Technical Reference [Draft]

DRAFT CIP-013-1 – Cyber Security - Supply Chain Management
November 2, 2016

Background

On July 21, 2016, the Federal Energy Regulatory Commission ("FERC" or "the Commission") issued Order No. 829 which directed the North American Electric Reliability Corporation ("NERC") to "develop a forward-looking, objective-driven Reliability Standard that provides security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations.[1] The Commission explains that a forward-looking "Reliability Standard should not dictate the abrogation or re-negotiation of currently-effective contracts with vendors, suppliers or other entities."[2]

Specifically, the Commission directs that the Reliability Standard require responsible entities to develop a plan that includes controls that address the following objectives:[3]

1. Software Integrity and Authenticity;
2. Vendor Remote Access to BES Cyber Systems;
3. Information System Planning and Procurement; and
4. Vendor Risk Management and Procurement Controls.

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."[4] The Commission elaborated that:[5]

> *The flexibility inherent in our directive should account for, among other things, differences in the needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies and risks. For example, the new or modified Reliability Standard may allow a responsible entity to meet the security objectives discussed below by having a plan to apply different controls based on the criticality of different assets.*
>
> *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*

[1] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829 156 FERC ¶ 61,050 at P 4 (July 21, 2016) (hereafter "Order No. 829"). The Commission also explains "the Reliability Standard should require the responsible entity's CIP Senior Manager to review and approve the controls adopted to meet the specific security objectives identified in the Reliability Standard at least every 15 months." This directive is addressed in CIP-013-1, Requirement 2, but is not discussed here as no specific controls are associated with implementing this directive.
[2] *Id.* at P 36.
[3] FERC also provided NERC the opportunity to propose equally efficient and effective means to meet the objectives outside the context of a Standard.
[4] *Id.* at P 13.
[5] *Id.* at P 44, 45.

> *allowing flexibility in how a responsible entity subject to the Reliability Standard achieves that goal (the "how"))*

FERC further stated that: [6]

> *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."*

The above passages help provide the context in which CIP-013-1 is drafted. The draft standard does not put direct obligations on third-parties and gives responsible entities the flexibility to address each of the security objectives in different ways based on the risk to the system and/or the risk created by the vendor. This flexibility is focused on the "what" or the security objective and not the "how" or the specific security controls used by each responsible entity. Flexibility is important to meet the Commission's expectation that the standards development process will consider establishing "provisions addressing compliance obligations in a manner that avoids shifting liability from a vendor for its mistakes to a responsible entity."[7] Also, the draft CIP-013-1 standard is forward-looking as discussed below. In Order No. 829, the Commission stated the Reliability Standard "should not dictate the abrogation or re-negotiation of currently-effective contracts with vendors, suppliers or other entities."[8]

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

This draft version of the reference document is intended as a starting point for development of Reliability Standard requirements, standard Guidelines and Technical Basis, and Implementation Guidance.[9] Many of the considerations and potential controls presented here require additional refinement and input by the various stakeholders.

CIP-013-1 Framework

Consistent with the Commission's directives, CIP-013-1 requires that responsible entities develop and implement a plan that addresses each of the objectives set forth in Order No. 829 without mandating controls in the standard. The proposed standard is forward looking in that it does not require entities to renegotiate currently-effective contracts in order to implement their plan.

---

[6] *Id.* at P. 21.
[7] *Id.* at P 89.
[8] *Id.* at P 36.
[9] See NERC Compliance Guidance Policy for a discussion of Implementation Guidance.
http://www.nerc.com/pa/comp/Resources/ResourcesDL/Compliance_Guidance_Policy_FINAL_Board_Accepted_Nov_5_2015.pdf

Responsible Entities

The initial draft standard uses the same applicability as found in other CIP standards.

Requirements R1 and R2

The Commission recognized stakeholder concerns expressed on how a supply chain Reliability Standard could impact vendor relationships. The Commission explained that it did not expect for a revised or new Reliability Standard to "impose obligations directly on vendors . . . [and responsible] entities will not be responsible for vendor errors beyond the scope of the controls implemented to comply with the Reliability Standards."[10] Also, the forward-looking nature of the Reliability Standard "should not dictate the abrogation or re-negotiation of currently-effective contracts with vendors, suppliers or other entities."[11]

The Reliability Standard should "require responsible entities to develop a plan to meet the four objectives, or some equally efficient and effective means to meet these objectives, while providing flexibility to responsible entities as to how to meet those objectives."[12] In addition, the Commission states that "our directive is meant to enhance bulk electric system cybersecurity by addressing the gap in the CIP Reliability Standards."

In summary, the new Reliability Standard must require a plan that is (1) focused on responsible entity obligations, (2) forward-looking, (3) flexible, and (4) addresses gaps in the CIP Standards. These goals are included in Requirements 1 and 2 of CIP-013-1.

Requirement R1 of draft CIP-013-1:

> **R1.** Each Responsible Entity shall develop one or more documented supply chain cybersecurity risk management plan(s) that set forth the controls used to collectively address the following supply chain cybersecurity objectives for BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Requirement R1 requires responsible entities to develop one or more documented supply chain cybersecurity risk management plan(s) that must address the Commission objectives, which are contained within the parts and subparts to this requirement and are described in detail below. For each of the objectives, the potential gaps in the CIP Standards are defined and addressed subsequently.

BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets are the focus of R1 because they include "industrial control system hardware, software, and computing and networking services associated with bulk electric system operations," which the Commission acknowledges in Order No. 829 as the class of assets that should be protected.[13]

[10] 156 FERC ¶ 61,050 at P 88.
[11] *Id.* at P 36.
[12] *Id*. at P 13.
[13] *See e.g.*, 156 FERC ¶ 61,050 PP 24, 34, 48, and 52.

To achieve the flexibility needed for supply chain cybersecurity risk management, responsible entities could use a "risk-based approach" to addressing the objectives. The risk-based approach may be system-based with specific controls for high, medium, and low impact BES Cyber Systems or it could be vendor-based, allowing entities to develop its plan 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."[14]

Requirement R2 of draft CIP-013-1:

> **R2.** Each Responsible Entity shall implement its supply chain cybersecurity risk management plan(s) specified in Requirement R1. Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts.

Requirement R2 addresses implementation of the R1 plan(s). A responsible entity implements its supply chain cybersecurity risk management plan by putting selected controls in place to address identified risks as specified in the plan. The controls could include procurement controls, entity risk-management controls, or a combination of both types of controls. A responsible entity may need to put entity risk-management controls in place that are within the responsible entity's control and do not rely on actions from vendors in some cases, such as when an existing contract is in place that does not contain enhanced provisions.

Requirement R1 Objectives

Objective 1: Software Integrity and Authenticity

For objective 1, the Commission states the existing CIP Reliability Standards:[15]

> Do not require responsible entities to verify the identity of the software publisher for all software and patches that are intended for use on their BES Cyber Systems or to verify the integrity of the software and patches before they are installed in the BES Cyber System environment. . .
>
> Do not provide sufficient protection against attacks that compromise software and software patch integrity and authenticity. . .
>
> Do not require the authorizer to first verify the authenticity of a patch. . .
>
> Have likely insufficient protection as many malware variants are programmed to execute only after the system is rebooted several times. . .
> [Do] not require the use of these techniques [such as patches should be approved or certified by another source before being assessed and applied]. Implementing controls that verify integrity and authenticity of software and its publishers may help mitigate security gaps listed above.

[14] *Id.* at 44.
[15] *Id.* at PP 72-75.

Specifically, the Commission requires that the standard:

> Address verification of: (1) the identity of the software publisher for all software and patches that are intended for use on BES Cyber Systems; and (2) the integrity of the software and patches before they are installed in the BES Cyber System environment.

Objective 1 Security Risk

Objective 1 should address the risk that "an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System." [16] The Commission provides additional context to this risk by stating that adequate authenticity and integrity controls will prevent malware campaigns or "Watering Hole" attacks that target the exploitation of vulnerable patch management processes.[17]

Requirements Addressing the Objective 1 Security Risk

Requirement R1 Part 1.1 of CIP-013-1 requires that the supply chain cybersecurity risk management plan(s) address the Objective 1 security risk and Commission directives. The following discussion describes the elements in Requirement R1 Part 1.1, considerations for responsible entities implementing the elements, and possible approaches to implementation.

Requirement R1 Part 1.1:

1.1 Software integrity and authenticity controls that address risks from compromised software and firmware. The controls shall provide for verification of the following prior to installation:

1.1.1. The identity of the publisher for software and firmware, and any upgrades and patches to software and firmware;

1.1.2. The integrity of software and firmware upgrades and patches.

Subpart 1.1.1 requires responsible entities to develop control(s) to verify the identity of the software publishers for patches before installing them on BES Cyber Systems. This subpart meets the Commission's authenticity requirement because control(s) that verify the software publisher ensure the patch is from the vendor and not an attacker who has compromised a vendor's patch delivery mechanism such as a website. The control(s) used by a responsible entity may vary. For example, the supplier may provide digital signatures with the files to validate authenticity. Some of the control options will vary based on the supplier's practices or capabilities. Flexibility is given here to account for different situations and circumstances.

Subpart 1.1.2 requires responsible entities to develop control(s) to verify the integrity of the patches before installing them on BES Cyber Systems. This subpart meets the Commission's integrity requirement. Verifying the integrity of patches will ensure that the software has not been altered in transit to the responsible entity from the vendor. Again, as aforementioned, the control(s) used by a responsible entity

[16] *Id.* at P 49.
[17] *Id.*

may vary. In this case, there may be checksums or hash totals that can be validated by both parties to ensure the files have not been altered and the integrity of the files have not been maliciously impacted prior to implementation. To reiterate, some of the control options will vary based on the supplier's practices or capabilities. Flexibility is suggested here to account for different situations and circumstances allowing responsible entities to determine the best methods to accomplish the security objectives.

It is also important to recognize that these new requirements may already be addressed by the responsible entity's existing patch management process used to comply with the existing CIP Standards. To avoid unnecessary administrative duplication, entities should closely coordinate addressing part 1.1 with their existing CIP policies and controls. In implementing R1, part 1.1, the responsible entity should consider their existing CIP cybersecurity policies and controls as well as the following:

- Mechanisms used by their vendors to deliver patches and appropriate control(s) that will verify the authenticity and integrity of the patches that are delivered through these mechanisms
- Existing and emerging tools and technologies for authentication and integrity verification
- Use of procurement controls such as the use of common control(s) for all vendors and/or control(s) tailored to specific vendors or vendor subsets and contract terms that specify software authentication and integrity verification processes used
- During procurement of new systems, ask vendors to describe the processes they use for delivering patches and the methods they use to verify authenticity and integrity of these patches
- Coordination of the responsible entity's integrity and authenticity control(s) with other cybersecurity polies and controls, including change management and patching processes, procurement controls, incident response activities, recovery and response plans

The above considerations are examples of what could be included in the Guidelines and Technical Basis for CIP-013-1 for Requirement R1, part 1.1.

Potential Software Integrity and Authenticity Controls

Responsible entities may use various control(s) to address the security risk for this objective. Below are a few possible controls, which could be further explored in implementation guidance:

- Ensure patches are from the original source before installation
- Implement server side encryption keys that may be validated and regularly tested
- Prior to installing a patch on a BES Cyber System, verify that the patch has been digitally signed to ensure that the software is genuine and valid
- Use of third party certificates to validate the identity of the vendor
- Obtain digital signatures and software directly from the developer
- Require vendors to provide fingerprints of checksums (e.g., a cipher hash) for all patches and verify the checksum prior to installing the patch on a BES Cyber System to verify the integrity of the patch. Use a different method for receiving the hash and the patch from the vendor to ensure the authenticity of the patch.

Objective 2: Vendor Remote Access to BES Cyber Systems

For objective 2, the Commission states that the existing CIP Reliability Standards:[18]

> Do not require remote access session logging for machine-to-machine remote access, nor do they address the ability to monitor or close unsafe remote connections for both vendor Interactive Remote Access and vendor machine-to-machine remote access. . .
>
> Do not adequately address access restrictions for vendors. For example, while Reliability Standard CIP-004-6, Requirements R4 and R5 provide controls that must be applied to vendors such as restricting access to individuals 'based on need,' these Requirements do not include post-authorization logging or control of remote access. . .
>
> Do not require a responsible entity to monitor data traffic that traverses remote communication to their BES Cyber Systems. . .
>
> Do not apply to vendor machine-to-machine remote access. . . . A machine-to-machine remote communication may access a BES Cyber System without any access credentials, over an unencrypted channel, and without going through an Intermediate System. . .
>
> [Do] not address the risks posed by inappropriate activity that could occur during a remote communication. The lack of a requirement addressing the detection of inappropriate activity represents a risk because the responsible entity may not be aware if an authorized user is performing inappropriate activity on a BES Cyber Asset via a remote connection.

The Commission concluded that objective 2:

> Must address responsible entities' logging and controlling all third-party (i.e., vendor) initiated remote access sessions. This objective covers both user-initiated and machine-to-machine vendor remote access.

Objective 2 Security Risk

Objective 2 should address:

> 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.[19]

Requirements Addressing the Objective 2 Security Risk

Requirement R1 Part 1.2 of CIP-013-1 requires that the supply chain cybersecurity risk management plan(s) address the Objective 2 security risk and Commission requirements. The following discussion

[18] *Id.* at PP 76-80.
[19] 156 FERC ¶ 61,050 at P 52.

describes the Objective 2 requirements, considerations for responsible entities implementing the requirements, and possible approaches to implementation of these requirements.

Requirement R1 Part 1.2:

1.2 Remote access controls to address risks from compromised third-party access credentials and risks of a compromise at a vendor or service provider from traversing over an unmonitored remote access connection. The controls shall provide for:

1.2.1 Controlling third-party initiated remote access, including machine-to-machine remote access;

1.2.2 Monitoring third-party remote access, including machine-to-machine remote access; and

1.2.3 Detecting and responding to unauthorized third-party remote access activity.

Subpart 1.2.1 requires responsible entities to implement a control(s) to restrict third-party access, which includes access by a person or a machine. The control(s) used by a responsible entity may vary. For example, the vendor may be given limited access consistent with the responsible entity's existing access management policies and programs, which may include preventing all third-party access. Flexibility is given here to account for different situations and circumstances.

In addition to controlling remote access, subpart 1.2.2 requires the implementation of a control(s) to monitor third-party access. 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 machine-to-machine session on the BES Cyber Systems, during which malicious intrusion attempts could take place. Monitoring control(s) are used rather than "logging" because logging is a specific control or the "how" a responsible entity could meet this requirement. As a result, logging remote access sessions could be used as a control to meet this part of the security objective.

Subpart 1.2.3 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 also important to recognize that these new requirements may already be addressed by the responsible entity's existing remote access controls used to comply with the existing CIP Standards. To avoid unnecessary administrative duplication, entities should closely coordinate addressing part 1.2 with their existing CIP policies and controls. In implementing Requirement R1 Part 1.2, the responsible entity should consider their existing CIP cybersecurity policies and controls as well as the following:

- The feasibility of monitoring remote access sessions as well as detection and response to unauthorized access from personnel and technology standpoints
- Operator controlled pathways into the system that may use various identification methods

- Setting up logging, alerting, and monitoring parameters to monitor and alert remote access login attempts to detect unauthorized and illegitimate remote access
- Development of monitoring standards and technical specifications to monitor traffic during remote sessions
- Methods to prevent third-party remote access or disable third-party remote access sessions if unauthorized or illegitimate access is detected
- Use of procurement controls to aid with remote access controls. For example, contract terms may be negotiated to include: designation of vendor employees who will have access to the Entity system, requiring vendors to have specific software/ security in place if using own computers to remote in, and incorporation of DOE Cybersecurity provisions for access, logging, malware and vulnerability management where applicable.

The above considerations are examples of what could be included in the Guidelines and Technical Basis for CIP-013-1 for Requirement R1 Part 1.2.

Potential Remote Access Controls

Responsible entities may use various control(s) to address the security risk for this objective. Below are a few possible controls, which could be further explored in implementation guidance:

- Use an operator controlled, time limited (e.g., lock out, tag out) process for third-party remote access. Example approaches may include:
    - For user initiated sessions, use token authentication by specifically identified authorized personnel who have had background checks going back 7 years, and token is activated for specific timeframe, or can only be used in a specific location. For machine-to-machine sessions, use encryption and multi-factor authentication that is changed out on specifically determined timeframe.
    - The designation of specific timeframe access that will be needed for the exchange of information. The responsible entity will then be responsible for ensuring access is terminated on the date as provided. And termination of access immediately upon notification the underlying business purpose has ended.
    - Remote access must specifically be requested and granted to allow for operator controlled and time limited access
- Logging third-party remote access sessions, reviewing the logs for abnormal behavior, and a method for terminating suspicious sessions
- Set up alert and monitoring parameters on key attributes and thresholds such as number of failed log-in attempts
- Use of jump hosts required for access to protected networks
- Use of monitoring and control mechanisms and processes at the boundary between the responsible entity and vendors
- Changing default authentication mechanisms (e.g., passwords) prior to installing Cyber Assets
- Monitoring supply chain compromises for lessons learned and adapting your control(s) as appropriate
- Contract terms to help ensure the vendor follows your access control(s)

Objective 3: Information System Planning and Procurement

For objective 3, the Commission states the existing CIP Reliability Standards:[20]

> Do not address information system planning. Recent cybersecurity incidents have made it apparent that overall system planning is as important to overall BES Cyber System security and reliability as any other component of security architecture. . .
>
> Do not provide a framework for maintaining ongoing awareness of information security, vulnerabilities, and threats to support . . . organization risk management decisions; nor do they address the concept of integrating continuous improvement of organizational security posture with supply chain risk management as recommended by NIST SP 800-161. . .
>
> Do not provide for procurement controls for industrial control system hardware, software, and computing and networking services.

The Commission concluded that Objective 3:

> Must address how a responsible entity will include security considerations as part of its information system planning and system development lifecycle processes. As part of this objective, the new or modified Reliability Standard must address a responsible entity's CIP Senior Manager's (or delegate's) identification and documentation of the risks of proposed information system planning and system development actions.

Objective 3 Security Risk

Objective 3 should address:

> 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.[21]

The Commission 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.[22]

Requirements Addressing the Objective 3 Security Risk

Requirement R1 Part 1.3 of CIP-013-1 requires that the supply chain cybersecurity risk management plan(s) address the Objective 3 security risk and the Commission requirement to include security considerations as part of information system planning and system development. Requirement R3

[20] *Id.* at PP 81-83.
[21] *Id*. at P 57.
[22] *Id*.

discussed below, addresses the continuous improvement aspect related to the CIP Senior Manager or delegate(s).

Also, Requirement R1 Part 1.3 does not directly address procurement controls since this is the focus of Objective 4, discussed below. Although, procurement controls are potential control(s) that are mentioned for consideration in each of the objectives because including security in procurement processes can help responsible entities meet their security objectives. More discussion on procurement controls is below, under Objective 4.

The following discussion describes the elements of Requirement R1 Part 1.3, considerations for responsible entities implementing Part 1.3, and possible approaches to implementation.

Requirement R1 Part 1.3:

1.3 Information system planning controls to address the consideration of cyber security supply chain risks in information system development. The controls shall:

1.3.1 Assess risks that may be introduced by a third-party;

1.3.2 Evaluate methods to address identified third-party risk.

1.3.3 [*Should the standard address implementation here? Or should implementation be covered by Requirement R2?*]

Part 1.3.1 is intended to address the Commission's directive that "a responsible entity will include security considerations as part of its information system planning and system development lifecycle processes."[23] As part of this objective, the new or modified Reliability Standard must address a responsible entity's… identification and documentation of the risks of proposed information system planning and system development actions."[24] Part 1.3.1 requires responsible entities to incorporate a control(s) to assess the cybersecurity risk that can be introduced by a third-party, Measure 1 (M1) requires documentation of the control(s), and Measure 2 requires evidence or documentations that the risk was assessed. Risk assessment requires the responsible entity to consider threats, vulnerabilities, and potential consequences of an attack on their systems and operations.

Part 1.3.2 is meant to require responsible entities to consider "available options for hardening the responsible entity's information system and minimizing the attack surface."[25] Based on the Part 1.3.1 risk assessments, responsible entities must use control(s) to mitigate the risk under Part 1.3.2. Risk mitigation will harden the responsible entity's information system to minimize the attack surface.

In implementing Requirement R1 Part 1.3, the responsible entity should consider the following:

- Risk(s) to the existing responsible entity's infrastructure

[23] *Id*. at P 56.
[24] *Id*.
[25] 156 FERC ¶ 61,050 at P 56.

- Criticality of a specific vendor from which information system development and procurement occurs
- Vendor security processes and related procedures, including: system architecture, change control processes, remote access requirements, and security notification processes
- Known system vulnerabilities; known threat techniques, tactics, and procedures; and related mitigation measures
- Methods to minimize network exposure, e.g., prevent internet accessibility, use of firewalls, and use of secure remote access techniques
- Use of procurement controls to aid with vendor risk assessments and mitigation measures

The above considerations are examples of what could be included in the Guidelines and Technical Basis for CIP-013-1 for R1, part 1.3.

Potential Information System Planning Controls

Responsible entities may use various control(s) to address the security risk for this objective. Below are a few possible controls, which could be further explored in implementation guidance:

- Establish an assessment process that requires the entity to assess cybersecurity risk that may be introduced by a third-party. Entities could have a defined set of criteria or threshold that, if a new system meets, initiates a more in-depth security architecture review process. The criteria's aim is to ensure an in-depth technical review of high-risk changes to architecture and systems.
- In the design and implementation of new systems: develop layered protections; establish sound security policy, architecture, and controls; incorporate security requirements; and reduce risk to acceptable levels to inform risk management decisions
- "Controls to address unsupported system components, recommending the replacement of information and communication technology components when support is no longer available, or the justification and approval of a unsupported system component to meet specific business needs"[26]
- For high risk scenarios:
    - Gather necessary vendor information including security processes and related procedures. Document identified security vulnerabilities.
    - Perform a threat analysis and security review of software and hardware systems to detect and correct software and hardware errors that could adversely impact the existing computing environment.
    - Involve IT security architects, supply chain, legal and appropriate business units in all planning phases for development and implementation of key systems and infrastructure.
    - Consider engaging specific vendors for penetration testing of vendor system vulnerabilities.
    - Consider a third party security assessment for "cloud based" services including website and online access and storage reviews.
    - Consider establishing a corporate approval process for all contracts for high risk scenarios.

[26] *Id*. at P 58.

  - Consider requiring that appropriate information technology security is included within change management processes and is required to sign-off on changes made to CIP related systems.
  - Consider reviewing standard cyber security contract provisions are reviewed twice annually to ensure terms include the latest and most current standards.
  - Consider including information security requirements within the contract for information systems and services.
- Procurement controls, including requiring vendors to identify methods and processes used to minimize vulnerabilities as well as security best practices used by the vendor in system development

Objective 4: Vendor Risk Management and Procurement Controls

The existing CIP Reliability Standards to not require procurement controls. As a result, the Commission states that Objective 4:

> Must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations.

The Commission also indicated that the controls associated with Objective 4 must address:

> (1) vendor security event notification processes; (2) vendor personnel termination notification for employees with access to remote and onsite systems; (3) product/services vulnerability disclosures, such as accounts that are able to bypass authentication or the presence of hardcoded passwords; (4) coordinated incident response activities; and (5) other related aspects of procurement.

The Commission also expects NERC to consider the implementation of provisions to assist a responsible entity in obtaining the necessary information from its vendors to minimize potential disruptions from vendor-related security events.

Objective 4 Security Risk

Objective 4 should address:

> 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.[27]

[27] *Id*. at P 60.

Requirements Addressing the Objective 4 Risk

Requirement R1 Part 1.4 of CIP-013-1 requires that the supply chain cybersecurity risk management plan(s) address the Objective 4 security risk and Commission requirements. The following discussion describes the part 1.4 requirements, considerations for responsible entities implementing the requirements, and possible approaches to implementation of these requirements.

Requirement R1 Part 1.4:

1.4 Procurement controls to identify and verify security controls used by vendors or service providers in delivering products or services. These procurement controls should address the following security controls used by the vendor or service provider:

- **1.4.1** Notification of security events that may impact the Responsible Entity;
- **1.4.2** Notification when employees should no longer be granted remote or onsite access due to employment termination, reassignment, or transfer;
- **1.4.3** Disclosure of known vulnerabilities that may impact the Responsible Entity; and
- **1.4.4** Coordination of response to vendor-related cyber security incidents affecting the Responsible Entity.

Part 1.4 requires responsible entities to use procurement controls to identify and verify the security controls used by their vendors and service providers, which must at least address the four topics the Commission provided in Order No. 829.

As noted under Objective 3, each of the above objectives includes the consideration of procurement controls, which responsible entities should consider under this objective. In implementing procurement controls, especially contract terms, responsible entities must 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. If the responsible entity implements this control under CIP-013-1, they must be prepared to demonstrate that the contract term was used in the contract to auditors. 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 should also carefully consider the consequences of a vendor breaching their contract term(s) either intentionally or unintentionally and whether these terms were considered material enough to allow the responsible entity to gain damages and restitution. Responsible entities should consider using their entire procurement process, e.g., request for proposal requirements, rather than just contract terms to help them meet Objective 4 and give them flexibility to negotiate contracts with vendors to efficiently mitigate risks. However, requiring specific contract terms may also be a viable option for responsible entities.

Also, “vendor risk management” was left out of part 1.4 because it was unnecessary and confusing as the entire supply chain cybersecurity risk management standard (CIP-013-1) is focused on vendor cybersecurity risk management. This is supported by the fact that the descriptions under each of the objectives discuss the cybersecurity risk that is introduced to responsible entity systems by vendors. CIP-

013-1 could even be called a vendor risk management standard, but since the Commission directed a standard "that addresses supply chain risk management," CIP-013-1 is focused on supply chain cybersecurity risk management. "Cybersecurity" was also added to the standard title since the security risks identified by the Commission are all cybersecurity risks.

In implementing Requirement 1, part 1.4, the responsible entity should consider:

- The subpart 1.3 risk assessments and identified mitigation measures
- Including procurement controls to address subparts 1.1, 1.2, and 1.3
- Including procurement controls that may help with the implementation of the other CIP Reliability Standards the responsible entity is subject to
- Various methods of procurement controls, which may include requiring vendors and service providers to describe their cybersecurity policies and procedures, including the part 1.4 subparts in a request for proposal, and/or contract
- The Cybersecurity Procurement Language for Energy Delivery Systems document developed by the Energy Sector Control Systems Working Group and published by the Department of Energy. But recognize that requiring specific contract terms may cause some vendors to walk away and may cause others to accept the legal risk that they may breach the terms
- Consider whether the vendor or service providers use third-party (e.g., product/personnel certification processes) or independent review methods to verify product and/or service provider security practices
- Consider methods to periodically monitor third-party risk such as right to audit clauses and establish reasonable audit expectations and resulting mitigation or contract termination clauses to address risks discovered during audit
- Use of the Information and Communications Technology supply chain risk management plans, as applicable, for respective systems and missions throughout acquisition activities.
- Other topics, e.g., regulatory requirements; technical requirements; chain of custody; transparency and visibility; personnel background checks and training; sharing information on security incidents; rules for disposal or retention of elements such as components, data, or intellectual property
- Require vendors to provide a bill of materials to aid in identifying imbedded third party components

The above considerations are examples of what could be included in the Guidelines and Technical Basis for CIP-013-1 for R1, part 1.4.

Potential Procurement Controls

Responsible entities may use various control(s) to address the security risk for this objective. Below are a few possible controls, which could be further explored in implementation guidance:

- Inclusion of specific inquiries in request for proposals to enable the responsible entity to assess risk under subpart 1.3

- Establish procurement review teams to review subpart 1.3 risk assessment and mitigation measures, including the Senior CIP Manager or delegate(s), to inform procurement decisions and CIP-013-1 compliance activity
- Use contract terms that address each of the subpart 1.4 topics as well as other topics and include methods to verify the supplier is following these terms as well as notification and compensation for breach of these terms
- Use commercially available tools and technology to establish a vendor risk baseline (subpart 1.3 control) and continue to monitor risk post-contract, including post-contract mitigation considerations
- Ask the supplier to demonstrate their capabilities to remediate emerging vulnerabilities and respond to security incidents in request for proposals
- Ask suppliers to provide details on expected life spans of systems from suppliers and potential mitigation options once the supplier stops supporting these systems
- Ask suppliers to share third-party/independent product testing results during the request for proposal stage of acquisition
- Conduct periodic security reviews of specific suppliers, which should be agreed upon in contract terms
- Restrict the use and publication of responsible entity information in contracts, e.g., don't allow suppliers to publish your entity name on their websites or in sales materials

Requirement R3

The Commission directed that the standard should require "a periodic reassessment of the utility's selected controls" that could be similar to the CIP-003-6 R1 approach.[28] This reassessment was addressed by a periodic review by a CIP Senior Manager in Requirement R3. The Commission also required that "this periodic assessment should better ensure that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities."[29] The Commission stated that the:

> CIP Senior Manager should consider any guidance issued by NERC, the U.S. Department of Homeland Security (DHS) or other relevant authorities for the planning, procurement, and operation of industrial control systems and supporting information systems equipment since the prior approval, and identify any changes made to address the recent guidance.

This is also addressed by Requirement R3:

> **R3.** Each Responsible Entity shall review and obtain CIP Senior Manager or delegate(s) approval at least once every 15 calendar months of the security controls set forth in the supply chain cybersecurity risk management plan(s) used to address the security objectives identified in Requirement R1. The review of the security controls shall include the consideration of new risks and mitigation measures and the identification of related changes, if any, made to the controls. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

[28] *Id*. at P 46.
[29] *Id*.

Requirement R3 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review. In the Requirement R3 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 3 and 4 address the identification and delegation process for the CIP Senior Manager for this and the other CIP Standards.