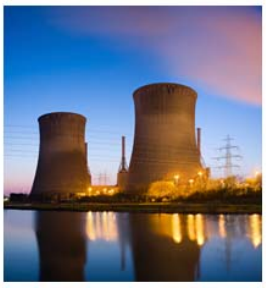
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Guidance and Examples

DRAFT CIP-013-1 – Cyber Security - Supply Chain Risk Management

January 17, 2017

RELIABILITY | ACCOUNTABILITY

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

Introduction

Background

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 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.*

The Commission established a filing deadline of one year from the effective date of Order No. 829, which is September 27, 2017.

The Commission also explains that it "does not require NERC to impose any specific controls nor does the Commission require NERC to propose 'one-size-fits-all' requirements." (P 13)

> *Responsible entities should be required to achieve these four objectives but have the flexibility as to how to reach the objective (i.e., the Reliability Standard should set goals (the "what"), while allowing flexibility in how a responsible entity subject to the Reliability Standard achieves that goal (the "how"))*

Furthermore, FERC clarified the scope of the directives in Order No. 829 by stating (P 21):

> *we reiterate the statement in the NOPR that any action taken by NERC in response to the Commission's directive to address the supply chain-related reliability gap should respect "section 215 jurisdiction by only addressing the obligations of responsible entities" and "not directly impose obligations on suppliers, vendors or other entities that provide products or services to responsible entities."*

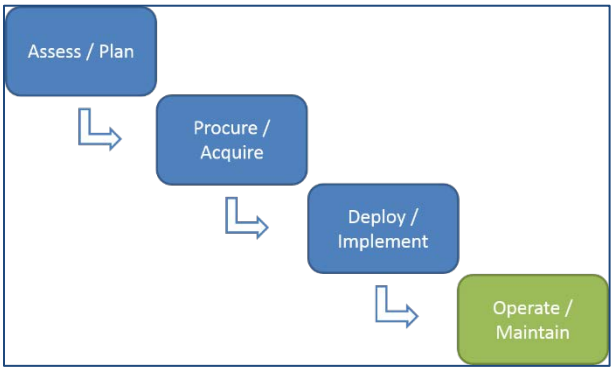
This technical reference provides a summary of the CIP-013-1 framework, which includes a description of the requirements that meet FERC's directives, including each of the objectives; the risk each objective is intended to address; some considerations for implementing the requirements; and examples of controls that responsible entities could use to meet the requirements.

CIP-013-1 Framework

Consistent with the Commission's directives, CIP-013-1 requires that responsible entities address each of the objectives set forth in Order No. 829 by developing and implementing a cyber security risk management plan and documented operating processes to protect against supply chain risks. The proposed standard is forward looking in that it does not require entities to renegotiate currently effective contracts in order to implement their plan.

Collectively, the provisions of Requirement R1 and R2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirements R3 through R5 address controls for software integrity and authenticity and vendor remote access that apply to the operate/maintain phase of the system life cycle. The term *vendors* as used in the standard includes (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Responsible Entities

Proposed CIP-013-1 uses the same applicability as found in other CIP cyber security standards.

Requirement R1

R1. *Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The plan(s) shall address:*

1.1. *The use of controls in BES Cyber System planning and development to:*

1.1.1. *Identify and assess risk(s) during the procurement and deployment of vendor products and services; and*

1.1.2. *Evaluate methods to address identified risk(s).*

1.2. *The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets:*

1.2.1. *Process(es) for notification of vendor security events;*

1.2.2. *Process(es) for notification when vendor employee remote or onsite access should no longer be granted;*

1.2.3. *Process(es) for disclosure of known vulnerabilities;*

1.2.4. *Coordination of response to vendor-related cyber security incidents;*

1.2.5. *Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;*

1.2.6. *Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and*

1.2.7. *Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable.*

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes controls for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (P 45):

(1) Software integrity and authenticity;
(2) Vendor remote access;
(3) Information system planning; and
(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to BES Cyber Systems and, to the extent applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. These cyber systems cover the scope of assets needed to address FERC Order No. 829 directives, which specified that the standards must address supply chain risks to "industrial control system hardware, software, and computing and networking services associated with bulk electric system operations" (P 43).

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P 36) as specified in the Implementation Plan.

To achieve the flexibility needed for supply chain cyber security risk management, responsible entities could use a "risk-based approach" to addressing the objectives. One example of a risk-based cyber security risk management plan is system-based, which describes specific controls for high, medium, and low impact BES Cyber Systems. Another example of a risk-based approach is vendor-based, allowing entities to develop its plan(s) around risk posed by various vendors of its BES Cyber Systems. 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 (P 44)."

Objective: Information System Planning and Procurement

Requirement R1 Part 1.1 addresses Order No. 829 directives for identification and documentation of risks in the planning and development processes related to proposed BES Cyber Systems (P 56). The objective is to ensure entities consider risks and options for mitigating these risks when planning, acquiring, and deploying BES Cyber Systems.

Requirement R1 Part 1.2 addresses Order No. 829 directives for procurement controls to address vendor-related security concepts in future contracts for BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets (P 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of elements contained in the entity's plan related to Part 1.2 is accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs) and in negotiations with vendors. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.

Security Risks in Information System Planning and Procurement

The objective addresses risks identified in Order No. 829 (P 57):

> *The risk that responsible entities could unintentionally plan to procure and install unsecure equipment or software within their information systems, or could unintentionally fail to anticipate security issues that may arise due to their network architecture or during technology and vendor transitions.*

FERC also cited to the BlackEnergy malware campaign that used a zero day vulnerability (previously unknown) to remotely execute malicious code on devices that contain this vulnerability. Steps to "(1) minimize network exposure for all control system devices/subsystems; (2) ensure that devices were not accessible from the internet; (3) place devices behind firewalls; and (4) utilize secure remote access techniques" during system development and planning could mitigate such risk (P 57).

The objective also addresses additional risks identified in Order No. 829 (P 60):

> *the risk that responsible entities could enter into contracts with vendors who pose significant risks to their information systems, as well as the risk that products procured by a responsible entity fail to meet minimum security criteria. In addition, this objective addresses the risk that a compromised vendor would not provide adequate notice and related incident response to responsible entities with whom the vendor is connected.*

Entity Considerations in Meeting the Objective

In implementing Requirement R1, the responsible entity should consider the following:

- 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 reviewed and evaluated during the planning, bidding, evaluation and contracting phases of the procurement process.
- Using periodic review processes 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 or service provider use of third party (e.g., product/personnel certification processes) or independent review methods to verify product and/or service provider security practices.
- Using third parties to conduct security assessments and penetration testing for specific vendors or "cloud based" service providers.
- 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. Consider establishing additional controls based on risk.
- 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.
- Use of procurement controls to aid with vendor risk assessments and mitigation measures for cyber security during the procurement process.

In implementing procurement controls, especially contract terms, responsible entities should be careful not to limit their negotiating ability with vendors through their CIP-013-1 plans. An example of this would be a procurement control that requires specific contract terms. This may have unintended consequences such as significant and unexpected cost increases for the product or service or vendors walking away from contracts.

Responsible entities may use their entire procurement process (e.g. defined requirements, request for proposal, bid evaluation, external vendor assessment tools and data, third party certifications and audit reports, etc.) rather than just contract terms to help them meet the objective and give them flexibility to negotiate contracts with vendors to efficiently mitigate risks.

Obtaining the desired specific cyber security controls in the negotiated contract may not be feasible with each vendor. Baseline controls should be established with the knowledge that every negotiated contract will be different. Factors such as competition, sole source of supply, or supplier's progression will determine the negotiated outcomes of the contract. This variation in contract terms is anticipated and is not considered failure to implement an entity's plan. In the event the vendor is unwilling to engage in the negotiation process for cyber security controls, the entity may explore other sources of supply or mitigating controls to reduce the risk to the BES cyber systems.

Potential Information System Planning Controls

Responsible entities may use various control(s) to address the security risk for this objective. Below are some examples of controls:

1.1. *The use of controls in BES Cyber System planning and development to:*

1.1.1. *Identify and assess risk(s) during the procurement and deployment of vendor products and services; and*

- Responsible Entity can develop plans to identify potential cyber security risks during the information system planning, system development, acquisition and deployment lifecycle processes. The plans can define the required security controls within the lifecycle that address threats, vulnerabilities, adverse impacts and risk to BES Cyber Systems.
- Participation of identified cross-organizational subject matter experts with appropriate representation of business operations, security architecture, information communications and technology, supply chain, compliance, and legal to be included in the planning and acquisition process.
- Identify potential risks based on information systems, system components, and/or information system services / integrators.
- Assess vendors based on their risk management controls. Examples of vendor risk management controls to consider include[1]:
  - Personnel background and screening practices by vendors
  - Training programs and assessments of personnel on cyber security
  - Formal 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
  - Review of 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 their processes
  - Review of certifications and their alignment with recognized industry and regulatory controls
  - Summary of any internal and independent cyber security testing performed on the products to ensure secure and reliable operations. Ask vendors to share third-party/independent product testing results during the request for proposal stage of acquisition process
  - Understand product roadmap to determine vendor support of software patches, firmware updates, replacement parts and ongoing maintenance support
  - Define any critical elements or components that may impact the operations or reliability of BES Cyber Systems

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

- Identify processes and controls for ongoing management of Responsible Entity and vendor's intellectual property ownership and responsibilities, if applicable. This may include use of encryption algorithms for securing software code, data and information, designs, and proprietary processes while at rest or in transit.
- Identify any components of products that are not owned and managed by the vendor that may introduce additional risks, such as use of open source code or third party developers and manufacturers.

- Plan for information systems component end-of-life or discontinuation of product support. Define plans for replacement when support from the developer, vendor, or manufacturer is no longer provided. Provide justification and documented approval for the continued use of system components required to satisfy mission needs and ensure ongoing cyber security protection and reliability. (see NIST SP 800-53 SA-22 – Unsupported System Components)

1.1.2. *Evaluate methods to address identified risk(s).*

- Based on risk assessment, determine mitigating controls that can be applied in procurement and/or operation phase of product or service acquisition and implementation. Examples include:
  - Hardening the information systems and minimizing the attack surface vulnerabilities introduced with vendor products and services.
  - Ensure ongoing support and availability of system components for duration of expected life of products. Define the primary and alternate sources (if any) of components, parts and support services.
  - Controls to ensure system components, parts and support services are only acquired through trusted sources.
  - Identify alternative vendors that may supply critical elements and components, provide support services, or offer equivalent business functional solutions.
  - Review and address other risks in Requirement R1 Part 1.1.1.

Potential Procurement Controls

Responsible entities may use various control(s) to address the security risk for this objective. Below are examples of some controls:

1.2. *The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets:*

- Responsible Entity can define cyber security terms in the procurement request for proposal (RFP) for BES Cyber Systems to ensure the vendor(s) understands the cyber security expectations and implements proper security controls throughout the design, development, testing, manufacturing, delivery, installation, support, and disposition of the product lifecycle. 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). Each Responsible Entity will need to determine the applicability of these sample terms and how such terms may complement other cyber security expectations in a clear and measurable manner.

- During negotiations of procurement contracts, 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 supplier's system component, system integrators, or external service providers.

1.2.1. *Process(es) for notification of vendor security events;*

- Request vendor cooperation to obtain Responsible Entity notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems ("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. Notifications could include information on (i) mitigating controls that may be implemented by Responsible Entity, (ii) availability of patch or corrective components.
- Security Event notifications to the vendor should be sent to designated point of contact as determined by the vendor. Vendor should respond within a defined timeframe with information on (i) mitigating controls that may be implemented by Responsible Entity, (ii) availability of patch or corrective components.

1.2.2. *Process(es) for notification when vendor employee remote or onsite access should no longer be granted;*

- Using contract language, the Responsible Entity can maintain the right in its sole discretion to suspend or terminate remote or onsite access of vendor, or any individual employee of vendor, at any time without further notice for any reason. The vendor and Responsible Entity should define alternative methods that will be implemented in order to continue ongoing operations or services as needed.
- Request vendor cooperation in obtaining Responsible Entity notification of 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.
- If vendor utilizes third parties to perform services to Responsible Entity, request vendor cooperation to obtain Responsible Entity's prior approval and third party adherence to the requirements and access termination rights imposed on the vendor directly.

1.2.3. *Process(es) for disclosure of known vulnerabilities;*

- Review vendor summary documentation of publicly disclosed vulnerabilities in the procured product and the status of the vendor's disposition of those publicly disclosed vulnerabilities.
- Request vendor 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.
- After contract award and for duration of relationship with vendor, request vendor cooperation in obtaining access to summary documentation within a negotiated period of any identified security breaches involving the procured product or its supply chain. Documentation should include a summary

description of the breach, its potential security impact, its root cause, and recommended corrective actions involving the procured product.

1.2.4. *Coordination of response to vendor-related cyber security incidents;*

- Responsible Entity can agree on service level agreements for response to cyber security incidents and commitment from vendor to collaborate with Responsible Entity in implement mitigating controls and product corrections.
- In the event the Responsible Entity identifies a security incident that may or has resulted in an adverse impact to the availability or reliability of BES Cyber Systems, the Responsible Entity will seek vendor cooperation on notification processes, assistance and support requirements from the vendor.
- In the event the vendor identifies a vulnerability that has resulted in a cyber security incident related to the products or services provided to the Responsible Entity, vendor should provide notification to Responsible Entity per contract agreements. The vendor could 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.

1.2.5. *Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;*

- Request access to vendor documentation detailing the vendor patch management program and update process for all system components (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.
- Request 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.
- For duration of the product life cycle, require vendor to provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within a reasonable period. 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.
- Request vendors 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.
- Request vendors 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.
- When third-party components are provided by the vendor, request vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses.

1.2.6. *Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and*

- 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.
- Request vendors 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.
- 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.
- For vendor system-to-system connections that may limit the Responsible Entity's capability to authenticate the personnel connecting from the vendor's systems, request vendors maintain complete and accurate books, user logs, access credential data, records, and other information applicable to connection access activities for a negotiated time period.

1.2.7. *Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable.*

- Request vendors provide Responsible Entity with audit rights that allow the Responsible Entity or designee to audit vendor's security controls, development and manufacturing controls, access to certifications and audit reports, and other relevant information.
- If vendor is not the original manufacturer of the products, require the vendor to certify that replacement parts supplied are made by the original equipment manufacturer and meet the applicable manufacturer data sheet or industry standard.
- For any replacement parts that vary from OEM specifications, request the vendor obtain prior approval by the Responsible Entity before substitution. Consider requiring vendor to provide testing certification or specifications that the replacement parts meet original product requirements.
- Require vendor to use designated or trusted providers for product delivery and services.
- Restrict the use and publication of Responsible Entity information in contracts, e.g., do not allow suppliers to publish your entity name, products or services on their websites or in sales materials.

Requirement R2

R2. *Each Responsible Entity shall review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months, which shall include:*

2.2. *Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and*

2.3. *Obtaining CIP Senior Manager or delegate approval.*

Objective: Review Supply Chain Cyber Security Risk Management Plans

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Order No. 829 also directs that the periodic assessment "ensure that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities" (P. 47). Examples of sources of information that the entity considers include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Entity Considerations in Meeting the Objective

Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review. In the Requirement R2 review, responsible entities must consider new risks and available mitigation measures, which could come from a variety of sources that may include NERC, DHS, and other sources. The requirement also requires the identification of changes made, if any, to the controls based on this review.

CIP-003-6, Requirements R3 and R4 address the identification and delegation process for the CIP Senior Manager for this and the other CIP Standards.

Potential Supply Chain Cyber Security Risk Management Plan Controls

Responsible Entities may use various control(s) to address the security risk for this objective. Below are examples of potential controls:

2.1. *Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and*

- Responsible Entity will maintain a documented supply chain cyber security risk management plan
- Cross-organizational representative subject matter experts from appropriate business operations, security architecture, information communications and technology, supply chain, compliance, legal, etc. should collaboratively develop and be responsible to review the supply chain cyber security risk management plan at least once every 15 calendar months to reassess for any changes needed. Considerations for changes may include:
  - Requirements or guidelines from regulatory agencies
  - Industry best practices and guidance that improve cyber security risk management controls (e.g. NERC, DOE, DHS, ICS-CERT, Canadian Cyber Incident Response Center (CCIRC), 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. Examples may include changes to contract terms based on market maturity, capabilities, and cyber security advancements.

- Development of communications or training material to ensure any organizational areas affected by revisions to the supply chain cyber security risk management plan(s) are informed.

2.2. *Obtaining CIP Senior Manager or delegate approval.*

- 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). Entities may incorporate the review into their annual CIP-003 review.
- 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.

Requirement R3

R3. *Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems:*

- **3.1.** *Operating System(s);*
- **3.2.** *Firmware;*
- **3.3.** *Commercially available or open-source application software; and*
- **3.4.** *Patches, updates, and upgrades to 3.1 through 3.3.*

Objective: Software Integrity and Authenticity

The proposed requirement addresses Order No. 829 directives for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Security Risks from Compromised Software

The Objective addresses the risk that an attacker could exploit legitimate vendor software delivery or patch management processes to deliver compromised software updates or patches to a BES Cyber System. [2] In Order No. 829, FERC provides additional context to this risk by stating that adequate authenticity and integrity controls could prevent malware campaigns or "Watering Hole" attacks that target the exploitation of vulnerable patch management processes.[3]

Entity Considerations in Meeting the Objective

In implementing Requirement R3, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used by their vendors to deliver software and appropriate control(s) that will verify the integrity and authenticity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software integrity and authenticity can be verified through those processes.
- Integration of procurement controls from the responsible entity's supply chain cyber security risk management plan as identified in Requirement R1. During procurement of new systems, such as systems with preinstalled software, 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.
- Coordination of the responsible entity's integrity and authenticity control(s) with other cyber security policies and controls, including change management and patching processes, procurement controls, and incident response plans.
- Use of a secure central software repository after software authenticity and integrity have been validated, so that authenticity and integrity checks do not need to be performed before each installation.

[2] *Id.* at P 48 and P 49. "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" *(P 49).* FERC explains that the objective applies to all software (P 48).
[3] *Id.*

- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the responsible entity.

Potential Software Integrity Controls

Responsible entities may use various control(s) to address the security risk for this objective. Below are examples of potential controls:

- Prior to installing software or placing software into operation on a BES Cyber System, verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require vendors to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the vendor.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Potential Software Authenticity Controls

Responsible entities may use various control(s) to address the security risk for this objective. Below are examples of potential controls:

- Obtain software from an authenticated source before installation.
- Prior to installing software or placing software into operation on a BES Cyber System, verify that the software has been digitally signed and validate the signature to ensure that the software is authentic.
- Use public key infrastructure (PKI) with encryption to ensure that the software is authentic by enabling only intended recipients to decrypt the software.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping).

Requirement R4

R4. Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

4.1. Authorization of remote access by the Responsible Entity;

4.2. Logging and monitoring of remote access sessions to detect unauthorized activity; and

4.3. Disabling or otherwise responding to unauthorized activity during remote access sessions.

Objective: Vendor Remote Access to BES Cyber Systems

The proposed requirement addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective of the Requirement is to mitigate potential risks of a compromise at a vendor from traversing over an unmonitored remote access connection.

The objective of Requirement R4 Part 4.3 is for entities to have the ability to rapidly disable remote access sessions in the event of a system breach as specified in Order No. 829 (P 52).

Security Risk Related to Vendor Remote Access

The objective addresses risks identified in Order No. 829:

> *the threat that vendor credentials could be stolen and used to access a BES Cyber System without the responsible entity's knowledge, as well as the threat that a compromise at a trusted vendor could traverse over an unmonitored connection into a responsible entity's BES Cyber System.*[4]

Entity Considerations in Meeting the Objective

Requirement R4 Part 4.1 requires responsible entities to implement a control(s) to restrict vendor access, which includes access by a person or a machine. The control(s) used by a responsible entity may vary depending on entity-specific factors and existing cyber security policies (i.e. different entities grant varying levels and amounts of vendor remote access depending on entity needs.)

In addition to authorizing remote access, Requirement R4 requires the implementation of a control(s) to monitor vendor access (Part 4.2). Therefore, if a vendor is allowed to access BES Cyber Systems, then the responsible entity is required to monitor this access. This control(s) will address the Commission's concern that the responsible entity may not have the level of visibility over the remote access system-to-system session on the BES Cyber Systems, which could allow malicious intrusion attempts to take place.

Requirement R4 Part 4.3 addresses the detection of unauthorized (i.e., inappropriate) activity as well as the response to the detection of such activity, while allowing the responsible entity flexibility in the control(s) it uses to meet this part of the security objective.

It is important to recognize that these new requirements may be partially addressed by the responsible entity's existing remote access controls used to comply with approved CIP Standards. In implementing Requirement R4, the responsible entity should consider their existing CIP cyber security policies and controls.

[4] 156 FERC ¶ 61,050 at P 52.

For Requirement R4 Part 4.1, an entity may already have some authorization controls in place that will support meeting this objective.[5] If these controls do not fully cover vendor-initiated Interactive Remote Access and system-to-system remote access with a vendor(s), additional remote access controls are needed to meet the objective. For example, if an entity allows vendor remote access only during specific circumstances, such as response to system problems, the entity put other controls in place to disable vendor remote access at other times. Other entities may find that vendor remote access is required at all times and may use other controls as discussed below to achieve the objective. For example, the entity could employ operator-based controls that use various identification methods to control vendor remote access pathways into BES Cyber Systems.

For Requirement R4 Part 4.2, an entity may have monitoring controls in place for some BES Cyber Systems, however the controls may not necessarily address remote access session monitoring and alerting.[6] These existing monitoring controls could be enhanced to meet the objective. Entities should consider:

- Available capabilities and technologies for monitoring session activity with a vendor
- Setting up processes and parameters to monitor and log remote access login attempts to detect unauthorized remote access
- Development of procurement technical specifications for vendor remote access to support monitoring vendor remote access traffic during remote sessions

Entities may find it appropriate to modify their existing controls associated alert and response processes for Requirement R4 Part 4.3 including the threshold for alerting, persons alerted, as well as the timelines for alerting and responding. Entities may also find it appropriate to modify their existing controls and processes associated with CIP-008-5 - Cyber Incident Response Plan. Other considerations:

- Entity determination of appropriate response to unauthorized access from personnel, technology, and risk standpoints
- Thresholds for alerting, persons alerted, and the timelines for alerting and responding to unauthorized activity in order ensure reliable BES operations
- Availability and reliability of methods to prevent vendor remote access or disable vendor remote access sessions if unauthorized or illegitimate access is detected.

Potential Remote Access Controls

Responsible Entities may use various control(s) to address the security risk for this objective. Below are examples of potential controls:

<u>For Requirement R4 Part 4.1 (Authorization Controls):</u>

- Use an operator controlled, time limited (e.g., lock out, tag out) process for vendor remote access. Example approaches may include:
  - For user initiated sessions, use token authentication by authorized personnel. Token activation is for a specific timeframe or specific location. For machine-to-machine sessions, use encryption and multi-factor authentication that changes on a determined timeframe.

[5] For example, CIP-004-6 - Personnel and Training, which covers training and personnel risk assessment requirements, and CIP-007-6 Requirement 5 – System Access Control, which covers account access controls.

[6] CIP-005-5 Requirement R1.5 covers detection of malicious communications for medium and high BES Cyber Systems in Control Centers, and CIP-007-6 Requirements 4.1 and 4.2 covers logging of access and detection of failed access attempts.

- Designate specific timeframe access for the exchange of information. The responsible entity is responsible for ensuring access is terminated at the conclusion of the timeframe.
- Terminate access upon notification the underlying purpose has ended.
- Consider requiring vendors to specifically request remote access in order to support operator controlled and time limited access.

For Requirement R4 Part 4.2 (Logging and Monitoring Controls):

- Set up logging and monitoring parameters on key attributes and thresholds as appropriate, such as number of failed log-in attempts.
- Log and monitor vendor remote access sessions and review logs for abnormal behavior. Have a method for terminating suspicious sessions.
- Consider extended use of jump hosts for access to protected networks (e.g. specific jump hosts dedicated to vendor remote access).
- Use monitoring and control mechanisms and processes at the boundary between the responsible entity and vendors (e.g. application level firewalls or intrusion detection/prevention systems).
- Change default parameters for authentication mechanisms (e.g., passwords) or access/network protocols prior to installing Cyber Assets.

For Requirement R4 Part 4.3 (Disable Access and Entity Response Controls):

- Set up alerting parameters and thresholds on key attributes as appropriate for the entity (e.g., number of failed login attempts or detection of inappropriate activities).
- Set up alerting and response processes so that inappropriate vendor remote access sessions may be disabled or otherwise responded to in a timely manner.

Requirement R5

R5. *Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:*

5.1. *Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and*

5.2. *Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s).*

Objective: Software and Vendor Remote Access Risk Mitigation in Low Impact BES Cyber Systems

The proposed requirement addresses Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems. (P. 48 and P. 51).

Security Risks

Preceding sections discuss the related risks as identified in Order No. 829. Requirement R5 is intended to address these risks as they apply to low impact BES Cyber Systems. Responsible Entities have flexibility to use an approach for low impact BES Cyber Systems that is different from the approach used for medium and high impact BES Cyber Systems.

Entity Considerations for Meeting the Objective

In implementing Requirement R5, the responsible entity should consider the following:

- Considerations and controls for addressing software risks and vendor remote access risks to high and medium impact BES Cyber Systems discussed above that the entity determines are also applicable to its low impact BES Cyber Systems.
- Entity processes for addressing software risks and vendor remote access risks per Requirements R3 and R4. Consider whether to include low impact BES Cyber Systems in these processes, or alternatively develop a separate cyber security policy or process(es) to address low impact BES Cyber Systems.
- Existing CIP cyber security policies and controls that can be included or referenced in a cyber security policy to meet the objective. For example, some electronic access controls established by an entity for low impact BES Cyber Systems pursuant to approved CIP-003 requirements may be part of the cyber security policy specified in Requirement R5 for controlling vendor-initiated remote access, including system-to-system remote access with vendor(s).
- Asset management factors applicable to the entity. Entities can develop its cyber security policies either by individual asset or by groups of assets. As noted in the rationale section of proposed CIP-013-1, an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

Potential Controls for Cyber Security Policies to Meet the Objective

Responsible entities may use various control(s) to address the security risks for this objective. Below are examples of potential controls that an entity could include in its cyber security policy or process(es):

- Policies, procedures, and/or checklists for personnel to check that software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Policies, procedures, and/or checklists that support obtaining software from trustworthy sources.
- Policies for using trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)
- Policies, procedures, and/or checklists for applying other controls discussed above that address software risks and vendor remote access.

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”