NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Standards Update

Version 5

RELIABILITY | ACCOUNTABILITY




NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Ongoing Steps

- Filed with FERC February 1, 2013 (after 5:00 PM on 1/31)
  - FERC Docket RM13-5
  - 10,483 page filing (yes, ten thousand pages)
  - Available on NERC Website at:
    - http://www.nerc.com/files/Final_Petition_CIP_V5_01-31-13%20and%20Exhibits%20A-E.pdf
    - http://www.nerc.com/fileUploads/File/Filings/Exhibit%20F%20(Part%201%20of%202).pdf
    - http://www.nerc.com/fileUploads/File/Filings/Exhibit%20F%20(Part%202%20of%202).pdf
    - http://www.nerc.com/fileUploads/File/Filings/Exhibits%20G-H.pdf
  - FERC version at http://elibrary.ferc.gov/idmws/common/OpenNat.asp?fileID=13167892 (76MB file)
- FERC will need to go through its process
- Filings to Canadian Regulators made on February 7, 2013

CIP Standards – Version 5

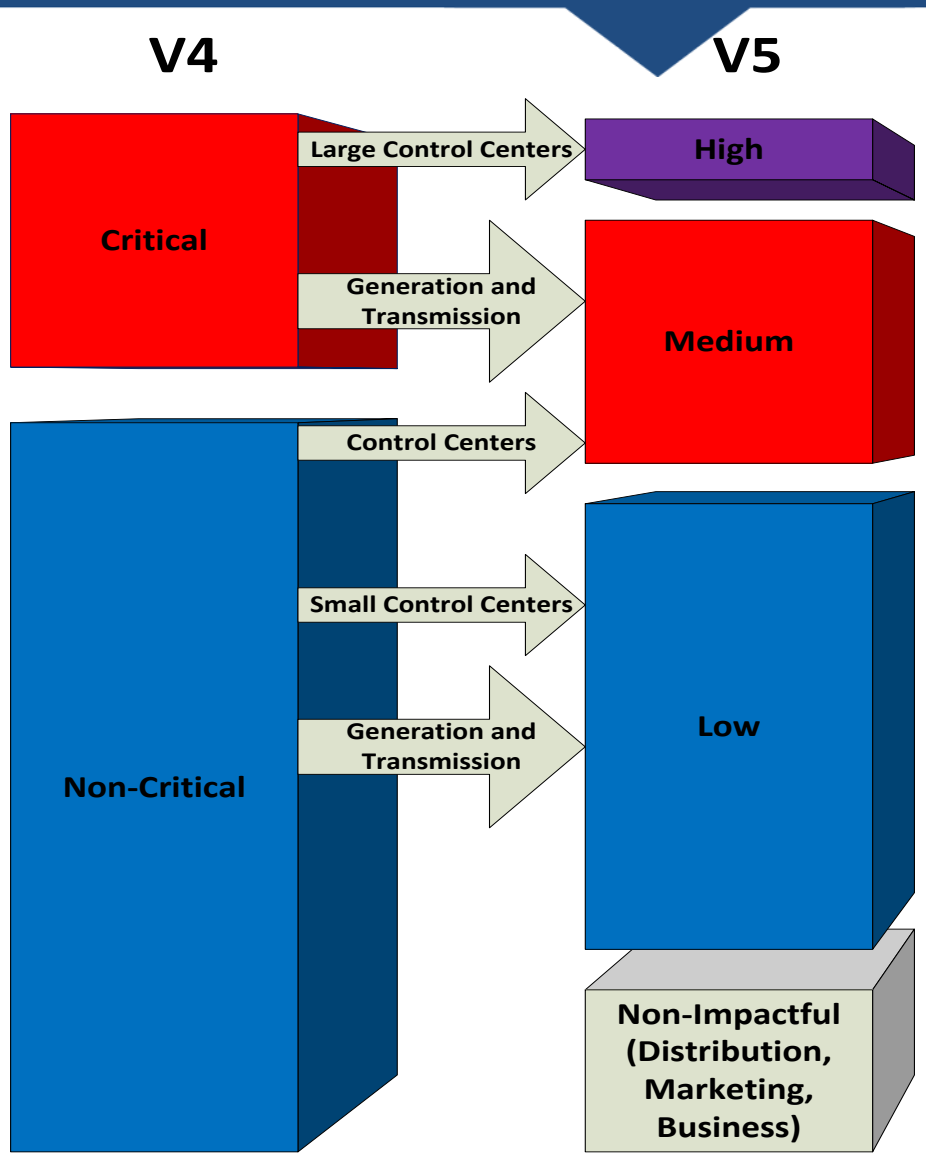
- New / Modified Terms:
  - BES Cyber Asset
  - BES Cyber System
  - BES Cyber System Information
  - CIP Exceptional Circumstance
  - CIP Senior Manager
  - Control Center
  - Cyber Assets
  - Cyber Security Incident
  - Dial-up Connectivity
  - Electronic Access Control and Monitoring Systems (EACMS)
  - 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

- CIP-002
  - Eliminates the “Critical Asset” step of the identification process
  - Builds on “bright lines” from 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 a “capacity calculation” 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

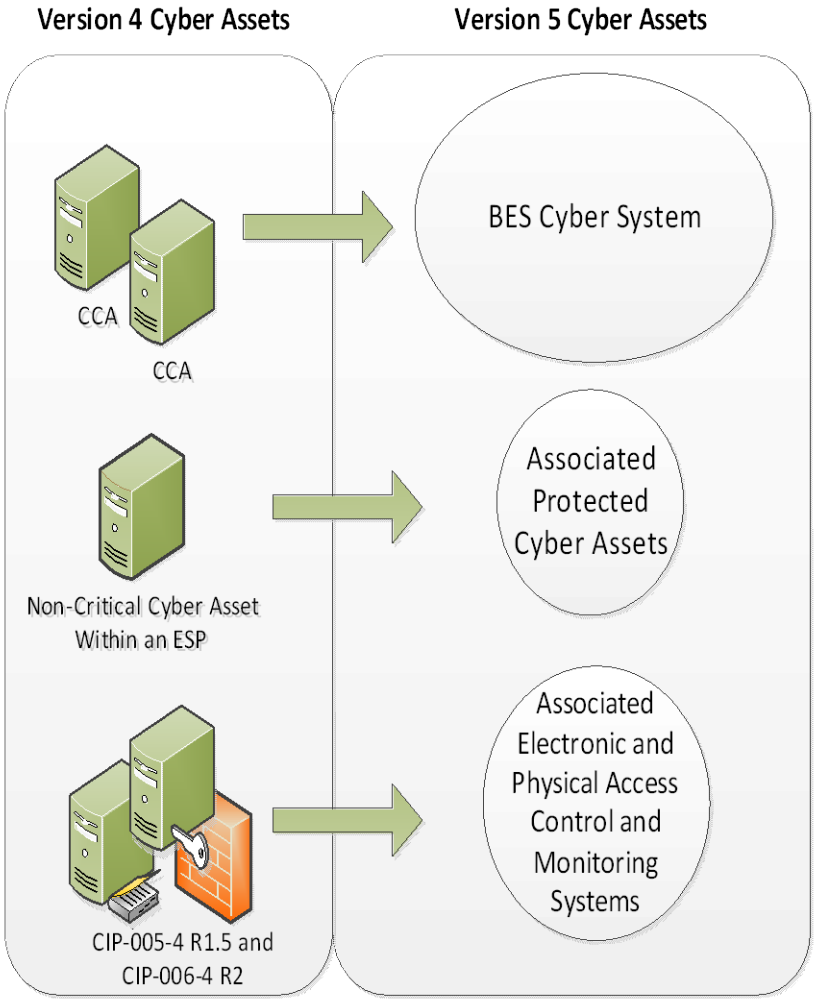
CIP Standards – Version 5

- High Impact
  - Large Control Centers
  - CIP-003 to 009 V4 "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



CIP Standards – Version 5

- Non-CCA assets in Version 4 are also covered
  - "Non-Critical Cyber Assets within an ESP" are now named Protected Cyber Assets, are associated with a BES Cyber System, and called out in the Applicable Systems column
  - EACMS and PACS are associated with a BES Cyber System, and are called out in the Applicable Systems column



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 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, …"

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions

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

RELIABILITY | ACCOUNTABILITY