Update on Supply Chain Risk Management [SCRM] Standard

Dr. Joseph B. Baugh

Senior Compliance Auditor, Cyber Security

WECC Compliance Workshop – Portland OR – November 14, 2017

Speaker Credentials

- Electrical Utility Experience (45 years)
  - Senior Compliance Auditor, Cyber Security
  - IT Manager & Power Trading/Scheduling Manager
  - IT Program Manager & Project Manager
  - NERC Certified System Operator
  - Barehand Qualified Transmission Lineman
- Educational Experience
  - Degrees earned: Ph.D., MBA, BS-Computer Science
  - Certifications: PMP, CISSP, CISA, CRISC, CISM, PSP, NSA-IAM/IEM
  - Academic & Technical Course Teaching Experience (20+ years)
    - Business Strategy, Leadership, and Management
    - Information Technology, IT Security, and Project Management
    - PMP, CISA, CISSP, CISM, ITIL, & Cisco exam preparation
    - CIP Compliance workshops and other outreach sessions

Impact to Reliability

Ensure entities are aware of new CIP Compliance Requirements and identify WECC's potential audit approach to guide and inform the implementation period for CIP-013-1.

Agenda

- CIP-013-1 SCRM Standard
  - Where have we been?
  - Where we are?
  - Where are we going?
- SCRM related changes for other Standards
  - CIP-005-6 (Part 2.4 - vendor remote access)
  - CIP-010-3 (Part 1.6 - software integrity & authenticity)
- SCRM Implementation Plan
- SCRM Preliminary Audit Approach
- Questions

What is SCRM?

- Project 2016-03 Cyber Security Supply Chain Risk Management (NERC, 2017, *Project Website*)
- FERC (2016) directed "*NERC to develop a forward-looking, objective-based 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 829,* P. 2, p. 49879).

What is SCRM?

- Order 829 described four key security objectives[1] [SO] for SCRM:
  1. Software integrity and authenticity;
  2. Vendor remote access;
  3. Information system planning; and
  4. Vendor risk management and procurement controls.
- SDT set up to develop CIP-013-1

[1] See FERC Order 829 (PP. 48-62, pp. 49885-49887) for Security Objective details

Where Have We Been? First Posting

- R1 – Procurement plans, processes, controls, and methodologies [SO-1; SO-2; SO-3; SO-4]
- R2 – Plan reviews at least every 15 months, with updates, as necessary [Order 829, P. 47]
- R3 – Process(es) for verifying integrity and authenticity of software and firmware for High and Medium BCS [SO-1]
- R4 – Process(es) for controlling vendor remote access to High and Medium BCS [SO-2]
- R5 – Cybersecurity policies for Low impact BES Assets [SO-1; SO-2]

What Happened? The First Ballot

- A record-setting first ballot rejection by industry with major objections to or concerns about:
  - Inclusion of Low impact BES Assets did not align with the other CIP Standards that focus on High and Medium BCS
  - Unclear vendor cooperation expectations
  - Combination of plan development and implementation
  - Ensure CIP-013-1 does not require entities to renegotiate or abrogate existing contracts (i.e., forward-looking as of the effective date)

What Happened? After the Ballot

- The SDT changed directions to focus on High and Medium BCS only,
- Retained SCRM procurement planning, reviews/approvals, and implementation in CIP-013-1, and
- Decided to work with other SDTs to incorporate SCRM security objective language into other Standards, where applicable:
  - CIP-005-6 (added Parts 2.4 & 2.5)
  - CIP-010-3 (added Part 1.6)

Where Are We Now? CIP-013-1: R1.1

R1. Focuses on SCRM procurement plans for High and Medium BCS

- R1.1. Develop processes used in planning procurement to identify and assess cyber security risks to the BES from vendor products or services resulting from:
  i. Procuring and installing vendor equipment and software; and
  ii. Transitions from one vendor to another vendor

Where Are We Now? CIP-013-1: R1.2

- R1.2. One or more processes used in procuring High and Medium BCS to address, as applicable, for products or services supplied to the entity that pose cyber security risk to the entity:
  - R1.2.1. Notification by vendor of vendor-initiated incidents;
  - R1.2.2. Coordination of responses to vendor-initiated incidents;
  - R1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representative(s);

Where Are We Now? CIP-013-1: R1.2

- R1.2. One or more processes used in procuring High and Medium BCS to address, as applicable, for products or services supplied to the entity that pose cyber security risk to the entity:
  - R1.2.4. Disclosure by vendors of known vulnerabilities;
  - R1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES;
  - R1.2.6. Coordination of controls for:
    i. Vendor-initiated Interactive Remote Access, and
    ii. System-to-system remote access with a vendor.

Where Are We Now? CIP-013-1: R2

- R2. Each entity shall implement its SCRM plan specified in R1
  - Implementation does not require entities to renegotiate or abrogate existing contracts, including amendments to master agreements and purchase orders
  - These issues are beyond the scope of R2:
    1) The actual terms and conditions of a procurement contract, and
    2) Vendor performance and adherence to a contract

Where Are We Now? CIP-013-1: R3

- R3. Each entity shall review and obtain CIP Senior Manager or delegate approval of its SCRM plan specified in R1 at least once every 15 calendar months
- The implementation plan calls for the R3 initial review and CIP Senior Manager or delegate's approval of the R1 SCRM plan to occur on or before the effective date of CIP-013-1 (NERC, 2017 July, *Implementation Plan*, p. 3)

Where Are We Going? Second Ballot

- Final Ballot closed on July 20, 2017
- Gained approval for changes to all three Standards

Standard	Quorum / Approval
CIP-005-6	81.59% / 88.79%
CIP-010-3	81.33% / 81.40%
CIP-013-1	82.84% / 84.19%

- NERC Board of Trustees approved CIP-013-1 on August 10, 2017
- All three Standards are pending FERC approval

SCRM Related Changes: Other Standards

- High impact BCS & Medium impact BCS
  - CIP-005-6
  - CIP-010-3
- Low impact BES Assets
  - Removed from industry approved draft
  - SCRM for Low impact BES Assets to be determined
    - May be covered in CIP-003-x
    - May instigate another FERC directive

CIP-005-6 R2 Scope Change

- *The scope of Requirement R2 in CIP-005-6 is expanded from approved CIP-005-5 to address all remote access management, not just Interactive Remote Access.*
- *If a Responsible Entity does not allow remote access (system-to-system or Interactive Remote Access) then the Responsible Entity need not develop a process for each of the subparts in Requirement R2.*
- *The entity could document that it does not allow remote access to meet the reliability objective.*

Source: NERC, 2017 July, CIP-005-6, *Rationale for R2* section, p. 24.

CIP-005-6 Part 2.4 & 2.5 - Objectives

- *The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions*.
- *While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement*.
- *The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52)*.

Source: CIP-005-6 (p. 24).

SCRM Provisions – CIP-005-6: Part 2.4

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-6: Part 2.4

- Indicates monitoring and control of active vendor remote access sessions is appropriate
- Vendor remote access sessions includes Interactive Remote Access and system-to-system access for vendor sessions
- A *vendor,* as used in the standard, is NOT a defined term, but may include:
    i. Developers or manufacturers of information systems, system components, or information system services;
    ii. Product resellers; or
    iii. System integrators (CIP-005-6, p. 24).

SCRM Provisions – CIP-005-6: Part 2.5

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

CIP-005-6: Part 2.5

- Requires one or more documented methods to disable active vendor remote access, including
  - Interactive Remote Access, and
  - System-to-system remote access.
- May have separate methods to disable each category of vendor remote access, as applicable.

CIP-005-6: Parts 2.4 & 2.5 Evidence

- The Part 2.4 *Measures* section provides some methods that may be used to identify, monitor, and control vender remote access sessions
- Part 2.5 evidence may include:
  - Documented methods for disabling the two types of vendor remote access
  - Evidence that vendor remote access was disabled, when and as applicable
  - Internal controls to ensure vendor remote access is disabled when no longer required, or the entity is notified by the vendor of a cyber security event

SCRM Provisions – CIP-010-3: Part 1.6

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

CIP-010-3: Part 1.6 - Objective

- *The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software.*
- *This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System.*
- *The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.*

Source: NERC, 2017 July, CIP-010-3, *Software Verification* section, p. 24.

CIP-010-3: Part 1.6

- Requires entities to:
  - Verify the identity of the software source
  - Verify the integrity of the software source
- The methodology used for such verifications is left to the entity to define
- Part 1.6 is not limited to security patches

CIP-010-3: Part 1.6 – Evidence

- Evidence may include change request records to confirm the entity's documented process(es) for such identity and integrity verifications occurred as described
- Leverage existing documented CIP cyber security policies and controls
- Document new processes and controls to manage verifications for identify of software sources and integrity of software obtained from those sources (e.g., *Guidelines and Technical Basis* section, p. 39)

SCRM Implementation Plan - Timeline

- Three Standards currently pending FERC Approval
- Effective 1st day of 1st quarter that is 18 months after applicable approval order
- If FERC approves at the November or December meeting, SCRM may be effective as early as July 1, 2019

2017		2018												2019						
Q4		Q1			Q2			Q3			Q4			Q1			Q2			Q3
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	20
Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul

Effective Date - July 1, 2019

- What if FERC issues a NOPR for CIP-013-1 and provides a typical stakeholder comment period?
  - We could easily add another six to twelve months

SCRM Implementation Plan – R1

- R1.1. Develop documented processes to provide a risk-based approach to identify potential cyber security risks resulting from:
  i. Procuring and installing vendor equipment and software, and
  ii. Transitions from one vendor to another vendor
- R1.2. Document procurement plans and processes to manage identified risks
- See NERC (2017 April, *Implementation Guidance: R1.2.1 – R1.2.6*, pp. 2-7) for more details

SCRM Implementation Plan – R2

- Implement SCRM plans specified in R1:
  - *Does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).*
  - *Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1.*
  - *Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.*

Source: NERC, 2017 April, *Implementation Guidance*, p. 8.

SCRM Implementation Plan – R3

- Review SCRM plans and processes identified in R1 by Entity SMEs using:
  - Requirements and guidelines
  - Industry best practices
  - Mitigating controls
  - Internal entity continuous improvement feedback
- Obtain CIP Senior Manager or delegate approval:
  - Initially, on or before the effective date
    - Implies R1 documented plans and processes must be developed on or before the effective date, as well
  - At least once every 15 calendar months, thereafter

SCRM Audit Approach

- The CIP team is still evaluating its audit approach
- This process will continue until FERC approves CIP-013-1 and the effective date is established
- The CIP Team will present updated information on the audit approach in a future outreach event
- For now, consider how vendor products and services impact your High and Medium BCS
- Evaluate and document cyber security risks associated with each applicable BCS
- Consider preliminary procurement planning and RFP template development to address cyber security risks

Questions & Contact Information

Joseph B. Baugh
(360)600-6631 – Office
(520)331-6351 – Cell
jbaugh@wecc.biz

References

- FERC. (2016 July 29). *Order No. 829: Revised Critical Infrastructure Protection Reliability Standards*. 18 CFR Part 40: 156 FERC ¶ 61,050: Docket No. RM15-14-002. Published in *Federal Register, 81*(146*)* [pp. 49879-49894]. Retrieved from https://www.gpo.gov/fdsys/pkg/FR-2016-07-29/pdf/2016-17842.pdf
- NERC. (2017). *Project 2016-03 Cyber Security Supply Chain Risk Management* [*Project Website*]. Retrieved from http://www.nerc.com/pa/Stand/Pages/Project201603CyberSecuritySupplyChainManagement.aspx
- NERC. (2017 April). *Cyber Security Supply Chain Risk Management Plans*: *Implementation Guidance for CIP-013-1*. Retrieved from http://www.nerc.com/pa/Stand/Project%20201603%20Cyber%20Security%20Supply%20Chain%20Managem/Implementation_Guidance_071117.pdf

References

- NERC. (2017 July). *CIP-005-6 – Cyber Security – Electronic Security Perimeter(s)*. Retrieved from http://www.nerc.com/pa/Stand/Project%20201603%20Cyber%20Security%20Supply%20Chain%20Managem/CIP-005-6_Clean_071117.pdf
- NERC. (2017 July). *CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments.* Retrieved from http://www.nerc.com/pa/Stand/Project%20201603%20Cyber%20Security%20Supply%20Chain%20Managem/CIP-010-3_Clean_071117.pdf
- NERC. (2017 July). *CIP-013-1 – Cyber Security - Supply Chain Risk Management.* Retrieved from http://www.nerc.com/pa/Stand/Project%20201603%20Cyber%20Security%20Supply%20Chain%20Managem/CIP-013-1_Clean_071117.pdf
- NERC. (2017 July). *Implementation Plan: Project 2016-03 Cyber Security Supply Chain Risk Management Reliability Standard*. Retrieved from http://www.nerc.com/pa/Stand/Project%20201603%20Cyber%20Security%20Supply%20Chain%20Managem/Implementation_Plan_Clean_071117.pdf