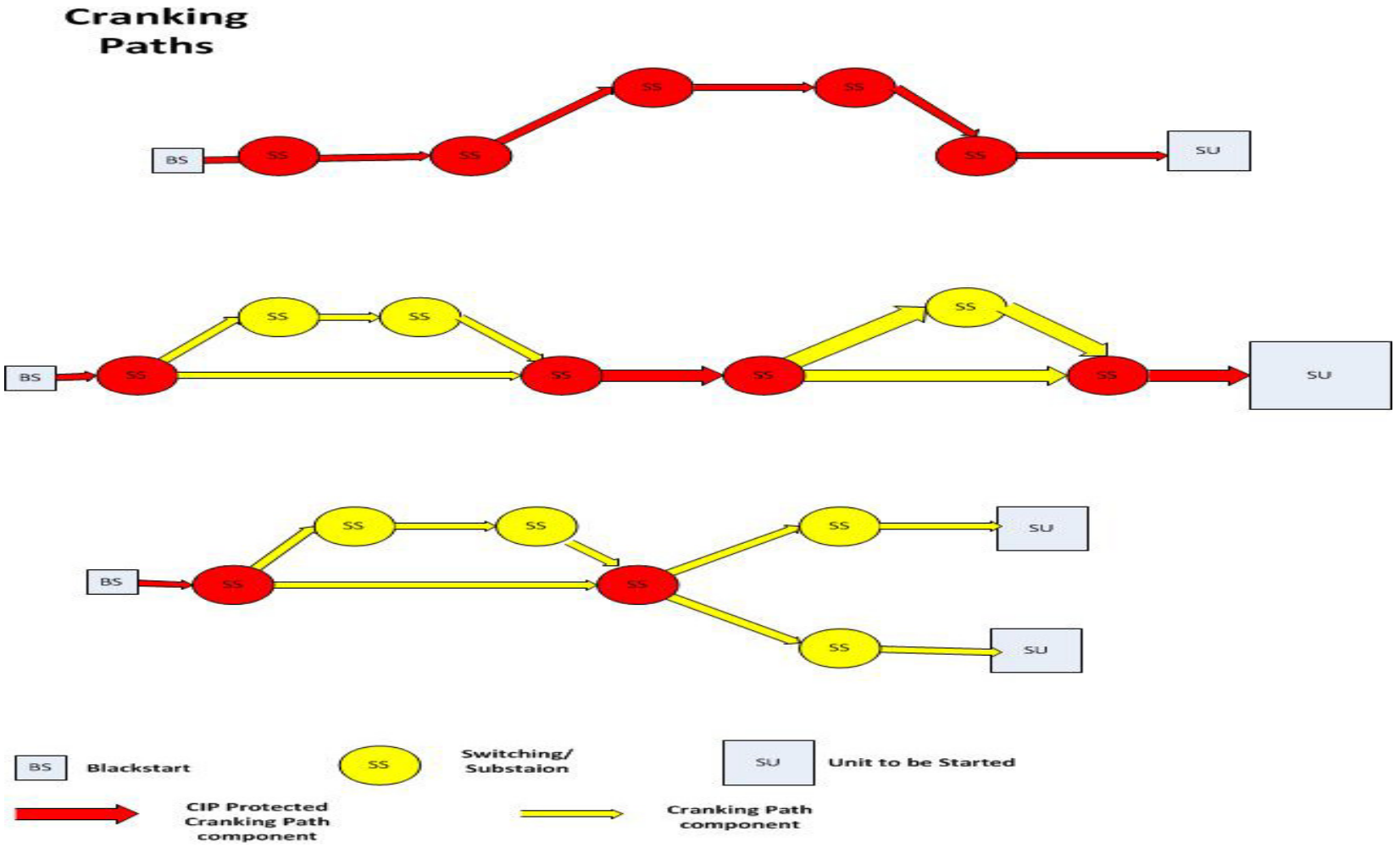
CIP-002-5 Attachment 1 (2 of 9) Medium Impact

- Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for:
  - 2.1. Generation with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single interconnection.
  - 2.2. An aggregate net Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities).
  - 2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

CIP-002-5 Attachment 1 (3 of 9) Medium Impact

- 2.4. Each Blackstart Resource identified in its Transmission Operator's restoration plan.
- 2.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource:
  - Up to and including the first interconnection point of the generation unit(s) to be started, or
  - up to the point on the Cranking Path where two or more path options exist and including any single failure points in the Cranking Path to and including the first interconnection point of the generation unit(s) to be started, or
  - up to and including the point on the Cranking Path where two or more path options exist to two or more independent generation unit(s) to be started as identified in its Transmission Operator's restoration plan.

CIP-002-5 Attachment 1 (4 of 9)
Medium Impact



CIP-002-5 Attachment 1 (5 of 9) Medium Impact

- 2.6. Transmission Facilities operated at 500 kV or higher.
- 2.7. Transmission Facilities operating at 200 kV or higher, but at less than 500 kV,… connected to three or more transmission stations or substations…and where the "total weighted aggregate value" … exceeds a value of 3,000.

Voltage Value of a Line	Weight Value per Line
200 kV to 299 kV	700
300 kV to 499 kV	1300

CIP-002-5 Attachment 1 (6 of 9) Medium Impact

- 2.8. Transmission Facilities … critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.
  - In the WECC Region, Transmission Facilities … critical to the derivation of SOLs and their contingencies for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System".
- 2.9. Flexible AC Transmission Systems (FACTS), … critical to the derivation of Interconnection Reliability Operating Limits (IROLs), and their associated contingencies.
  - In the WECC Region, Flexible AC Transmission Systems (FACTS), … critical to the derivation of SOLs and their contingencies for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System."

CIP-002-5 Attachment 1 (7 of 9) Medium Impact

- 2.10. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.
- 2.11. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system… that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations.
  - In the WECC Region, each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system …that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more System Operating Limits (SOLs) violations … in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System" and each RAS listed in the most current table titled " Major WECC Remedial Action Schemes (RAS)."

CIP-002-5 Attachment 1 (8 of 9) Medium Impact

- 2.12. Each system or Facility that performs automatic load shedding,… of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by its regional load shedding program.
- 2.13. Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners; or (2) generation control centers that control 300 MW or more of generation.

CIP-002-5 Attachment 1 (9 of 9) Low Impact

Low impact:

- All other BES Cyber Assets and BES Cyber Systems not categorized in Section 1 as having a High Impact Rating (H) or Section 2 Medium Impact Rating (M).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Version 5 Implementation Plan

Philip Huff, Arkansas Electric Cooperative Corporation

RELIABILITY | ACCOUNTABILITY




Effective Date

The later of:

- January 1, 2015
- 18 Months Minimum – seven calendar quarters after regulatory approval

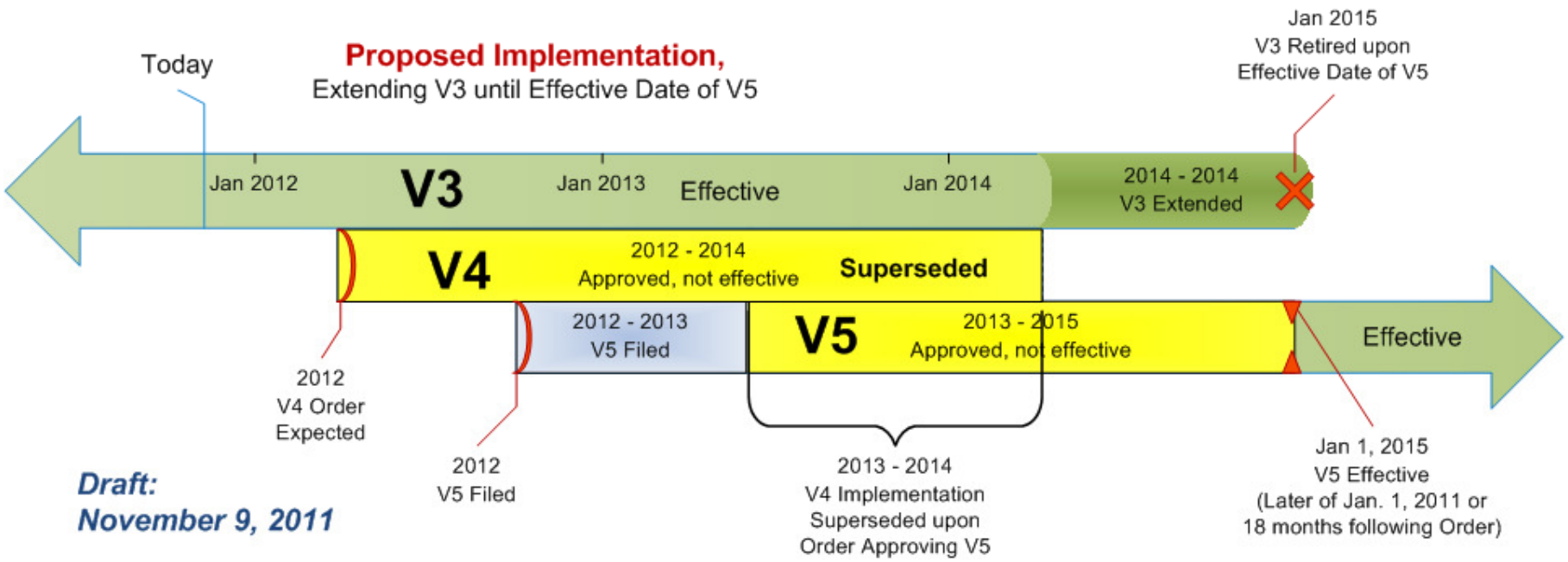
Effective Date – Version Transition

Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.

Effective Date – Version Transition

Implementation Plan for Version 5 of CIP Cyber Security Standards

(Graphic for illustrative and comparative purposes only; dates are estimates only and based on assumptions. There is no way to know or anticipate when FERC may take action on pending matters)



Effective Date – Canadian Entities

In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Implementation Plan Other Changes

- **Single Implementation Plan**
  - Incorporated Unplanned Changes from “Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities”
- **Single Effective Date**
  - No staggered implementation. No Compliant/Auditably Compliant dates

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:
  - Technical Webinar, Part II: November 29, 2011, 1:00 – 3:00 p.m. ET
  - CIP Version 5 Balloting and Process: December 13, 2011 (tentative)