CIP – NERC Critical Infrastructure Protection

NERC CIP V5 and How It Affects You

March 16, 2015

John Lim
Lim Consulting LLC
limconsultingllc@gmail.com
Biographic Summary

- More than 30 years in Electric Power industry
- 29 years in a large IOU Distribution and Transmission company in the North East
- Experience in IT and OT infrastructure
- NERC Drafting Team for CIP V1-V5
- Chair of the CIP Drafting Team for V4 and V5
- Former member: regional and NERC CIP committees
- Former Co-Vice Chair of Smart Grid CSWG/IP
- Drafting team of DoE Cyber Security Risk Management Process Guideline
Disclaimer

The information presented here is the presenter’s interpretation of official sources of that information. Opinions presented are the presenter’s own and do not represent WSU’s or any other organization’s positions.
NERC CIP Standards Version 5

- Approved by FERC in a final rule in November 2013
- Effective April 1\textsuperscript{st}, 2016
- Supersedes version 3
- Version 4 is bypassed
Significant Changes from Current Effective Version

- All BES Cyber Systems must be identified and categorized
  - High, Medium and Low Impact
- High Impact: mostly large Control Centers
- Medium Impact: other Control Centers and generation and transmission assets meeting certain “bright-line” thresholds for impact
- Low Impact: any not already qualified as High or Medium
BES Cyber Systems

- Brings in significant generation and transmission systems not previously in scope
  - Removal of non-routable connectivity exclusions
  - Bright line criteria removes entity defined Risk Based methodology
- CIP-002-5 provides these criteria to categorize systems in scope
Impact Categorization Criteria

- **High Impact**
  - RC Control Centers
  - Large BA Control Centers
  - TOP Control Centers
  - Large GOP Control Centers

- **Medium Impact**
  - Large Generation
    - Qualified relays in Generation significantly affected
    - Subject to Generation threshold impacts
  - Large Transmission Substations
    - Qualified relays in Transmission Substations significantly affected
    - Distance Relay Issue
  - Special Protection Systems
  - Other Control Centers

- **Low Impact**
  - All others not in High or Medium
Cyber Assets

V5 Definition: “Programmable electronic devices, including the hardware, software, and data in those devices.”

In Scope: Microprocessor-based programmable relays, numeric relays

Out of Scope: Electro-mechanical relays, solid state relays that are not externally programmable
From NERC Draft Lessons Learned

- Programmable Electronic Device
  - As noted above, in determining whether a device is programmable, the ERO will look at whether the device has a microprocessor and field-updateable firmware or software.
  - “Field-Updatable” would include devices that have a management port, web interface, socketed chipset, or any external interface that would allow the introduction of a firmware, software or logic update.
  - If the device’s case is sealed in such a way that would require it to be damaged to gain access to the chipset or internal ports then the device in to be considered to be not Field-Updatable.
Configurable Device (versus Programmable Device):
A configurable device is a device that will not allow user changes to its internal programming, but otherwise allows the user to change between pre-defined operational parameters or change hardware options. • If a parameter allows for the entry of formulas, functions and/or any other series of logic steps then this would constitute “programming” and would make the device a programmable electronic device.

E.g. A solid state relay that allows the user to set when the relay will operate but not how the relay operates. These are not considered “programmable”.
BES Cyber Asset

“A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)”

Most microprocessor-based programmable relays meet this definition. Relays are considered to perform the BES function of Dynamic Response.
BES Cyber System

“One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.”

e.g. Group of relays in a relay protection scheme

- Likely to be by same manufacturer
- Primary and secondary groups may have significant differences when from different manufacturers
Identification and Categorization is Critical Path

- For physical security requirements
- For v5 cyber security protection requirements
- New configuration management and change control standard (CIP-010-1)
  - Critical to on-going and sustainable compliance
- Planning and securing resources (financial and other)

**ALL CIP V5 REQUIREMENTS FOR HIGH AND MEDIUM IMPACT MUST BE MET BY APRIL 1\(^{st}\), 2016**

- Targeted completion of identification and categorization of qualified BES Cyber Systems must account for implementation of controls and audit preparedness on April 1\(^{st}\), 2016
Applicable Controls

- Once qualified as a BES Cyber System
  - Qualified relays are subject to cyber security requirements
  - Number of requirements depends on impact category and connectivity, but ALL are subject to some level of protective requirements
- Controls include, among others:
  - Protection from malware
  - Access controls (Passwords)
  - **Configuration Management** (significant effect on updates/upgrades and testing processes)
  - **Transient devices** (significant effect on maintenance and support processes)
Physical Protection – Medium Impact

Relays are required to be physically secured

- Implications on securing relay rooms
- Access control and Authorization
- Background checking
- Training
Electronic Security Requirements – Medium Impact

Connectivity is significant factor in number of applicable requirements

- More requirements if externally connected using a routable protocol
- Security patch monitoring
- Malware protection
- Electronic access control requirements
  - Remote access
  - Default passwords must be changed
  - Password complexity
  - Password change frequency
Incident Response and Backup/Recovery – Medium Impact

- Cyber Security Incident response plan
  - Development, Review and Exercise

- Backup and Recovery Plan
  - Development, Review and Exercise
Configuration Management – Medium Impact

Probably the most impactful from the process standpoint

- Required to document a baseline configuration
- Manage changes (testing, authorization, baseline modifications)
- Vulnerability Assessments
  - Performance, and remediation plans
BES Cyber System Information

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.
BES Cyber System
Information Protection

- Identification of such information
- Access Control and Authorization
- Handling and disposal
A Word on Low Impact

- CIP Version 7 approved by stakeholders in February
- Implementation Plan generally extends another 6 months for certain requirements, different implementation dates
  - Check implementation plan
- More specific requirements, attachments to CIP-003.
Questions