NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Supply Chain Risk Management

Corey Sellers, SDT Chair, Southern Company
JoAnn Murphy, SDT Vice Chair, PJM Interconnection
February 2, 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

Security Objectives

- Plans must address four objectives as they relate to 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

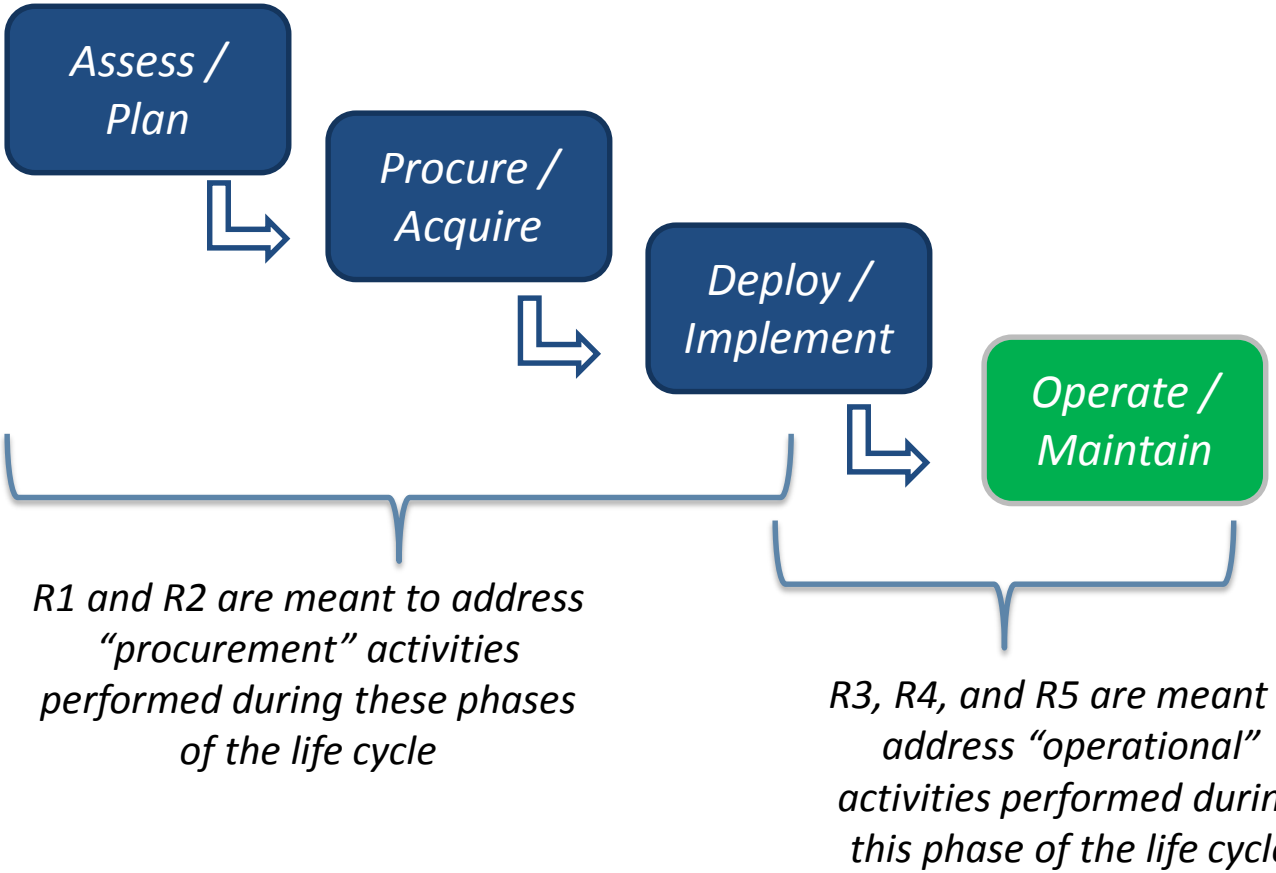
"The Commission does not require NERC to impose any specific controls nor… to propose 'one-size-fits-all' requirements. The new or modified Reliability Standard should instead require responsible entities to develop a plan to meet the four objectives… while providing flexibility to responsible entities as to how to meet those objectives."

(see Order No. 829 P. 13)

Standards Development Process

- Drafting team appointed September 2016
- Standards Authorization Request posted October 2016
- Technical conference November 2016
- September 2017 filing deadline will limit ballot opportunities

Notional BES Cyber System Life Cycle



*Note: Plans developed in R1 should "identify and assess risk(s) during the procurement and deployment of vendor products and services" (R1 1.1.1) thus addressing risks during the 1st three life cycle phases

Draft CIP-013-1

- **Title:** Cyber Security – Supply Chain Risk Management
- **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

- Link to draft CIP-013-1

Requirement R1

- Requires entities to **implement one or more documented supply chain risk management plan(s)** for mitigating risks to BES Cyber Systems and associated cyber systems

- Plan(s) shall address:
  - The use of controls in BES Cyber System planning and development to:
    - Identify and assess risk(s) during the procurement and deployment of vendor products and services; and
    - Evaluate methods to address identified risk(s)
  - The use of controls in procuring vendor product(s) or service(s)

Requirement R1

- The procurement controls must address processes for or coordination of:
  - Notification of vendor security events;
  - Notification when vendor employee remote or onsite access should no longer be granted;
  - Disclosure of known vulnerabilities;
  - Response to vendor-related cyber security incidents;
  - Verifying software integrity and authenticity of all software and patches that are intended for use;
  - Remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and
  - Other process(es) to address risk(s), if applicable.

Notes on Requirement R1

- Plans should address all BES Cyber Systems (high, medium, and low) but can do so with a risk-based approach
  - "…*flexibility as to how to reach the objective*…" (see Order No. 829 P. 13)

- ***Vendors*** as used in proposed CIP-013-1 include:
  - Developers or manufacturers of information systems, system components, or information system services
  - Product resellers
  - System integrators

Notes on Requirement R1

- Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (see Order No. 829 P. 36)

- Implementation of procurement controls is accomplished through the entity's procurement processes
  - Requests for Proposals
  - Negotiations with vendors

- Obtaining specific controls in the negotiated contract may not be feasible and is not a failure to implement an entity's plan

Requirement R2

- Requires entities to review the plan every 15 calendar months and address new risks or mitigation measures, if any

Notes on Requirement R2

- Periodic assessment ensures plans remain up-to-date (Order No. 829 P 46-47)
- Sources of information to consider include:
  - NERC
  - Electricity Information Sharing and Analysis Center (E-ISAC)
  - Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
  - Canadian Cyber Incident Response Centre (CCIRC)

Requirement R3

- 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 Systems

- Ensures software was not modified without the awareness of the supplier and is not counterfeit

Requirement R4

- Requires entities to implement a process for **controlling vendor remote access** to **high** and **medium** impact BES Cyber Systems
  - Authorization of remote access by the Responsible Entity;
  - Logging and monitoring of remote access sessions to detect unauthorized activity; and
  - Disabling or otherwise responding to unauthorized activity during remote access sessions.

- Applies to vendor-initiated Interactive Remote Access and system-to-system remote access with a vendor

Requirement R5

- 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

- Similar to approved CIP-003-6 Requirement R1 Part 1.2

- Consistent with approved standards in not requiring inventory of low impact BES Cyber Systems or lists of authorized users

Considerations

- Combination of procurement controls and operational controls needed to satisfy directives
- Development of a new standard was needed given directives and deadline (v. revising approved standards)
  - Scope of existing standards v. scope of Order No. 829 directives
  - Regulatory deadline does not allow for expanding existing standards
- Order No. 829 implies broad scope of cyber systems
  - High, Medium, Low BES Cyber Systems
  - BES Cyber Systems and associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets

Considerations

- Effective procurement and contract negotiation is a collaborative process between the entity and vendor
  - Requirements are not intended to directly impose obligations on vendors
  - Requirements should not limit the productive two-way conversation that occurs in effective procurement
- Results-based requirements are needed to provide entities with flexibility to meet the objectives (v. prescriptive requirements)
  - SDT developed ***Technical Guidance and Examples*** document to promote industry understanding of results-based requirements

Questions and Answers

Send questions using webinar chat

Standards Development Process

- Formal comment period January 20th – March 6, 2017
  - Initial Ballot February 24 – March 6, 2017

- SDT is seeking stake holder input to further develop ***Technical Guidance and Examples***

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