EPRI | ELECTRIC POWER RESEARCH INSTITUTE

NERC CIP Tools and Techniques

Supplemental Project - Introduction Webcast

Scott Sternfeld, Project Manager

Smart Grid Substation & Cyber Security Research Labs

ssternfeld@epri.com

(843) 619-0050

October 17, 2013

NERC CIP Compliance Challenges

- Difficulties in maintaining documentation and audit evidence
- Lack of communication with industry peers
- Legacy devices cannot meet current and future requirements
- Lack of compliance trained staff
- Change is inevitable

NERC CIP Standards

Version 3 / 4

- **CIP-002:** Critical Cyber Asset Identification
- **CIP-003:** Security Management Controls
- **CIP-004:** Personnel and Training
- **CIP-005:** Electronic Security Perimeter(s)
- **CIP-006:** Physical Security of CCAs
- **CIP-007:** Systems Security Management
- **CIP-008:** Incident Reporting and Response Planning
- **CIP-009:** Recovery Plans for CCAs

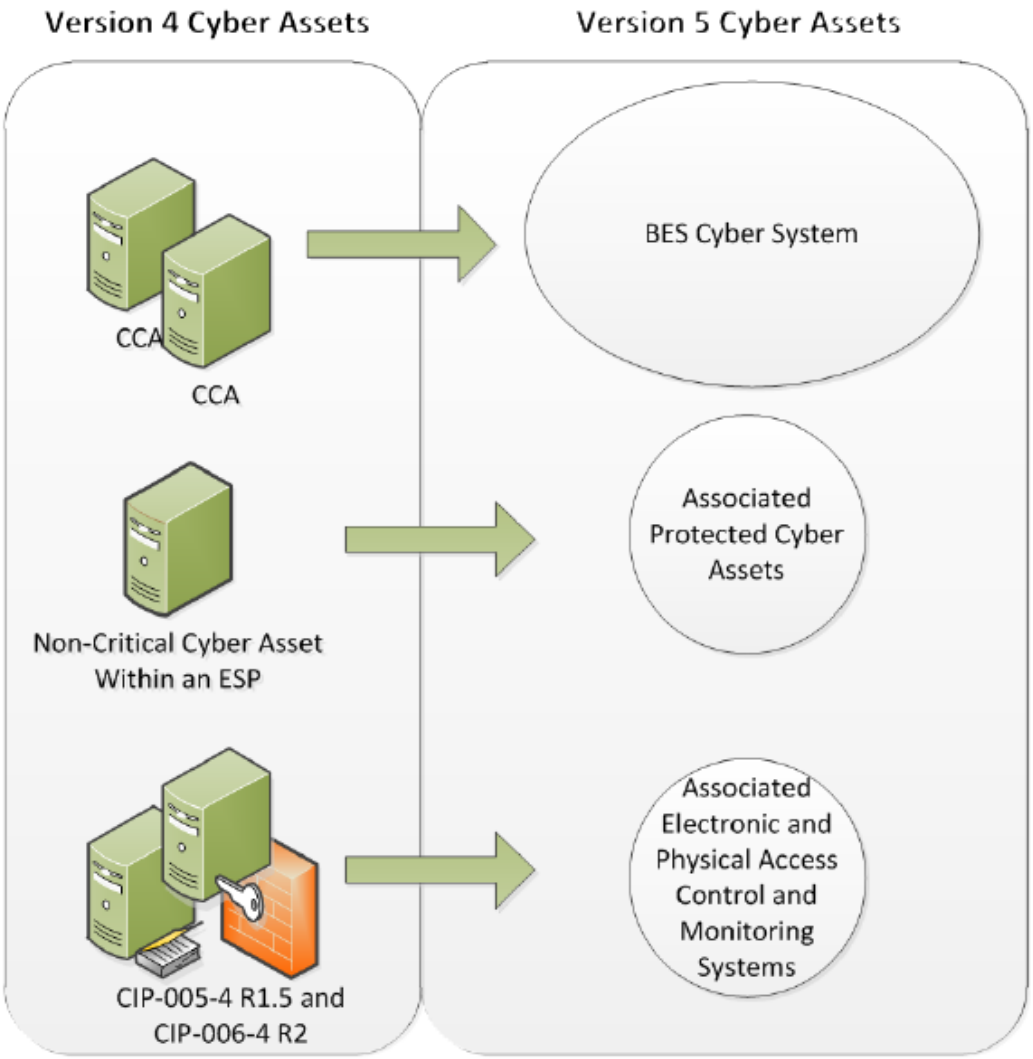
Version 5 Changes/Adds:

- **CIP-002:** BES Cyber Asset and BES Cyber System Categorization
- **CIP-010:** Configuration Change Management and Vulnerability Assessments
- **CIP-011:** Information Protection

Changes in Version 5 Standard Key Definitions

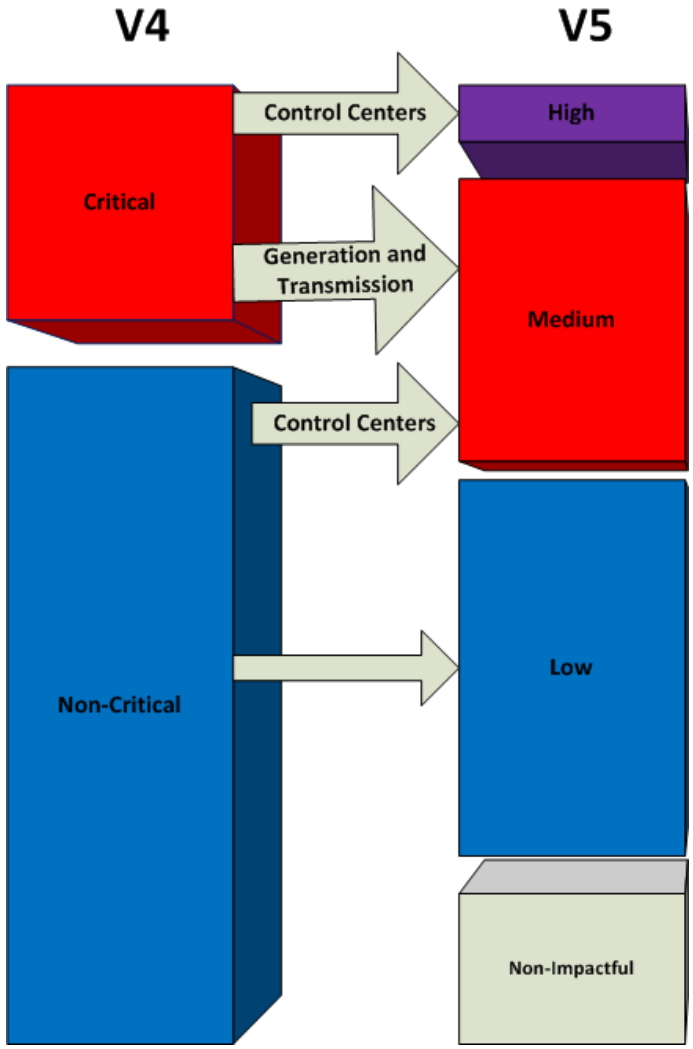
- Critical Assets (CAs)
  - Replaced by CIP-002 Attachment 1 and BES
- Critical Cyber Assets (CCAs)
  - Replaced by BES Cyber Asset and BES Cyber System
- Physical Security Perimeters (PSPs)
  - Replaced by Defined Physical Boundary
  - Removed the “six-wall” specification

New Cyber System Categorization



New Impact Ratings for BES Cyber Systems

- High Impact
  - Large control centers and backup centers
- Medium Impact
  - Generation and transmission facilities
  - Other control centers not covered in CIP-002-4
- Low Impact
  - All other BES Cyber Systems not covered by CIP Version 4



New Challenges With NERC CIP Version 5

- Ten standards instead of the eight in the previous four versions
- Total of fifteen newly defined terms
- Encryption requirement
- Multi-factor authentication requirement
- Configuration management requirement
- All serial connections are to be considered
- Systems must be categorized in three impact levels
- Physical I/O ports requirement
- All policy and procedure documentation must be updated with new terminology and impact levels

NERC CIP Tools and Techniques Supplemental Project

This project will provide techniques for transitioning to NERC CIP Version 5:

- Identification of gaps in current tools
- Provide guidance and techniques for complying with NERC CIP requirements
- Areas of focus may include:
  - Configuration change management
  - Patch management
  - Identity access management
  - Determination of BES Cyber Assets and BES Cyber Systems

Configuration Change Management

NERC CIP-010-1:

- New requirement consisting of the consolidation of previous sub-requirements
- Utilize and verify existing baselines to develop configuration lists of the BES Cyber Systems
- Utilize “safe” enumeration tools to verify existing assets
- Collect configuration data from the assets
- Create effective processes for verifying “changes” to those assets

Patch Management

NERC CIP-007-5 R2:

- Traditionally a difficult requirement to maintain compliance

- New wording provides more granularity
  - Documenting the sources that are monitored for release of patches
  - "… create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source …"

Identity Access Management

NERC CIP-004-5 R6 & R7:

- Pulled the access management requirements from CIP-003-4, 004-4, and 007-4 into a single requirement
- 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
- For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day

Key Definitions of Applicable Core 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

Determination of BES Cyber Assets and BES Cyber Systems

NERC CIP-002-5 R1:

- Shift from identifying Critical Cyber Assets to identifying BES Cyber Systems
- Scope is restricted to BES Cyber Assets and BES Cyber Systems that would impact the reliable operation of the BES
- BES Cyber Assets are those cyber assets that, if rendered unavailable, degraded, or misused, would impact the BES Reliability Operating Services within 15 minutes of the activation or exercise of the compromise
- High, Medium, Low classification (Bright-line Criteria)

NERC CIP Tools and Techniques

Research Goals

- Strategies and tools for transitioning existing cyber security programs from the current Version 3/4 to Version 5
- Guidance for reaching effective regulatory compliance with Version 5 of the NERC CIP Standards

Deliverables

- Workshop – NERC CIP Version 5 workshop at EPRI's Cyber Security Research Lab in Knoxville, TN and resulting Training DVD.
- Webcast Discussion Forums and Updates (Bi-Monthly)
- Technical Report – "NERC CIP Tools and Techniques"

Guidelines and Training for Meeting Compliance with Version 5

NERC CIP Tools and Techniques

Objectives and Scope

- Provide guidance for transitioning to NERC CIP Version 5
- Project may focus on:
  - Configuration change management
  - Patch management
  - Identity access management
  - Determination of BES cyber assets and BES Cyber Systems

Value

- Identify gaps in current tools that have been deployed to address the CIP requirements
- Provide guidance and techniques for complying with CIP requirements

Details and Contact

- Price: $50,000
- Qualifies for TC and SDF

Scott Sternfeld

- ssternfeld@epri.com
- 843-619-0050

SPN Number: 3002001768

Guidance for Efficiently Meeting NERC CIP v5 Requirements

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Discussion

Scott Sternfeld
ssternfeld@epri.com
843-619-0050

Together…Shaping the Future of Electricity