NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security Supply Chain Risk Management Plans

Implementation Guidance for CIP-013-2

RELIABILITY | ACCOUNTABILITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction iii
Requirement R1 1
General Considerations for R1 1
Implementation Guidance for R1 2
Requirement R2 8
General Considerations for R2 8
Requirement R3 9
General Considerations for R3 9
Implementation Guidance for R3 9
References 10

Introduction

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that addresses cyber security supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

> [The Commission directs] 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. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

On October 18, 2018, the Federal Energy Regulatory Commission (FERC) issued Order No. 850 approving the supply chain risk management Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments) submitted by the North American Electric Reliability Corporation (NERC), and directing NERC to include Electronic Access Control or Monitoring Systems (EACMS).

On May 17, 2019, NERC published Cyber Security Supply Chain Risks Report recommending the inclusion of Physical Access Control Systems (PACS).

Reliability Standard **CIP-013-2 – Cyber Security – Supply Chain Risk Management** addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems[1] and their associated EACMS and PACS.

This implementation guidance provides considerations for implementing the requirements in CIP-013-2 and examples of approaches that responsible entities could use to meet the requirements. The examples do not constitute the only approach to complying with CIP-013-2. Responsible Entities may choose alternative approaches that better fit their situation.

[1] Responsible Entities identify high and medium impact BES Cyber Systems, and their associated EACMS and PACS, according to the identification and categorization process required by CIP-002-5, or subsequent version of that standard.

Requirement R1

R1. *Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include:*

1.1. *One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).*

1.2. *One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:*

1.2.1. *Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

1.2.2. *Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

1.2.3. *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

1.2.4. *Disclosure by vendors of known vulnerabilities;*

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; and*

1.2.6. *Coordination of controls for vendor-initiated remote access.*

General Considerations for R1

The following are some general considerations for Responsible Entities as they implement Requirement R1:

First, in developing their supply chain cyber security risk management plan(s), Responsible entities should consider how to leverage the various components and phases of their processes (e.g. defined requirements, request for proposal, bid evaluation, external vendor assessment tools and data, third party certifications and audit reports, etc.) to help them meet the objective of Requirement R1 and give them flexibility to negotiate contracts with vendors to efficiently mitigate risks. Focusing solely on the negotiation of specific contract terms could have unintended consequences, including significant and unexpected cost increases for the product or service or vendors refusing to enter into contracts.

Additionally, a Responsible Entity may not have the ability to obtain each of its desired cyber security controls in its contract with each of its vendors. Factors such as competition, limited supply sources, expense, criticality of the product or service, and maturity of the vendor or product line could affect the terms and conditions ultimately negotiated by the parties and included in a contract. This variation in contract terms is anticipated and, in turn, the note in Requirement R2 provides that the actual terms and conditions of the contract are outside the scope of Reliability Standard CIP-013-2.

Note: Implementation of the plan 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 Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

The focus of Requirement R1 is on the steps the Responsibility Entity takes to consider cyber security risks from vendor products or services during BES Cyber System planning and procurement. In the event the vendor is unwilling to engage in the negotiation process for cyber security controls, the Responsible Entity could explore other sources of supply or mitigating controls to reduce the risk to the BES cyber systems, as the Responsible Entity's circumstances allow.

In developing and implementing its supply chain cyber security risk management plan, a Responsible Entity may consider identifying and prioritizing security controls based on the cyber security risks presented by the vendor and the criticality of the product or service to reliable operations. For instance, Responsible Entities may establish a baseline set of controls for given products or services that a vendor must meet prior to transacting with that vendor for those products and services (i.e., "must-have controls"). As risks differ between products and services, the baseline security controls – or "must haves" – may differ for the various products and services the Responsible Entities procures for its BES Cyber Systems. This risk-based approach could help create efficiencies in the Responsible Entity's procurement processes while meeting the security objectives of Requirement R1.

The objective of addressing the verification of software integrity and authenticity during the procurement phase of BES Cyber System(s) (Part 1.2.5) is to identify the capability of the vendor(s) to ensure that the software installed on BES Cyber System(s) is trustworthy. Part 1.2.5 is not an operational requirement for Responsible Entities to perform the verification; instead, Part 1.2.5 is aimed at identifying during the procurement phase the vendor's capability to provide software integrity and authenticity assurance and establish vendor performance based on the vendor's capability in order to implement CIP-010-4, Requirement R1, Part 1.6.

Implementation Guidance for R1

Responsible entities use various processes as they plan to procure BES Cyber Systems. Below are some examples of approaches to comply with this requirement:

R1. *Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include:*

- The Responsible Entity could establish one or more documents explaining the process by which the Responsible Entity will address supply chain cyber security risk management for high and medium impact BES Cyber Systems and their associated EACMS and PACS. To achieve the flexibility needed for supply chain cyber security risk management, Responsible Entities can use a "risk-based approach". One element of, or approach to, a risk-based cyber security risk management plan is **system-based**, focusing on specific controls for high and medium impact BES Cyber Systems and their associated EACMS and PACS to address the risks presented in procuring those systems or services for those systems. A risk-based approach could also be **vendor-based**, focusing on the risks posed by various vendors of its BES Cyber Systems. Entities may combine both of these approaches into their plans. This flexibility is important to account for the varying "needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risk (FERC Order No. 829 P 44)."

1.1. *One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when planning for the procurement of BES Cyber Systems to identify and assess cyber security risks to the Bulk Electric System from vendor products or services as specified in the requirement. Examples of processes, or outcomes of these processes, for complying with Part 1.1 are described below. A Responsible Entity could comply with Part 1.1 using either the first (team review) approach, or the second (risk assessment process) approach, a combination of the two approaches, or another approach determined by the Responsible Entity to comply with Part 1.1.

- A Responsible Entity can develop a process to form a team of subject matter experts from across the organization to participate in the BES Cyber System planning and acquisition process(es). The Responsible Entity should consider the relevant subject matter expertise necessary to meet the objective of Part 1.1 and include the appropriate representation of business operations, security architecture, information communications and technology, supply chain, compliance, and legal. Examples of factors that this team could consider in planning for the procurement of BES Cyber Systems as specified in Part 1.1 include:
  - Cyber security risk(s) to the BES that could be introduced by a vendor in new or planned modifications to BES Cyber Systems.
  - Vendor security processes and related procedures, including: system architecture, change control processes, remote access requirements, and security notification processes.
  - Periodic review processes that can be used with critical vendor(s) to review and assess any changes in vendor's security controls, product lifecycle management, supply chain, and roadmap to identify opportunities for continuous improvement.
  - Vendor use of third party (e.g., product/personnel certification processes) or independent review methods to verify product and/or service security practices.
  - Third-party security assessments or penetration testing provided by the vendors.
  - Vendor supply chain channels and plans to mitigate potential risks or disruptions.
  - Known system vulnerabilities; known threat techniques, tactics, and procedures; and related mitigation measures that could be introduced by vendor's information systems, components, or information system services.
  - Corporate governance and approval processes.
  - Methods to minimize network exposure, e.g., prevent internet accessibility, use of firewalls, and use of secure remote access techniques.
  - Methods to limit and/or control remote access from vendors to Responsible Entity's BES Cyber Systems.
  - Vendor's risk assessments and mitigation measures for cyber security during the planning and procurement process.
  - Mitigating controls that can be implemented by the Responsible Entity of the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.
- A Responsible Entity can develop a risk assessment process to identify and assess potential cyber security risks resulting from (i) procuring and installing vendor equipment and software and (ii) transitions from one vendor(s) to another vendor(s). This process could consider the following:
  - Potential risks based on the vendor's information systems, system components, and/or information system services / integrators. Examples of considerations include:

- Critical systems, components, or services that impact the operations or reliability of BES Cyber Systems.
- Product components that are not owned and managed by the vendor that may introduce additional risks, such as open source code or components from third party developers and manufacturers.

- Potential risks based on the vendor's risk management controls. Examples of vendor risk management controls to consider include[2]:
  - Personnel background and screening practices by vendors.
  - Training programs and assessments of vendor personnel on cyber security.
  - Formal vendor security programs which include their technical, organizational, and security management practices.
  - Vendor's physical and cyber security access controls to protect the facilities and product lifecycle.
  - Vendor's security engineering principles in (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development lifecycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are training on how to build security software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. (NIST SP 800-53 SA-8 – Security Engineering Principles).
  - System Development Life Cycle program (SDLC) methodology from design through patch management to understand how cyber security is incorporated throughout the vendor's processes.
  - Vendor certifications and their alignment with recognized industry and regulatory controls.
  - Summary of any internal or independent cyber security testing performed on the vendor products to ensure secure and reliable operations.[3]
  - Vendor product roadmap describing vendor support of software patches, firmware updates, replacement parts and ongoing maintenance support.
  - Identify processes and controls for ongoing management of Responsible Entity and vendor's intellectual property ownership and responsibilities, if applicable. Examples include use of encryption algorithms for securing software code, data and information, designs, and proprietary processes while at rest or in transit.
- Based on risk assessment, identify mitigating controls that can be implemented by the Responsible Entity or the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.

[2] Tools such as the Standardized Information Gathering (SIG) Questionnaire from the Shared Assessments Program can aid in assessing vendor risk.

[3] For example, a Responsible Entity can request that the vendor provide a Standards for Attestation Engagements (SSAE) No. 18 SOC 2 audit report.

1.2. *One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when procuring BES Cyber Systems to address Parts 1.2.1 through 1.2.6. The following are examples of processes, or outcomes of these processes, for complying with Part 1.2.

- Request cyber security terms relevant to applicable Parts 1.2.1 through 1.2.6 in the procurement process (request for proposal (RFP) or contract negotiation) for BES Cyber Systems to ensure that vendors understand the cyber security expectations for implementing proper security controls throughout the design, development, testing, manufacturing, delivery, installation, support, and disposition of the product lifecycle[4].
- During negotiations of procurement contracts or processes with vendors, the Responsible Entity can document the rationale, mitigating controls, or acceptance of deviations from the Responsible Entity's standard cyber security procurement language that is applicable to the vendor's system component, system integrators, or external service providers.

Examples of ways that a Responsible Entity could, through process(es) for procuring BES Cyber Systems required by Part 1.2, comply with Parts 1.2.1 through 1.2.6 are described below.

1.2.1. *Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems (*e.g.,* "security event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. Security event notifications to the Responsible Entity should be sent to designated point of contact as determined by the Responsible Entity and vendor. Examples of information to request that vendor's include in notifications to the Responsible Entity are(i) mitigating controls that the Responsible Entity can implement, if applicable (ii) availability of patch or corrective components, if applicable.

1.2.2. *Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*

- A Responsible Entity and vendor can agree on service level agreements for response to cyber security incidents and commitment from vendor to collaborate with the Responsible Entity in implement mitigating controls and product corrections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that, in the event the vendor identifies a vulnerability that has resulted

[4] An example set of baseline supply chain cyber security procurement language for use by BES owners, operators, and vendors during the procurement process can be obtained from the "Cybersecurity Procurement Language for Energy Delivery Systems" developed by the Energy Sector Control Systems Working Group (ESCSWG).

in a cyber security incident related to the products or services provided to the Responsible Entity, the vendor should provide notification to Responsible Entity. The contract could specify that the vendor provide defined information regarding the products or services at risk and appropriate precautions available to minimize risks. Until the cyber security incident has been corrected, the vendor could be requested to perform analysis of information available or obtainable, provide an action plan, provide ongoing status reports, mitigating controls, and final resolution within reasonable periods as agreed on by vendor and Responsible Entity.

1.2.3. *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification to the Responsible Entity when vendor employee remote or onsite access should no longer be granted. This does not require the vendor to share sensitive information about vendor employees. Circumstances for no longer granting access to vendor employees include: (i) vendor determines that any of the persons permitted access is no longer required, (ii) persons permitted access are no longer qualified to maintain access, or (iii) vendor's employment of any of the persons permitted access is terminated for any reason. Request vendor cooperation in obtaining Responsible Entity notification within a negotiated period of time of such determination. The vendor and Responsible Entity should define alternative methods that will be implemented in order to continue ongoing operations or services as needed.
- If vendor utilizes third parties (or subcontractors) to perform services to Responsible Entity, require vendors to obtain Responsible Entity's prior approval and require third party's adherence to the requirements and access termination rights imposed on the vendor directly.

1.2.4. *Disclosure by vendors of known vulnerabilities;*

- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining access to summary documentation within a negotiated period of any identified security breaches involving the procured product or its supply chain that impact the availability or reliability of the Responsible Entity's BES Cyber System. Documentation should include a summary description of the breach, its potential security impact, its root cause, and recommended corrective actions involving the procured product.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining, within a negotiated time period after establishing appropriate confidentiality agreement, access to summary documentation of uncorrected security vulnerabilities in the procured product that have not been publicly disclosed. The summary documentation should include a description of each vulnerability and its potential impact, root cause, and recommended compensating security controls, mitigations, and/or procedural workarounds.
- During procurement, review with the vendor summary documentation of publicly disclosed vulnerabilities in the product being procured and the status of the vendor's disposition of those publicly disclosed vulnerabilities.

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; and*

- During procurement, request access to vendor documentation detailing the vendor patch management program and update process for all system components being procured (including third-party hardware, software, and firmware). This documentation should include the vendor's method or recommendation for how the integrity of the patch is validated by Responsible Entity. Ask vendors to describe the processes they use for delivering software and the methods that can be used to verify the integrity and authenticity of the software upon receipt, including systems with preinstalled software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide access to vendor documentation for the procured products (including third-party hardware, software, firmware, and services) regarding the release schedule and availability of updates and patches that should be considered or applied. Documentation should include instructions for securely applying, validating and testing the updates and patches.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within a reasonable period for duration of the product life cycle. Consideration regarding service level agreements for updates and patches to remediate critical vulnerabilities should be a shorter period than other updates. If updates cannot be made available by the vendor within a reasonable period, the vendor should be required to provide mitigations and/or workarounds.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide fingerprints or cipher hashes for all software so that the Responsible Entity can verify the values prior to installation on the BES Cyber System to verify the integrity of the software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that when third-party software components are provided by the vendor, the vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses of the third-party software components.

1.2.6. *Coordination of controls for vendor-initiated remote access.*

- During procurement, request vendors specify specific IP addresses, ports, and minimum privileges required to perform remote access services.
- Request vendors use individual user accounts that can be configured to limit access and permissions.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to maintain their IT assets (hardware, software and firmware) connecting to Responsible Entity network with current updates to remediate security vulnerabilities or weaknesses identified by the original OEM or Responsible Entity.
- During procurement, request vendors document their processes for restricting connections from unauthorized personnel. Vendor personnel are not authorized to disclose or share account credentials, passwords or established connections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that for vendor system-to-system connections that may limit the Responsible Entity's capability to authenticate the personnel connecting from the vendor's systems, the vendor will maintain complete and accurate books, user logs, access credential data, records, and other information applicable to connection access activities for a negotiated time period.

Requirement R2

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

Note: Implementation of the plan 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 Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

General Considerations for R2

Implementation of the supply chain cyber security risk management plan(s) 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-013-2. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-2.

Requirement 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.*

General Considerations for R3

In the Requirement R3 review, responsible entities should consider new risks and available mitigation measures, which could come from a variety of sources that include NERC, DHS, and other sources.

Implementation Guidance for R3

Responsible entities use various processes to address this requirement. Below are some examples of approaches to comply with this requirement:

- A team of subject matter experts from across the organization representing appropriate business operations, security architecture, information communications and technology, supply chain, compliance, legal, etc. reviews the supply chain cyber security risk management plan at least once every 15 calendar months to reassess for any changes needed. Sources of information for changes include, but are not limited to:
  - Requirements or guidelines from regulatory agencies
  - Industry best practices and guidance that improve supply chain cyber security risk management controls (e.g. NERC, DOE, DHS, ICS-CERT, Canadian Cyber Incident Response Center (CCIRC), and NIST).
  - Mitigating controls to address new and emerging supply chain-related cyber security concerns and vulnerabilities
  - Internal organizational continuous improvement feedback regarding identified deficiencies, opportunities for improvement, and lessons learned.
- The CIP Senior Manager, or approved delegate, reviews any changes to the supply chain cyber security risk management plan at least once every 15 calendar months. Reviews may be more frequent based on the timing and scope of changes to the supply chain cyber security risk management plan(s). Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.

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 (ESCSWG) - "Cybersecurity Procurement Language for Energy Delivery Systems"