Federal Energy Regulatory Commission | Washington D.C.

FERC Order No. 829 Supply Chain Risk Management

SERC CIP Compliance Seminar

September 27, 2016

Summary

- Background: Revised CIP NOPR, Order No. 822, and the SCRM Technical Conference
- Order No. 829
- 4 Objectives:
  - Software integrity and authenticity
  - Vendor remote access
  - Information system planning
  - Vendor risk management and procurement controls
- Flexibility

Revised CIP Reliability Standards NOPR

- Issued July 16, 2015
- Changes in the bulk electric system threat landscape
- Malware campaigns targeted supply chain vendors
- Gap in the protections under CIP Reliability Standards

Risks Posed by Lack of Controls

- Global ICT and ICS supply chains provide hardware, software and operations support for computer networks
- Adversaries can directly or indirectly affect the management/operations of companies:
  - Insertion of counterfeits
  - Unauthorized production, tampering, theft, or insertion of malicious software

Order No. 822

- Issued January 21, 2016
- After reviewing comments, Commission scheduled a staff-led technical conference for January 28, 2016 –

  "... in order to facilitate a structured dialogue on supply chain risk management issues identified by the NOPR."
- Commission would determine appropriate action after the scheduled technical conference

SCRM Technical Conference

- Held January 28, 2016
- Three panels addressed:
  - Need for a New or Modified Reliability Standard
  - Scope and Implementation of a New or Modified Standard
  - Current Supply Chain Risk Management Practices and Collaborative Efforts

Order No. 829

- Issued July 21, 2016
- Directed NERC "to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated bulk electric system operations."

Order No. 829 (contd)

- Requires four objectives to be met
  - Software integrity and authenticity
  - Vendor remote access
  - Information system planning
  - Vendor risk management and procurement controls
- NERC must submit the proposed standard by September 27, 2017

Objective 1: Software Integrity & Authenticity

- Risk:
  - Attacker could exploit legitimate vendor patch management processes
  - Examples
    - 2014 ICS-CERT alert on ICS Focused Malware included “Watering Hole” attack
    - Operation Dust Storm and the Japanese electric sector infrastructure

Objective 1: Software Integrity & Authenticity

- Scope:
  - Ensure identity of the software publisher for all software and patches that are intended for use on BES Cyber Systems
  - Ensure integrity of the software and patches before they are installed in the BES Cyber System environment

Objective 2: Vendor Remote Access

- Risk:
  - Vendor credentials could be stolen, used to access a BES Cyber System without responsible entity's knowledge
  - Compromise at trusted vendor could traverse an unmonitored connection into a responsible entity's BES Cyber System
  - 2015 cyberattack on Ukraine's power grid

Objective 2: Vendor Remote Access

- Scope
  - "Covers both user-initiated and machine-to-machine vendor remote access."
  - Control vendor remote access
  - Example controls from NIST
    - Control SC-7 addresses monitoring and control mechanisms at the boundary between the entity and its suppliers
    - Control AC-17 addresses usage restrictions, configuration/connection requirements, including the ability to rapidly disconnect or disable remote access

Objective 3: Information System Planning

- Risk:
  - Responsible entity could unintentionally plan to procure and install unsecure equipment or software within their information systems
  - Responsible entity could unintentionally fail to anticipate security issues that may arise due to network architecture or during technology and vendor transitions
  - For example, BlackEnergy malware campaign

Objective 3: Information System Planning

- Scope:
  - Requires a responsible entity to "include security considerations as part of its information system planning and system development lifecycle processes."
  - Requires responsible entity's CIP Senior Manager to ID and document "the risks of proposed information system planning and system development actions."

Objective 3: Information System Planning

- Scope (con.)
  - Example controls from NIST
    - SA-3 addresses managing information systems using an organizationally-defined system development life cycle that incorporates information security
    - SA-8 recommends using secure engineering principles for future projects, such as developing layered protections
    - SA-22 addresses replacement of components when support is no longer available

Objective 4: Vendor Risk Management and Procurement Controls

- Risk:
  - Responsible entities could enter into contracts with vendors who pose significant risks to their information systems
  - Products procured by a responsible entity could fail to meet minimum security criteria
  - Compromised vendor may not provide adequate notice to responsible entities with whom the vendor is connected

Objective 4: Vendor Risk Management and Procurement Controls

- Scope:
  1. Vendor security event notification processes
  2. Vendor personnel termination notification for employees with access to remote and onsite systems
  3. Products/services vulnerability disclosures, such as accounts that are able to bypass authentication or the presence of hardcoded passwords

Vendor Risk Management and Procurement Controls (contd)

- Scope (con.):
  4. Coordinated incident response activities
  5. Other related aspects of procurement
- Example controls
  - *DOE Cybersecurity Procurement Language for Energy Delivery Systems*
  - NIST SA-4 addresses defining requirements for systems acquisition

Flexibility

- Directive to develop a forward-looking, objective-based Reliability Standard that includes security objectives that a responsible entity must achieve
- No specific controls are imposed
- No requirement for “one-size-fits-all”

QUESTIONS