NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Standards Update: Version 5

January 17, 2013

Scott Mix, CISSP
CIP *Technical Manager*

RELIABILITY | ACCOUNTABILITY




NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda

- Version 5
  - Impact Levels
  - Format
  - Features

CIP Standards – Version 5

- CIP Version 5 - Draft 4 – Final Version
  - Approved by industry on Nov 5, 2012
  - Approved by NERC Board of Trustees on Nov 26. 2012
  - Filing to FERC and other regulators in progress

CIP Standards – Version 5

- CIP-002-5: BES Cyber Asset and BES Cyber System Categorization
- CIP-003-5: Security Management Controls
- CIP-004-5: Personnel and Training
- CIP-005-5: Electronic Security Perimeter(s)
- CIP-006-5: Physical Security of BES Cyber Systems
- CIP-007-5: Systems Security Management
- CIP-008-5: Incident Reporting and Response Planning
- CIP-009-5: Recovery Plans for BES Cyber Assets and Systems
- CIP-010-1: Configuration Management and Vulnerability Assessments
- CIP-011-1: Information Protection

CIP Standards – Version 5

- New / Modified Terms:
  - BES Cyber Asset
  - BES Cyber System
  - BES Cyber System Information
  - CIP Exceptional Circumstance
  - CIP Senior Manager
  - Control Center
  - Cyber Assets
  - Cyber Security Incident
  - Dial-up Connectivity
  - Electronic Access Control and Monitoring Systems (EACMS)
  - Electronic Access Point (EAP)
  - Electronic Security Perimeter (ESP)
  - External Routable Connectivity
  - Interactive Remote Access
  - Intermediate Device
  - Physical Access Control Systems (PACS)
  - Physical Security Perimeter (PSP)
  - Protected Cyber Asset (PCA)
  - Reportable Cyber Security Incident

CIP Standards – Version 5

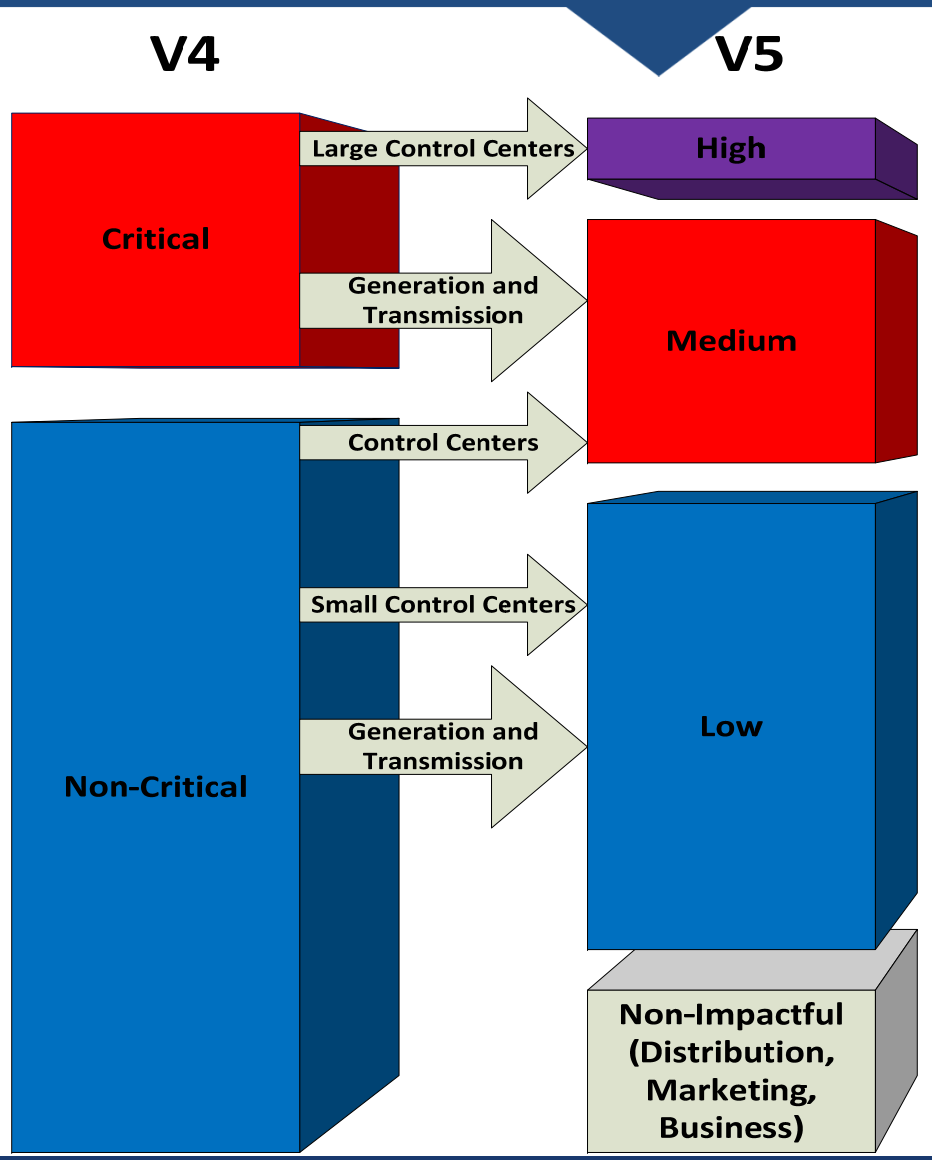
- Retired Terms
  - Critical Assets
  - Critical Cyber Assets

CIP Standards – Version 5

- CIP-002
  - Builds on “bright lines” in CIP-002-4
  - “Version 4” Critical Asset control centers – High
  - Other “Version 4” Critical Assets – Medium
  - Larger “Version 4” non-critical asset control centers – Medium
  - Transmission now looking at “capacity” rather than number of lines at a voltage level
  - Catch-all category for non-specifically categorized – Low
    - “Something everywhere” – within the BES
    - Programmatic requirement: CIP-003-5 Requirement R2

CIP Standards – Version 5

- High Impact
  - Large Control Centers
  - CIP-003 through 009 “plus”
- Medium Impact
  - Generation and Transmission
  - Control Centers
  - Similar to CIP-003 to 009 V4
- All other BES Cyber Systems (Low Impact) must implement a policy to address:
  - Cybersecurity Awareness
  - Physical Security Controls
  - Electronic Access Controls
  - Incident Response
- High Watermarking



CIP Standards – Version 5

Rationale, Guidance & Changes,

Rationale for R3: To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.

Main Requirement and Measure

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

Applicable Systems for requirement part

Requirement part text

Requirement part Measure text

CIP-004-5 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Addressed interpretation request in guidance. Specified that identity confirmation is only required for each individual's initial assessment. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.*	

Requirement part Reference

Requirement part change rationale

CIP Standards – Version 5

- Format
  - Following Results-based Standards format
  - Background section before requirements
  - Requirement and Measurement next to each other
  - Measurement “more useful”
  - Rationale and guidance developed in parallel with requirements – still being developed and augmented
  - Two posting formats – one with guidance/rationale text boxes inline; other with guidance and rational text grouped at end
  - Still must audit only to the requirement
  - Guidelines and Technical Basis section at end

CIP Standards – Version 5

- Applicable Systems column in tables
  - What systems or entities the row in the table apply to
  - Listed in each standard
  - Specific phrases – consistent across all standards
  - A requirement part (row) may have multiple applicability statements
  - Examples:
    - High Impact BES Cyber Systems
    - Medium Impact BES Cyber Systems
    - Medium Impact BES Cyber Systems at Control Centers
    - Medium Impact BES Cyber Systems with External Routable Connectivity
    - Protected Cyber Assets
    - Electronic Access Control Systems

CIP Standards – Version 5

- Connectivity
  - No longer a blanket exemption
  - Now listed in applicability section – Routable Connectivity or Dial-up Connectivity
  - "Routable protocol" applicability now applies where large volume, real-time communications requirements are listed – e.g., logging
- Low Impact
  - CIP-003-5 Requirement R2
  - "Programmatic" controls (i.e., have a program for …)
  - Requires physical and cyber security protections for "locations" containing low
  - Does not require lists of every low impact BES Cyber System

CIP Standards – Version 5

- TFEs
  - Attempting to minimize required TFEs (e.g., anti-malware on switches)
  - Reduced from 14 requirements to 10
  - But … still have TFEs (including new ones where existing V1 – V4 problems exist)
  - Have added “per Cyber Asset capability” language to allow strict compliance with the language of the requirement, without requiring a TFE (~5 requirements)
- Measures
  - Guidance to auditors as well as entities
  - “An example of evidence may include, but is not limited to, …”
  - No longer a “meaningless restatement of the requirement”

CIP Standards – Version 5

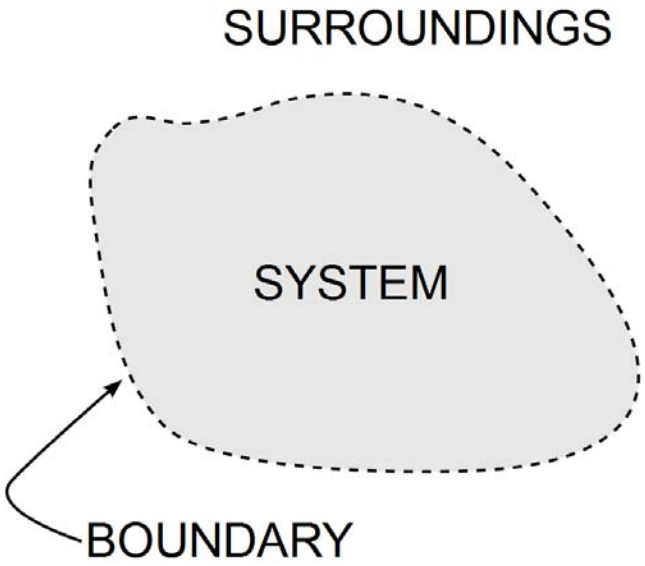
- Bulleted lists vs. numbered lists
  - Bulleted lists are separated by “or”
  - Bulleted lists imply that *not all* of the items in the list are required
  - Numbered lists are separated by “and”
  - Numbered lists imply that *all* of the items in the lists are required
- Both bulleted and numbered lists are used in both requirements and measures

Features of Version 5

- Closes out directives in FERC Order No. 706 (also, FERC Order No. 761 imposes March 31, 2013, filing deadline)
- Results-based standards
  - Focus on reliability and security-related result
  - Non-technology specific
  - Smarter use of Technical Feasibility Exception (TFE) process
  - “Plain language of the requirement”, i.e., “per device capability”
- Risk-informed systems approach
  - Adopt solutions and tailor security based on function and risk
  - No longer a harsh “in or out” demarcation for applicability
  - Impact and connectivity informs applicability

Features of Version 5

- Systems approach illustration
  - Cyber Assets function together as a complex system
  - Identify the system and apply requirements to the whole rather than the part



  - "High Watermarking" inside boundary

CIP V5 Approach to Correcting Deficiencies

- Empowers industry
  - Shifts focus from *whether* deficiencies occur to *correcting* deficiencies
  - Continuous Improvement
    - ***From:*** backward-looking, individual violations
    - ***To:*** forward-looking, holistic focus
- Reliability and security emphasis that promotes the identification and correction of deficiencies
- Consistent with NERC "Internal Controls" approach to compliance
- Version 5 triggering language: "… implement, in a manner that identifies, assesses, and corrects deficiencies, …"

CIP V5 Approach to Correcting Deficiencies (Continued)

- Corrected deficiency is a component of satisfying the requirement
- **Does not *require* "internal controls" or additional process**
- *Standards* approach of correcting deficiencies complements the *compliance* concept of internal controls
- Reliability Standard Authorization Worksheets (RSAWs) and Violation Severity Levels (VSLs) must support approach
  - Does not expand obligations
  - Clarifies that *method* of identifying, assessing, and correcting deficiencies is not evaluated

Draft RSAW

- **Deficiencies** refer to possible non-compliances with the standard; **not all deficiencies would become issues of non-compliance**
- Entities are not required to self-report deficiencies if they are identifying, assessing and correcting them
- CEA samples identified, assessed and corrected deficiencies
  - CEA considers impact of correction in determining the sample size

When to Self-Report

- Plan **does not exist**
- Plan **has not been implemented**
- Did **not assess or correct** identified deficiencies
- Deficiencies that create **high risk** to the Bulk Electric System

Implementation Plan

- Proposed Effective Date (from CIP-002-5; all standards use the same language):
  1. 24 Months Minimum – CIP-002-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
  2. In those jurisdictions where no regulatory approval is required CIP-002-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Implementation Plan

- Implementation issues:
  - Specified initial performance of all periodic requirements in implementation plan
  - 24 months following regulatory approval for all requirements
  - Identity Verification does not need to be repeated
  - Discussion of unplanned re-categorization to a higher impact level
  - Discussion of disaster recovery actions
  - Discussion of requirements applied to access control systems (physical and electronic), and Protected Cyber Assets

Applicability

- Applicability Section:
  - Section 4.1 Functional Entities
    - Describes which asset owners, based on their functional model designation, and specific ownership of assets, must comply with the standards
    - May have no qualifications – applies to all entities registered for that function
  - Section 4.2 Facilities
    - Describes which assets must comply with the standards
    - May have no qualifications – applies to all BES assets owned by that function

Applicability

- Applicability Example:
  - For Distribution Providers – only those registered DPs that own specifically called out pieces of equipment, such as UFLS systems, must comply with the standards
  - For those DPs, only the specifically called out pieces of equipment must comply with the standards
- If a DP does not own any called out equipment, it does not need to comply with the standards
- If a DP owns a piece of called out equipment, only that called out equipment must comply with the standards

Applicability

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

Applicability

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers:**

All BES Facilities.

Applicability

4.2.3. Exemptions: The following are exempt from Standard CIP-004-5:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

CIP Standards – Version 5

- CIP-002-5 through CIP-009-5, CIP-010-1, CIP-011-1
- "Results-based Standard" format
  - Requirements and measures together
  - Guidance and rational in text boxes
- "Looks" bigger
  - ~1" printout for Version 5 (includes VSLs) compared to ~¼" printout for Version 4
  - Includes much more guidance and rationale for each requirement

Version 5 Requirement Counts

- CIP-002
  - 2 Requirements; 5 Parts; Attachment with bright lines for High and Medium
- CIP-003
  - 4 Requirements; 13 Parts
- CIP-004
  - 5 Requirements; 18 Parts
- CIP-005
  - 2 Requirements; 8 Parts
- CIP-006
  - 3 Requirements; 13 Parts
- CIP-007
  - 5 Requirements; 20 Parts
- CIP-008
  - 3 Requirements; 9 Parts
- CIP-009
  - 3 Requirements; 10 Parts
- CIP-010
  - 3 Requirements; 10 Parts
- CIP-011
  - 2 Requirements; 4 Parts
- Total: 32 Requirements; 110 Parts

Version 4 Requirement Counts

- CIP-002
  - 3 Requirements; 0 parts, Attachment with Bright Lines
- CIP-003
  - 6 Requirements; 18 parts/sub-parts
- CIP-004
  - 4 Requirements; 12 parts/sub-parts
- CIP-005
  - 5 Requirements; 26 parts/sub-parts
- CIP-006
  - 8 Requirements; 15 parts/sub-parts
- CIP-007
  - 9 Requirements; 34 parts/sub-parts
- CIP-008
  - 2 Requirements; 6 parts
- CIP-009
  - 5 Requirements; 2 parts
- Total:
  - 42 Requirements; 113 parts/sub-parts

CIP Standards – Version 5

- Sub-Requirements
  - Each Requirement / Sub-Requirement is a compliance touch-point
  - Non-compliance with a sub-requirement stands on its own
  - Sub-requirements have independent VSLs (unless rolled-up)
- Requirement Parts
  - Only the Requirement is a compliance touch-point
  - Cannot be independently in non-compliance with a Part
  - VSLs written only at the Requirement level (making very long and complicated VSL language)
  - Parts allow flexibility in development and implementation of the requirement

Version 5 Technical Webinars

- Draft 1 Technical Webinar on format and CIP-002
  - SDT lead
  - November 15, 2011
- Draft 1 Technical webinar on CIP-003 through CIP-011
  - SDT lead
  - November 29, 2011
- Draft 2 Technical Webinar
  - SDT Lead
  - April 10, 2012
- (http://www.nerc.com/page.php?cid=1|83)

Version 5 Webinars

- Draft 3 Webinar: Version 5 CIP Standards: A Focus on "Correcting Deficiencies"
  - SDT's approach to "internal controls" concepts – but does not *require* an internal controls program
  - Industry (SDT and others) and NERC Staff Lead
  - September 11, 2012
- Draft 3 Technical Webinar
  - SDT Lead
  - September 21, 2012

- (http://www.nerc.com/page.php?cid=1|83)

Version 5 Features

- "Annual" – interaction with CAN – now "15 months"
- Monthly requirements – changed to 35 days
- Functional Entity / Facilities section
- Applicability issues (between requirements, standards, in requirement vs. applicability column)
- Measures are examples with bulleted lists; format, wording
- Compliance artifacts in requirements (e.g., "documentation of …")
- LSE (removed)
- 300 MW threshold on UFLS/UVLS
  - No justification for a different value

Version 5 Features

- Definition / threshold of Control Center
  - Includes “data centers”
- Connectivity (routable, dial-up)
- Notifications: IROL, “must run” (resolving as part of V4)
- IROL’s in WECC
- Low Impact (policy)
  - List not required
- Date tracking (PRA, training, access, etc)
- “Role-based training”
- Access revocation (reassignments, timing, immediate)
- “IDS” in measure
  - Added additional examples

Version 5 Features

- Removed 99.9% availability phrasing
  - Difficult to track and audit
  - Replaced with “IAC” language
- Interactive Remote Access
  - Clarify encryption and multi-factor authentication points
  - Remove examples from requirements
  - Remove purpose of encryption
- More use of “graded” VSLs, as opposed to many “binary” VSLs in previous versions
- Ports & Services –
  - Physical ports - FERC Directive
- Anti-malware – clarify system level
- “Per device capability” clauses added

Version 5 Features

- No remediation plan if install patches within 35 days
  - Allow updates to existing plans rather than new plans all the time
- Password changing / pseudorandom passwords (RuggedCom vulnerability impacts)
- Evidence Retention (compliance vs. security monitoring)
- Take back reporting requirement from EOP-004 into CIP-008
- Guidance on “active” vs. “passive” vulnerability assessment
- V4 bypass language still in implementation plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

References

- Standard project 2008-06 page:
  - http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html
- Version 4 page:
  - http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html
- Version 4 Guidance Document
  - http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean_20101220.pdf
- Version 5 page:
  - http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_Version_5_CIP_Standards_.html

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions

Scott Mix, CISSP
scott.mix@nerc.net
215-853-8204

RELIABILITY | ACCOUNTABILITY