NERC CIP Version 6 -

An EMS Vendor's Perspective

OSI

powering the future

Robert Koziy
Director – Cyber Security Compliance
Open Systems International

- CIP version 3/5 vs 6
- Vendor Challenges
- CIP-013 Supply Chain Security

Version 5 vs 6

- Version 6 resulted in updates to a number of CIP standards:
  - CIP-003-6 – Security Management Controls
  - CIP-004-6 – Personnel & Training
  - CIP-006-6 – Physical Security of BES Cyber Systems
  - CIP-007-6 – System Access Control
  - CIP-009-6 – Recovery Plans for BES Cyber Systems
  - CIP-011-2 – Information Protection
- SCADA/EMS vendor focus

CIP-004-6: Background Checks

- V6 Changes
  - Training for Transient Cyber Assets & Removable Media
- Other notable V5 changes (from v3):
  - PRA for current residence & all locations in prior 7 years
  - Review of vendor PRA criteria and process
  - Access revocation within 24 hours for remote interactive access for all terminations
  - Access for “exceptional circumstances”

CIP-004-6: Background Checks

A Vendor Perspective

- **Issues Encountered:**
  - **Responsible Entities want to conduct their own background checks**
    - This approach is problematic for protection of vendor employee private information
    - Increased liability for RE's that store vendor's employee private information
    - Not required by NERC – see CIP-004-6 R3.4
    - Don't write your policy to require background checks completed by your company
  - **Drug Test Requests**
    - Not required by NERC
    - Costs must be borne by the RE requesting this service
  - **Identity Confirmation – e.g. copies of I-9 forms, driver's license**
    - No protection of vendor employee private information provided to RE's
    - Vendors already collect this information for their employees
    - Vendors are considered a general contractor – our employees are not "contractors"
    - USCIS does not require collection of I9's for general contractors
    - Redacted copies are acceptable to most vendors
    - Don't require personal information in your policy

CIP-004-6: Background Checks

A Vendor Perspective

- **Recommended Vendor Approaches:**
  - Train all development and engineering personnel to NERC CIP v5-6 annually
  - Have all employees complete a background check that meets CIP-004-6 PRA requirements
  - Provide secure online access to employee redacted background checks and training records supporting CIP documentation
  - Provide attestation documents as required

CIP-007-6: System Access Control

- V6 Changes
  - Updates for Transient Cyber Assets & Removable Media

- Other notable V5 changes (from v3):
  - Ports & Services - protection against unnecessary use of ports
  - Security Patch Management changes
    - 35 day evaluation + 35 day implementation period
    - Designation of vendor as patching source
  - Malicious code prevention
    - Broader “non-prescriptive” definition not limited to Anti-virus tools
    - Consider white-listing, network isolation, & IDS/IPS solutions
    - Automatic mitigation recommended
  - Security event alerting
    - Requirement for separate alerting when logging system fails

CIP-007-6: System Access Control

A Vendor Perspective

Issues Encountered

- **Ports & Services**
  - What is acceptable level of detail for justification statements
  - Vendors can & should only provide basic description to confirm port usage
  - Anything more is vendor proprietary and a potential security risk
- **Malcious Code**
  - Automatic quarantine or IPS solutions can be dangerous
  - Several critical executables have been flagged as false positives by AV software
  - Automatic vulnerability scanning tools interfere with production communications
  - Security must be balanced with system reliability

CIP-007-6: System Access Control

A Vendor Perspective

Recommended Vendor Approaches:

- **Removable Media**
  - Options to disable all USB ports in software, re-enable by admin control
- **Ports & Services**
  - Provide complete & detailed documentation of all ports & services on all systems
  - Provide justification statements for all ports and services for vendor software and common O/S or 3rd party tools
- **Provide Patch Management Services for all O/S & 3rd party patches**
- **Malicious Code**
  - Support several 3rd party solutions for whitelisting & HIDS

CIP-013-1: Supply Chain Security

- FERC Order 829 Objectives:
  - Software Integrity and Authenticity
  - Security of Vendor Remote Access to BES Cyber Systems
  - Information System Planning & Procurement
  - Vendor Risk Management & Procurement Controls
- Schedule:
  - CIP-013 Requirements approved by NERC entities in July
  - NERC board adoption occurred in August
  - FERC review beginning September – approval in 3-9 months?
  - Implementation timeframe 1 year after FERC approval (late 2018/2019?)

CIP-013-1: Supply Chain Security

- CIP-013 contains 3 requirements:
  - R1 – develop supply chain security risk management plans for BES Cyber systems
  - R2 – Implement the plan
  - R3 – Review and update the plan
- CIP-013 Implementation Guidance Document (new)
  - Directions to responsible entities on example methods to comply
  - Expectations on utilities and vendors to negotiate new procurement contracts that include security controls based on risk assessment
  - Requirements for vendors to be audited/certified to an industry standard (eg. NIST, SOC2)
- Changes to CIP-010-3 to verify vendor software integrity/authenticity
- Changes to CIP-005-6 for vendor remote access

CIP-005-3: Vendor Remote Access

A Vendor Perspective

- CIP-005-3 Changes
  - R2.4 – Methods for monitoring vendor remote access sessions
  - R2.5 – methods to disable active vendor remote access sessions
- Vendor Recommended Approach
  - No permanent connections allowed
  - Connection initiated by utility using specific protocol/procedure to verify identity
  - Vendor employees are always electronically escorted
  - Vendor view-only session is available and preferred
  - Utility maintains dedicated accounts for vendor employees that conduct remote control sessions

CIP-005-3: Vendor Remote Access

A Vendor Perspective

Issues & Recommendations:

- Two factor tokens for vendors
  - Vendors can't maintain tokens for 10-20 employees for XXX utilities
  - Keep tokens at utility; provide code verbally to vendor when connecting
  - This ensures utility approval of connection and is consistent with NERC guidance on this topic
- Use utility vs vendor's preferred connection method
  - Special requirements for utility remote access arrangements can waste valuable time when systems are in trouble
  - Corporate remote access has different requirements than EMS remote access
  - Utilities should draft a remote access policy jointly with your EMS vendor to consider needs and capabilities on both sides

CIP-010-3: Configuration Management

A Vendor Perspective

- CIP-010-3 changes
  - R1.6 – for a change that deviates from the baseline: verify the identity of the software source and the integrity of the software
- Vendor Preferred Approach
  - Provide software updates/patches via secure sites (eg. HTTPS, SFTP)
  - Provide certified hash values of software via a separate link or repository
  - Use of vendor or 3rd party tools to verify hash values in baselines
  - Optional – vendor digital signature of software for authenticity

CIP-013-1: Supply Chain Security

A Vendor Perspective

- **Many vendor issues & challenges:**
  - Risk based vs prescriptive approach contradictions
  - Diversity of approaches in regions or by auditors will be expensive and unachievable by many suppliers
  - Potential requirement for vendors to meet multiple security certifications will be costly (e.g. NIST vs SOC2 vs SIG vs ISO)
  - EMS vendors can't control 3rd party software vendor security
  - Security departments gone wild

CIP-013-1: Supply Chain Security

A Vendor Perspective

- **Recommendations**
  - You have only 1 (or 2) EMS vendors
  - Don’t place EMS vendors in the same category as business partners providing HR services, financial, etc.
  - EMS vendors don’t have (or want) your Employee personal information (social security, HIPPA, etc) or customer information
  - Adjust & scale your security requirements appropriately based on risk
  - A high dose of common sense is required by all parties to arrive at sensible supply chain security