NRRI Colloquium
Washington, DC
8 February 2014

A Review of NERC's CIP Standard Version 5

Daniel Phelan
Research Assistant
National Regulatory Research Institute

CIP Version 5

- Cyber Security Standards for:
  - Balancing Authorities
  - Generator Operators/Owners
  - Interchange Coordinators and Authorities
  - Reliability Coordinators
  - Transmission Operators/Owners
  - Some Distribution Providers
- 10 Standards consisting of 37 Requirements
- FERC approval effective date February 3, 2014

Standard CIP-002-5.1

- Three levels of system classification
- High Impact
  - Control Centers or Backup Control Centers operating Medium Impact Assets
- Medium Impact
  - SPS, RAS, or Switching System that could cause IROL violations, Facilities needed to avoid an Adverse Reliability Impact, Generation with Real Power capability greater than 1500MW, etc.
- Low Impact
  - All otherwise uncategorized

Standard CIP-003-5

- Responsible Entities must have Cyber Security Policies for High and Medium Impact Systems
- All Systems must have policies in place addressing:
  - Cyber Security Awareness
  - Physical Security Controls
  - Electronic Access Controls for External Routable Protocol Connections
  - Incident Response to a Cyber Security Incident
- Each Responsible Entity must have a CIP Senior Manager, and a delegation process for that authority

Standard CIP-004-5.1

- Each quarter, a Security Awareness Program must occur reinforcing Cyber Security Practices
- A Training Program must be completed before authorizing access to Cyber Assets, and again once every 15 months
- Personnel must undergo a background check
- Process to authorize Electronic and Physical Access
  - Process to remove Access as well

Standard CIP-005-5

- High and Medium Impact Systems must be contained within an Electronic Security Perimeter
  - External Routable Connectivity must go through a defined Electronic Access Point
- Remote Access must utilize an Intermediate System, and require Multi-Factor authentication
  - Connection to Remote Access must be encrypted, terminating at Intermediate System

Standard CIP-006-5

- Operational or Procedural controls restricting Physical Access
  - High Impact Systems should use two or more controls, Medium Impact systems should use at least one
- Physical Access logs, Alarm or Alert in response to unauthorized Physical Access

Standard CIP-007-5

- Only ports determined necessary should be open to network access
- System Patches should undergo a defined evaluation process
- Deploy methods to deter, detect, or prevent malicious code
- Log Security Events at the BES Cyber System level or Cyber Asset level
- Have a method to authenticate user access

Standard CIP-008-5

- Identify, Classify, and Respond to Cyber Security Incidents
- Each Response Plan must be tested at least once every 15 months

Standard CIP-009-5

- Each High and Medium Impact System must have a Recovery Plan
- Recovery Plans must be tested at least once every 15 months
  - Each Recovery Plan must be tested once every 36 months through an Operational Exercise

Standard CIP-010-1

- Develop baseline configurations for Cyber Security Systems
  - Deviations from baseline must be authorized and documented
  - High Impact Systems must be monitored for deviations every 35 days
- Conduct a paper or active vulnerability assessment every 15 months
  - An active vulnerability assessment should be conducted on High Impact Systems every 36 months
  - Active vulnerability assessments should also be performed on any new Cyber Asset added to a High Impact BES Cyber System

Standard CIP-011-1

- One or more methods to identify BES Cyber System Information
  - Procedure for protecting and securing Information for use, storage, and transit
- Take action to prevent unauthorized retrieval of BES Cyber System Information before reuse of disposal of data storage media

FERC Changes

- Order 791, Docket No. RM13-5-000 (November 22, 2013)
- Approved CIP Version 5, but also prescribed revisions
  - Modifications to "identify, assess, and correct" language
  - Increase requirements for Low Impact Systems
  - Develop requirements for Transient Electronic Devices
  - Conduct a survey of Assets to determine if 15-minute parameter excludes some necessary Assets
  - Define Communication Networks, and develop standards for their protection
- 24 months for High and Medium Impact Systems to comply, 36 months for Low Impact Systems