NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Supply Chain Risk Management

Corey Sellers, Southern Company
JoAnn Murphy, PJM Interconnection
May 18, 2017

RELIABILITY | ACCOUNTABILITY




Administrative Items

- NERC Antitrust Guidelines
  - It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.
- Notice of Open Meeting
  - Participants are reminded that this webinar is public. The access number was widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

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

- Standard(s) must be filed by September 2017

Proposed Changes to CIP Standards

FERC Order 829 Objective	Version 1 of CIP-013	Version 2 of CIP-013	… plus modifications to other existing CIP Standards
1 – 4	R1 Implement the supply chain cyber security risk management plan for BES Cyber Systems (including Electronic Access Control and Monitoring Systems, Personnel Access Control Systems, and Protected Cyber Assets)	R1 – Develop the supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems, including specific procurement processes R2 – execute plan(s) from R1	No change – proposed changes to CIP-003 to cover low impact BES Cyber Systems have been removed
1 – 4	R2 Review plan(s) every 15 months	now R3 but remained essentially the same – Review plan(s) every 15 months	No change
1	R3 (software authenticity)	R3 removed and moved to >>	CIP-010-3 (“software integrity and authenticity”) • Table R1 Part 1.6 added
2	R4 (vendor remote access)	R4 removed and moved to >>	CIP-005-6 (“visibility and disabling”) • Table R2 Part 2.4/2.5 added
	R5 (Low impact BES Cyber Systems)	Removed	No change

Requirement R1 Key Changes

- Focus R1 on High and Medium Impact Bulk Electric System (BES) Cyber Systems
- Removed Low Impact BES Cyber System Requirements
- Split into two requirements:
  - R1 now “develop one or more… plan(s)”
  - R2 now “implement… plan(s)”
- Specifically note (1) renegotiation or abrogation of existing contracts is not required, (2) actual contract terms and conditions are out of scope, and (3) vendor performance and adherence to a contract are out of scope

Requirement R2 Key Changes

R2 (Prior Draft) Requires entities to review the plan every 15 calendar months and address new risks or mitigation measures, if any.

- Requirement (R3 in current draft) mirrors other 15 month review language
- No explicit “address new risks or mitigation measures” requirement

CIP-013-1 Requirements Summary

- R1 requires entities to develop supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. Include:
  - Process used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s)
  - Process used in procuring BES Cyber Systems that address the cyber security topics listed in the Parts 1.2.1 through 1.2.6

- R2 requires entities to implement the plan

Link to posted draft

CIP-013-1 Requirements Summary

- R3 requires entities to review and obtain CIP Senior Manager or delegate approval of the plan at least once every 15 calendar months

Link to posted draft

Requirement R3 Key Changes

Requires entities to implement a process for verifying the integrity and authenticity of software and firmware and any upgrades to software and firmware before being placed in operation on high and medium impact BES Cyber

- Moved this operational requirement into existing CIP standards
  - Received assistance from CIP Modifications Standard Drafting Team (SDT)
  - Proposed change to CIP-010 (Table R1 Part 1.6 added)
- Adding phrase *"when the method to do so is available to the Responsible Entity from the software source"* to account for situations in which a vendor cannot or will not provide needed functionality

Requirement R4 Key Changes

Requires entities to implement a process for controlling vendor remote access to high and medium impact BES Cyber Systems

- Moved this operational requirement into existing CIP standards
  - Received assistance from CIP Modifications SDT
  - Proposed change to CIP-005 (Table R2 Part 2.4/2.5 added)
- Focus on visibility and the ability to disable remote access
  - 2.4 – Have "one or more methods for determining active vendor remote access sessions" (including Interactive Remote Access (IRA) and system-to-system remote access)
  - 2.5 – Have "one or more methods to disable active vendor remote access" (including IRA and system-to-system)

Requirement R5 Key Changes

Require entities to have documented cyber security policies that address software integrity and vendor remote access as they apply to low impact BES Cyber Systems

- Removed R5 – no procurement and no new operational requirements on Low Impact BES Cyber Systems

Implementation Guidance

- SDT developed *Implementation Guidance* to provide examples of approaches for complying with CIP-013-1
- The following **examples** are included:
  - Risk-based approach to Cyber Security Supply Chain Risk Management plans (R1)
  - Processes for planning to procure BES Cyber Systems that identify and assess cyber security risks from vendor products or services (R1 Part 1.1)
  - Request-for-proposal or negotiation provisions to address topics in R1 Part 1.2.1 – 1.2.6
  - Processes for periodically reviewing and approving plans (R3)

- Implementation Guidance has been submitted for endorsement per NERC's *Compliance Guidance Policy*

Standards Development Process

- 1st formal comment period January 20 – March 6, 2017
- 2nd formal comment period May 2 – June 15, 2017
  - Ballot pools are open for CIP-005-6 and CIP-010-3 through May 31, 2017

Discussion

Type and send questions using webinar Q&A

Contact Information

- Refer to the Project 2016-03 page for more information
- Email mark.olson@nerc.net to join the email list
- Corey Sellers, Southern Company, SDT Chair
  - Email at mcseller@southernco.com
- JoAnn Murphy, PJM Interconnection, SDT Vice Chair
  - Email at joann.murphy@pjm.com