NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Supply Chain Risk Management – Drafting Team Perspective

James Chuber –Managing Director, Enterprise Supply Chain - Duke Energy

October 31, 2017

RELIABILITY | ACCOUNTABILITY




FERC Order No. 829

*[the Commission directs] that NERC, pursuant to section 215(d)(5) of the FPA, develop a **forward-looking, objective-driven** new or modified Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations.*

- Order No. 829, July 2016

- Four objectives as they relate to cyber security of BES Cyber Systems:
  - Software integrity and authenticity
  - Vendor remote access including machine-to-machine
  - Including security considerations during information system planning
  - Vendor risk management and procurement controls

Note: Plans use a risk-based approach to allow"…flexibility to responsible entities as to how to meet those objective." (see Order No. 829 P.13)

Standards Development Process

- 1st formal comment period January 20 – March 6, 2017
- 2nd formal comment period May 2 – June 15, 2017

CIP-013-1 R1-R3 Summary*

R1: Develop a supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems.

- **R1.1:** Process(es) used in planning for the procurement of BES Cyber Systems
- **R1.2:** Process(es) used in procuring BES Cyber Systems that address the following:
  - 1.2.1. Notification by the vendor of vendor-identified incidents;
  - 1.2.2. Coordination of responses to vendor-identified incidents;
  - 1.2.3. Notification by vendors when access should no longer be granted;
  - 1.2.4. Disclosure by vendors of known vulnerabilities;
  - 1.2.5. Verification of software integrity and authenticity of software/patches; and
  - 1.2.6. Coordination of controls for Interactive Remote Access (IRA) and system-to-system remote access.

*Refer to CIP-013-1 for specific language for each Requirement

CIP-013-1 R1-R3 Summary*

R2: Implement the plan(s) from R1.

- R2 specifically notes:
  - Renegotiation or abrogation of existing contracts not required,
  - Actual contract terms and conditions are out of scope, and
  - Vendor performance and adherence to a contract are out of scope.

R3. Obtain CIP Senior Manager (or delegate) approval of its plan(s) in R1 at least once every 15 calendar months.

*Refer to CIP-013-1 for specific language for each Requirement

Implementation Plan and Guidance

Compliance Guidance - Background

- November 2015, the NERC Board of Trustees approved the Compliance Guidance Policy
  - **Implementation Guidance** – Provides examples for implementing a standard
  - **Compliance Monitoring and Enforcement Program (CMEP**) – Provides direction to ERO Enterprise CMEP staff on approaches to carry out compliance
- Guidance is developed by industry and vetted through pre-qualified organizations
- Guidance does not prescribe the **only** approach to implement a standard
- Guidance is endorsed by ERO Enterprise

Implementation Guidance – CIP-013-1 – R1

R1. Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems

- Plans can use a "risk based approach"
  - System based – risk presented in procuring BES Cyber Systems or services
  - Vendor based – risk posed by suppliers of BES Cyber Systems or services

1.1 Identify process(es) in planning for procurement

- Needs identification
- Specifications
- RFP/RFQ terms and required information

Implementation Guidance – CIP-013-1 – R1

1.1 Continued

- Plans to identify and asses cyber security risk to BES System from a vendor's product or services

- Utilize a cross functional team of subject matter experts to participate in BES Cyber System planning and acquisition processes (Operations, Security, IT, Supply Chain, Legal, etc.)

- Examples of factors the cross functional team could consider in the planning for the procurement of BES Cyber Systems as specified in Part 1.1 include the following:

Implementation Guidance – CIP-013-1 – R1

1.1 Continued

Factors to consider:

- Risk that vendor can introduce to systems
- Vendor's own security processes
- Vendor's lifecycle management and roadmap for continuous improvement
- Vendor's use of third party for review and verification of their security practices
- Third party security assessments or penetration testing of vendor's systems
- Supply Chain channels for vendor to mitigate risk and/or disruptions
- Known system vulnerabilities
- Corporate governance and approval processes

Implementation Guidance – CIP-013-1 – R1

1.1 Continued

Factors to consider (Continued):

- Methods to minimize network exposure of vendor products (firewalls, prevent internet accessibility, etc.)
- Methods to limit and/or control remote access from vendor to Responsible Entity network if applicable
- What is vendor's risk assessment and mitigation plans during their planning and procurement process
- Mitigating controls Responsible Entity can put in place to limit exposure from vendor (alternate sources, minimizing the attack surface, ongoing support, etc.)
- Components not owned and managed by vendor (open source code, 3rd party manufactures)

Implementation Guidance – CIP-013-1 – R1

1.1 Continued

Vendor's Risk management controls to consider:

- Personnel background and screening practices
- Cyber Security training programs
- Formal vendor security programs
- Protection of facilities and systems
- Security engineering principles (see NIST SP 800-53 SA-8 Security Engineering Principles)
- Vendor certifications
- Patch management methodology and ongoing support

Implementation Guidance – CIP-013-1 – R1

1.2 *One or more process(es) used in Procuring BES Cyber Systems that address the following, as applicable (request terms in RFP or during negotiations of procurement contracts):*

1.2.1 Notification by the vendor of vendor-identified incidents related to procured products or services – can request this information during RFP or contract negotiations for vendor's obligation to provide notification

1.2.2 Coordination of responses to vendor-identified incidents related to procured products or services – service level agreements, risk mitigating controls, collaborate with Responsible Entity, etc.

Implementation Guidance – CIP-013-1 – R1

1.2.3 Notification by vendors when remote or onsite access should no longer be granted to vendor representatives. Vendors should have the obligation to inform the Responsible Entity when vendor employees no longer require access due to job changes, termination, etc. (only needed when vendor has access)

1.2.4 Disclosure by vendors of known vulnerabilities – commitment from the vendor for cooperation in obtaining access to summary documentation within a negotiated period of any identified or potential breaches involving the procured product or its supply chain that impact the availability or reliability of BES Cyber System so Entity can take action – review vendor's disposition of publicly disclosed vulnerabilities and uncorrected security vulnerabilities

Implementation Guidance – CIP-013-1 – R1

1.2.5 Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System. In an RFP or during contract negotiations request vendor's patch management program, schedule and availability of updates and patches, software and firmware updates and verification methods, and disclose any third-party components provided or supported by vendor

1.2.6 Coordination of control for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s). Consider the following:

- Minimum privileges required
- Limit vendor access and permissions
- Commitment from the vendor to maintain their IT assets connecting to Entity's network
- Vendor personnel under contract to not share or disclose account credentials
- Vendor to maintain complete and accurate user logs and access credential data for system-to-system connections

Implementation Guidance – CIP-013-1 – R2

R2. Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.

- Implementation of the plan does not require Responsible Entity to renegotiate or abrogate existing contracts

- Additionally, the following issues are beyond the scope of Requirement R2:
  - The actual terms and conditions of the procurement contract
  - Vendor performance and adherence to a contact (Entity has other legal remedies)

- Contracts entering the Responsible Entity's procurement process on or after the effective date are with scope of CIP-013-1

Implementation Guidance – CIP-013-1 – R3

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan (s) specified in Requirement R1 at least once every 15 calendar months

- Responsible Entities should consider new risk and available mitigation measures from a variety of sources (NERC, DOE,DHS, ICS-CERT, NIST, etc.). Some examples of approaches area:
  - Utilize team of subject matter experts from across the organization
  - Industry best practices and guidance
  - Continuous improvement regarding identified deficiencies

Next Steps

- Legal Petition from NERC to FERC requesting approval (Sept. 2017)
- Effective date is the first day of the first calendar quarter that is 18 months after the effective date of Commission's order to approve standard
- NERC Board directed NERC to request stakeholder groups to take actions to support implementation activities:
  - North American Transmission Forum and the North American Generation Forum develop white papers to address best and leading practices in supply chain management – that are shared across the membership
  - National Rural Electric Cooperative Association and the American Public Power Association develop white papers addressing issues contemplated by smaller entities
- NERC collaborate with NERC technical committees to evaluate effectiveness of Supply Chain Standards

References

- Utilities Technology Council (UTC) “Cyber Supply Chain Risk Management for Utilities – Roadmap for Implementation”
- ISO/IEC 27036 – Information Security in Supplier Relationships
- NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition SA-3, SA-8 and SA-22
- NIST SP 800-161 – Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- Energy Sector Control Systems Working Group (ESCWG) – “Cybersecurity Procurement Language for Energy Delivery Systems”

Comments & Questions