North American Transmission FORUM

Community   Confidentiality   Candor   Commitment

NATF CIP-013 Implementation Guidance: Supply Chain Risk Management Plans

Version 1.0
Document ID: 1605
Approval Date: 01/28/2022

Versioning

Version History

Date	Version	Notes
01/28/2022	1.0	Initial version

Review and Update Requirements

- Review: every 5 years
- Update: as necessary

Contents

1. Introduction

This Implementation Guidance addresses how the use of the NATF Supply Chain Security Assessment Model (NATF Model), if implemented appropriately, offers one method to meet compliance with CIP-013-1 and CIP-013-2, Requirements 1 and 2 to develop and implement supply chain cyber security risk management plans for high and medium impact Bulk Electric System (BES) Cyber Systems and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) (collectively, "CIP-013 Applicable Systems"). Throughout this document, CIP-013-1 and CIP-013-2 will be referred to as "CIP-013."

> To meet compliance with CIP-013-2 using the example contained herein, a Responsible Entity would need to ensure that their "associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS)" are included in its supply chain cyber security risk management plan(s) no later than October 1, 2022.

The NATF Model incorporates the NATF Supply Chain Security Criteria (NATF Criteria) and Energy Sector Supply Chain Risk ESSCR Questionnaire (ESSCR Questionnaire); the use of these tools is included in this guidance.

This guidance builds upon the October June 14, 2019, Electric Reliability Organization (ERO) Enterprise-Endorsed Implementation Guidance "*CIP-013-1 Supply Chain Risk Management Plans (NATF),*" which addressed the ability for Responsible Entities to rely upon the work of others by adding a process that increases the Responsible Entity's visibility of potential risks.

> The NATF Model, NATF Criteria, and ESSCR Questionnaire are security focused, and the NATF Model provides a process that covers the lifecycle of a procurement.
>
> Use of these tools does not create, suggest, or imply any increase or expansion of the requirements in the standard.
>
> *Guidance documents cannot expand upon the requirements of the Reliability Standard.[1] The failure of an entity to implement practices not required by the standard does not constitute a noncompliance.*

This implementation guidance was developed with the objective of providing Responsible Entities with assurance that a security-focused supply chain program, if implemented appropriately, will meet compliance requirements, and can increase the ERO's confidence in the Responsible Entity's program.

This Implementation Guidance does not prescribe the only approach but highlights one method that could be effective for supply chain risk management and achieving compliance with the standard. Because Implementation Guidance only provides examples, Responsible Entities may choose alternative approaches that better fit their individual situations.[2]

---

[1] The NERC Compliance Guidance Policy (November 5, 2015) *is available on the NERC website at* https://www.nerc.com/pa/comp/guidance/Documents/Compliance%20Guidance%20Policy.pdf.

[2] *Id.* at P.1.

Background

Following a Notice of Proposed Rulemaking (NOPR)[3] and subsequent technical conference,[4] the Federal Energy Regulatory Commission (FERC) issued Order 829 on July 21, 2016. This final rule directed NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. The standard was to require each affected entity to develop and implement a plan that includes security controls for supply chain management for those systems.

In response, the NERC board adopted the supply chain standards, which consisted of CIP-005-6, CIP-010-3, and CIP-013-1, in August 2017, and issued a resolution to request that NERC management, in collaboration with the appropriate NERC technical committees, industry representatives, and experts, including representatives of industry vendors,[5] further study the nature and complexity of cyber security supply chain risks. The NERC Board's resolution specifically requested the North American Transmission Forum (NATF) and the North American Generator Forum (NAGF) to "[d]evelop white papers to address best and leading practices in supply chain management, including procurement, specifications, vendor requirements, and existing equipment management that are shared across the membership of each Forum, and to the extent permissible under any applicable confidentiality requirements, distribute such white papers to industry."[6] In response to the NERC Board's resolution, the NATF developed and published the "*Cyber Security Supply Chain Risk Management Guidance*" white paper in June 2018, which is posted on the NERC website. Subsequently, the NATF developed and submitted the "*CIP-013-1 Supply Chain Risk Management Plans (NATF)*" implementation guidance. The ERO Enterprise endorsed this implementation guidance in 2019, which addressed Responsible Entities' ability to rely upon the work of others.

Since that time, the NATF and the NATF-led Industry Organizations Team (consisting of electric utilities, energy industry trade and forum representatives, vendors, third-party assessors, and solution providers) have produced—and openly shared—work that is responsive to the NERC board's resolutions to address supply chain risk management issues. The NATF and the Industry Organizations Team's objectives are to further supply chain security through identification and mitigation of risks; to unify industry on what information is needed for that purpose; and to develop practices that are efficient, effective, and meet compliance requirements.

With those objectives in mind, the NATF's Model, NATF Criteria, and ESSCR Questionnaire were developed. The Industry Organizations Team also developed guides for entities to understand third-party assessments and use solution providers for third-party risk management. A series of webinars was conducted to share entities' methods for conducting risk assessments, and the American Public Power Association (APPA), with input from other Industry Organization Team members, developed a guide on supply chain risk management, including

---

[3] 152 FERC ¶ 61,054 (July 2015).

[4] January 28, 2016 Technical Conference transcript available in Docket No. RM15-14-000.

[5] For the purposes of this guidance, the term "vendor" is used as a universal term to include original equipment manufacturers (OEMs) or software developers, resellers, or any source of a product or service to align with the NERC Reliability Standards. The term replaces the term "supplier" used In the NATF Model. For the purposes of this guidance and the NATF Model, the terms are interchangeable.

[6] The 2018 NATF and NAGF whitepapers are available on the NERC website at https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

methods for conducting a risk assessment. Information on available products and services to identify and mitigate risks was provided in another webinar series. The NERC Supply Chain Working Group (SCWG) developed a series of security guidelines that were supported and promoted by the NATF and the Industry Organizations Team.

The above efforts were focused on security practices that include and exceed the requirements of the NERC supply chain standards. Efforts to enhance security and regulatory requirements are synchronized; in being secure, a Responsible Entity also should meet compliance requirements. NERC has worked diligently with industry to respond to compliance questions through staff reports and Supply Chain Small Group Advisory Sessions in 2018 and 2021. Additionally, the NERC Compliance and Certification Committee (CCC), an Industry Organizations Team member, worked with NERC and the Regional Entities to develop a series of frequently asked questions contained in the Supply Chain Risk Mitigation Program FAQs.[7]

NERC Implementation Guidance "[p]rovides a means for registered entities to develop examples or approaches to illustrate how registered entities could comply with a standard [or requirement within a Standard] that are vetted by industry and endorsed by the ERO Enterprise. The examples provided in the Implementation Guidance are not exclusive, as there are likely other methods for implementing a standard."[8] This NATF Implementation Guidance document describes one method that a Responsible Entity could comply with CIP-013 Requirement R1 and, subsequently, CIP-013 Requirement R2.

2. Goal/Problem Statement

The goal for this Implementation Guidance is to unite supply chain security efforts with compliance efforts and provide Responsible Entities with one ERO-endorsed method of accomplishing these synchronized objectives.

3. Scope

This NATF Implementation Guidance document describes one way that a Responsible Entity could comply with CIP-013 Requirement R1 and, subsequently, CIP-013 Requirement R2.

This example does not address CIP-013 Requirement 3:

> **R3.** Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. [*Violation Risk Factor: Medium] [Time Horizon: Operations Planning*]

The NERC Compliance Guidance Policy provides clear direction that endorsement of an Implementation Guidance is not a guarantee a Responsible Entity will meet the requirements of the standard. The NERC Compliance Guidance Policy states "[t]he ERO Enterprise's endorsement means that the ERO Enterprise recognizes the guidance as appropriate for deference during Compliance Monitoring and Enforcement (CMEP) activities. Deference means that registered entities can rely on the guidance and be reasonably assured that

---

[7] These materials, plus other resources, are available on the NERC website at https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

[8] The NERC Compliance Guidance Policy (November 5, 2015) *is available on the NERC website at* https://www.nerc.com/pa/comp/guidance/Documents/Compliance%20Guidance%20Policy.pdf.

compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances and system configurations which vary across the interconnections."[9]

4. CIP-013 – Cyber Security - Supply Chain Risk Management

The purpose of the CIP-013 Reliability Standard is to "[m]itigate cyber security risks to the reliable operation of the BES by implementing security controls for supply chain risk management of BES Cyber Systems." The NATF Model represents an industry-vetted process for Responsible Entities' supply chain cyber security risk management plans.

Per Requirement R1, each Responsible Entity must develop one or more documented supply chain cyber security risk management plan(s) for CIP-013 Applicable Systems. This plan must include one or more processes for procuring and installing vendor equipment and software, transitions from one vendor to another, and must address the six risk areas defined in Requirement R1.2.

Requirements R1 and R2 of the standard[10] provides:

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems [*and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS)*]. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems [*and their associated EACMS and PACS*] to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

R1.2. One or more process(es) used in procuring BES Cyber Systems [*and their associated EACMS and PACS,*] that address the following, as applicable:

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

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

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

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

---

[9] *Id.*

[10] Additions from CIP-013-2 are shown in black italic text.

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System [*and their associated EACMS and PACS*]; and

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

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

5. Using the NATF Model to Develop Risk Management Plans (R1)

The NATF Model provides a process for Responsible Entities to use for the procurement of CIP-013 Applicable Systems that, if implemented appropriately, addresses supply chain risk management through procurement lifecycle phases translating each phase of the lifecycle into an action. The NATF Model addresses supply chain risk management through the procurement lifecycle phases, translating each phase of the lifecycle into an action. Responsible Entities implementing the NATF Model consider each of the action steps in their supply chain cyber security risk management plan(s) for CIP-013 Applicable Systems. As there are different approaches to addressing each action step, Responsible Entities document their organization's approaches.

The five-step NATF Model provides a process for identifying, assessing, and mitigating supply chain risks. The Model provides for the inclusion of vendors and solution providers, as well as flexibility for each Responsible Entity's implementation. Further, the NATF Model, the NATF Criteria, the ESSCR Questionnaire and complementary products from other participating organizations[11] provide tools that support good supply chain security practices. When executed properly and with a focus on security, the NATF Model assists entities with meeting the compliance requirements of the NERC supply chain reliability standards.[12] The five steps of the NATF Model are depicted below in Figure 1, and each step is examined in more detail.[13] The five steps of the NATF Model are used by Responsible Entities to mitigate supply chain risks by encapsulating the necessary actions and components of supply chain risk, without regard to whether the procurement is for IT or OT and whether it includes software, firmware, hardware, equipment, components, or services.

---

[11] Complementary products from other organizations are posted on the NATF public website at https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

[12] Information on the most current version of the supply chain standards can be located on the NERC website: https://www.nerc.com/Pages/default.aspx.

[13] A detailed illustration featuring the inputs to each step of the Model is provided in Appendix 4, Figure 6.

Figure 1: The NATF Supply Chain Security Assessment Model

6. Using the NATF Model to Meet CIP-013 R1, Part 1.1

Responsible Entities develop supply chain cyber security risk management plan(s) for CIP-013 Applicable Systems using the NATF Model. The NATF Model's process encompasses the compliance requirements for planning for the procurement of CIP-013 Applicable Systems to identify and assess cyber security risk(s) to the BES from vendor products or services resulting from procuring and installing vendor equipment and software, and transitions from one vendor(s) to another vendor(s), that address the six risk areas identified in Requirement R1, Part 1.2, as applicable.

Collect Information

Responsible Entities collect information from vendors to conduct a risk assessment of the vendor's security practices. Collecting information consists of obtaining information using the NATF Criteria and/or ESSCR Questionnaire and verifying that the information is accurate.

6.1   Collect Information

Responsible Entities obtain information from, or about, vendors using the NATF Criteria and/or ESSCR Questionnaire.[14]

> *The NATF Model provides the following tools for collecting information:*
>
> *1. The NATF Criteria, which can be used to collect information from a vendor or can be used as a basis for measuring a vendor's security posture/practices (i.e., a "best practices" list), and*
>
> *2. The ESSCR Questionnaire, which can be used to obtain more granular information on a vendor's security risk performance.*

---

[14] The NATF Criteria and Questionnaire may be modified from time to time pursuant to the *NATF Revision Process for the Energy Sector Supply Chain Risk Questionnaire and NATF Cyber Security Criteria for Vendors* (Revision Process), which is an open process for industry stakeholders and also provides for vetting by the ERO and E-ISAC.

> *The Responsible Entity uses these tools to collect information regarding the vendor's risk management at the **vendor's corporate level**, for a **specific product or service**, and/or at the **development system level**.*

Either or both tools can be used to collect information regarding the vendor's risk management at the vendor's corporate level, for a specific product or service, and/or at the development system level. Responsible Entities use these tools to identify risks. Once risks are identified, it is an opportunity for Responsible Entities to work with vendors on mitigation.

Using the NATF Criteria and/or ESSCR Questionnaire, Responsible Entities obtain responses that the Responsible Entity has determined are necessary to consider in the risk assessment, depending upon the vendor and the risk of the product(s) or service(s) to be procured. At a minimum, Responsible Entities include responses addressing the six risk areas specified by Requirement R1, Part 1.2 in the risk assessment.

6.2   Verify that the information is accurate

Responsible Entities verify that the information the vendor provided is accurate. To conduct an in-depth review of a vendor, Responsible Entities may conduct a complete review of a vendor's evidence and audits of the vendor's facilities. This verification method may provide the highest level of assurance of the vendor's security posture; however Responsible Entities find this is often not an efficient use of resources and, depending upon the resources and capabilities of the Responsible Entity, may not be effective. Therefore, Responsible Entities often rely upon the work of others to verify the accuracy of vendors' information.

Verifications from others that provide the highest level of assurance for Responsible Entities are obtained through either an independent assessment or certification from a qualified, credentialed third-party assessor or auditor. Also, there may be other third-party organizations that employ auditors that are trained but do not have auditing credentials. These third-party organizations may provide verifications of vendor information that can be relied upon, based upon evidence demonstrating their work processes and capabilities. Section 9 provides additional detail on Responsible Entities' actions when relying upon the work of others to verify vendor information.

In cases where the third-party certifications, assessments, or other verifications are not available, Responsible Entities may need to verify information using other available resources, which will be a consideration in the Responsible Entity's evaluation process. Further, where an assessment, certification or other form of verification does not address all the required criteria or questions for a procurement, Responsible Entities supplement the verification with other methods (or a combination of methods), which may include conducting their own review of evidence, gathering publicly available information, or obtaining another entity's review of the vendor which used the NATF Criteria or questions.

Evaluate the Information/Address Risks

The purchasing Responsible Entity can determine, based on the information and assurance provided, if any of the vendor's security practices raise a concern (i.e., are a risk) and whether that risk can be mitigated or accepted.[15]

> *When evaluating the information collected, the Responsible Entity determines:*
>
> *1. Whether the __level of the vendor's adherence__ to the NATF Criteria or the responses to the ESSCR Questionnaire identify any risks pertinent to the product or service being procured*
>
> *2. Whether the __level of assurance or verification of the accuracy__ of the vendor information is sufficient for the product or service being procured*
>
> *3. Whether __any identified risks could be mitigated__ by the vendor or the entity, or if the risk could be accepted.*

Considerations include:

6.3   An evaluation of the vendor's adherence to the NATF Criteria and/or response to the ESSCR Questionnaire (performance)

Does the vendor fully conduct all the pertinent actions contained in the NATF Criteria and/or ESSCR Questionnaire, or are there some pertinent actions that the vendor conducts partially? For any pertinent actions that are not fully conducted, the Responsible Entity can determine whether the non-action constitutes a risk.

6.4   An evaluation of the level of assurance the vendor has provided for its responses (verification)

Was the vendor able to provide the procuring Responsible Entity with assurance/verification that it performs as reported? Depending upon the potential impact the specific product or service could have on the Bulk Power System, the procuring Responsible Entity may require more assurance.

6.5   An evaluation of the significance of identified risks and how they could be addressed[16]

The procuring Responsible Entity can ascertain which identified risks require mitigation and whether it or the vendor could take actions or implement controls to mitigate each risk to lower the residual risk or

---

[15] The NERC Supply Chain Working Group (SCWG) has developed a series of supply chain security guidelines that provide guidance for evaluating vendor information and in determining whether or how to mitigate risks. These guidelines are concise three-page documents that provide a high-level summary of issues to be aware of and potential methods of addressing them. The guidelines are available on the NERC website: https://www.nerc.com/comm/CIPC/Pages/SCWG.aspx and are linked from the NATF website: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

[16] NERC Reliability Standard CIP-013 requires that, "The documentation will identify and include an assessment of the cyber security risk(s) to the Bulk Electric System specific to the registered entities organization."

potentially eliminate the risk. In some cases, the Responsible Entity may determine that the identified risk does not require mitigation because either the inherent risk is low or the residual risk is low due to existing internal controls.

Through Responsible Entities and vendors working together on solutions for identified risk, it is anticipated that repeated identification of the same risks and implementation of mitigating activities will bring an overall increase in security, as depicted by Figure 2:

Figure 2: The Vision for Alignment

6.6   Document the Determinations

The Responsible Entity maintains the vendor's responses and documents the evaluation, which helps the purchasing Responsible Entity monitor risks after the procurement as well as demonstrate compliance. Responsible Entities' secure and protect vendor responses identified as confidential information.

Monitoring risks after the procurement is a security practice beyond compliance requirements.

Conduct the Risk Assessment

After information is collected, the Responsible Entity conducts a risk assessment to determine the relative degree of residual risk among vendors that could provide the desired product or service.

6.7   Conduct Risk Assessment

> 1. *The Responsible Entity has a methodology to perform vendor risk assessments.[17]*
>
> 2. *The Responsible Entity documents the results of risk assessments.*

There are a variety of methods that could be used to conduct a risk assessment.[18] Some Responsible Entities use vendors' responses to the NATF Criteria in a staged approach, or "gates," determining which NATF Criteria are the most critical for the product or service and assessing vendor risk in phases. Other entities use a rating and ranking methodology, and some use a combination of both.

Make Purchase/Procurement Decision

The results from the supply chain risk assessment, including any mitigations that would need to be implemented and monitored, are one input into the Responsible Entity's procurement process.

> 1. *The Responsible Entity has a cross-functional process to include the information from the vendor risk assessment in the Responsible Entity's procurement procedure.*
>
> 2. *The Responsible Entity considers other entity-identified factors and the Responsible Entity's risk tolerance in selecting a vendor.*
>
> 3. *When making a procurement decision and entering into a procurement agreement or contract, the Responsible Entity considers whether implemented or agreed upon mitigations can be supported by contract terms and conditions.*

6.8   The Responsible Entity has a cross-functional process to include the information from the vendor risk assessment into the Responsible Entity's procurement procedure.

Cross-functional processes are required for the vendor risk evaluation, risk mitigation, development of contractual terms and conditions, procurement, and monitoring. Often, a single department is not responsible for these activities; therefore, Responsible Entities develop controls to ensure processes are implemented as intended across multiple functions.

---

[17] The American Public Power Association, an Industry Organizations participating member, has developed a guide for conducting risk assessments: *Cyber Supply Chain Risk Management*, available on the APPA website: https://www.publicpower.org/resource/cyber-supply-chain-risk-management and is linked from the NATF website: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination/all-resources .

[18] *Id*

6.9   The Responsible Entity considers other entity-identified factors and the Responsible Entity's risk tolerance in vendor selection.

The information obtained through the NATF Model does not dictate procurement decisions for the Responsible Entity; rather it provides supply chain security risk information to consider and weigh along with other factors.

The Responsible Entity selects the other factors and determines the importance, or weighting, of each factor it considers when awarding a procurement to a vendor. The Responsible Entity determines if the factors vary by procurement. Factors in addition to supply chain security information may include, among others:

- Financial
- Operational
- Vendor support levels
- Reputational
- Regulatory requirements
- The Responsible Entity's inherent risks
- The Responsible Entity's risk appetite
- Other information or factors as determined by the Responsible Entity

6.10   When making a procurement decision and entering into a procurement agreement or contract, a Responsible Entity considers whether implemented or agreed upon mitigations can be supported by contract terms and conditions.

Implement Controls and Monitor Risks

Supply chain risk is not limited to the procurement, completion of the service, or the installation of the product, and needs to be monitored through the lifecycle of the product or service procured. A vendor's supply chain security posture can be dynamic, requiring a Responsible Entity to have controls in place and to monitor risks.

The Responsible Entity has a plan to monitor:

1. Risks and controls associated with the procurement throughout the lifecycle of the products or services.

2. The vendor for any changes that could affect products or services (e.g., corporate changes or changes to the vendor's supply chain) as well as for any breaches or compromises.

Monitoring risks after the procurement is a security practice beyond compliance requirements.

6.11   The Responsible Entity monitors risks and controls associated with the procurement throughout the lifecycle of the products or services.

Any mitigations that have been implemented will need to be monitored to ensure that the mitigating actions remain effective, and the procured product or service should be evaluated for any changes in risk resulting from implementation or the installation of the product or service. In addition, new supply chain risks (such as concerns regarding a country of origin) may arise. A Responsible Entity may need to evaluate how these identified risks pertain to or affect existing or inventoried equipment, components, software, etc., and whether those risks can be mitigated.

6.12   The Responsible Entity monitors the vendor for any changes that could affect products or services (e.g., corporate changes or changes to the vendor's supply chain) as well as for any breaches or compromises.

How often a Responsible Entity reviews or refreshes a vendor's risk assessment may be approached differently depending upon the vendor, whether or how the vendor is being monitored for procured products or services, or whether the vendor is being considered for a new procurement. Responsible Entities may conduct vendor monitoring themselves or may employ a solution provider to conduct continuous monitoring.

7. Using the NATF Model to Meet CIP-013 R1, Part 1.2

To include the six risk areas provided in Requirement R1, Part 1.2 in process(es) used in procuring CIP-013 Applicable Systems, Responsible Entities implementing the NATF Model consider the criteria and questions that address each of the Part 1.2 risk areas for CIP-013 Applicable Systems. Responsible Entities include these criteria and questions as applicable, in the first four steps of the NATF Model's process – Collect Information, Evaluate Information/Assess Risks, Conduct the Risk Assessment, and Make Procurement Decision – and document how they approached each step and how the criteria and questions were considered.

> The Responsible Entity, with a focus on security, also implements the additional step in the NATF Model to conduct ongoing monitoring of the risk, controls, and the vendor.
>
> *Monitoring risks after the procurement is a security practice beyond compliance requirements.*

8. Using the NATF Model to Meet CIP-013 R2

Following the steps described below builds on the "*NATF CIP-013 Implementation Guidance: Using Independent Assessments of Vendors*" to provide clarity on how the Responsible Entity may meet the obligations in both Requirements R1 and R2 using the NATF Model, NATF Criteria, and ESSCR Questionnaire. The NATF Model, NATF Criteria, and ESSCR Questionnaire can be located on the NATF web site under Industry Initiatives/Supply Chain Industry Coordination[19] and individually at:

- The NATF Supply Chain Security Assessment Model
- The NATF Supply Chain Security Criteria

---

[19] https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

- [The Energy Sector Supply Chain Risk ESSCR Questionnaire (Unformatted)](#)
- [The Energy Sector Supply Chain Risk ESSCR Questionnaire (Formatted)](#)

The Responsible Entity provides evidence that it implements its supply chain cyber security risk management plan as required in CIP-013 Requirement R2. Responsible Entities may provide evidence through demonstration or documentation for how the Responsible Entity implements the NATF Model for each of the five steps.

Collected Information

8.1   For a procurement, the Responsible Entity obtains potential vendors' responses to the NATF Criteria and/or ESSCR Questionnaire as deemed necessary to evaluate the vendor security practices for corporate security hygiene and the product or service being procured; and

8.2   The Responsible Entity obtains verification of each of the vendor's information (also see Section 9).

Evaluated the Vendor Information

8.3   The Responsible Entity evaluates the vendor information to determine:

8.3.1   Each vendor's security practices (i.e., the level of adherence to the criteria/questions);

8.3.2   How confident the Responsible Entity is in determining each vendor's security practices (i.e., the level of assurance from the verification);

8.3.3   What risks are identified for each vendor that require mitigation; and

8.3.4   Whether actions or controls can be implemented to mitigate any identified risks for each vendor.

Conducted the Risk Assessment

8.4   The Responsible Entity uses its documented methodology to assess risk.

8.5   The Responsible Entity's risk assessment results identify how the methodology is applied to the vendor(s) of the desired product or service.

Made the Procure/Procurement Decision

8.6   The Responsible Entity considers the results of the supply chain security risk assessment in the procurement decision.

8.7   The Responsible Entity determines whether implemented or agreed upon mitigations for identified risks with the awarded vendor are supported by contract terms and conditions.

Implemented Controls and is Monitoring Risks

8.8   The Responsible Entity monitors the identified risks and implements controls associated with the procurement throughout the lifecycle of the product(s) or service(s).

8.9   The Responsible Entity monitors the vendor for any changes that could affect product(s) or service(s) (e.g., corporate changes or changes to the vendor's supply chain) as well as for any breaches or compromises.

> *Monitoring risks after the procurement is a security practice beyond compliance requirements.*

9. Using Independent Assessments to Verify Vendor Information (R1)

Using the NATF Model, the Responsible Entity develops its supply chain cyber security risk management plan(s) to address CIP-013 requirements. The supply chain cyber security risk management plan includes the Responsible Entity's use of the NATF Model's process for assessing risk in procuring and installing CIP-013 Applicable Systems, and in transitioning from one vendor to another vendor.

9.1   To incorporate reliance on third-party independent assessments of vendors to verify vendor information, a Responsible Entity's supply chain cyber security risk management plan, as required in CIP-013 R1, describes the Responsible Entity's process to:

     9.1.1   Ask vendors to provide a third-party independent assessment (including a description of the methodology for performing that assessment) from an auditor. The auditor evaluates the vendor's controls, tests specific control activities, or otherwise validates that the vendor's security posture meets, at a minimum, the criteria identified in CIP-013 Requirement R1, part 1.2.

     9.1.2   Evaluate the auditor's qualifications and cyber security framework used to perform the vendor assessment, ensuring that the third-party independent assessment is performed by auditor(s) with appropriate independence, credentials, and sufficient understanding of cyber security supply chain risk in the electric industry.

     9.1.3   Evaluate the scope and the results of the third-party independent assessment.

     9.1.4   Document its evaluation of the independent auditor's qualifications, the methodology and scope of the review, and conclusions to determine what existing or additional mitigating actions are appropriate to manage risk; documenting those mitigating actions. *Note:* Mitigating actions may include physical controls, logical controls, or contract modifications to address risk.

In this way, the third-party independent assessment is integrated into the Responsible Entity's overall process used in procuring CIP-013 Applicable Systems and addresses each of the security issues listed in Part 1.2 of Requirement R1.

10. Periodic Review for this Implementation Guidance

The periodicity of review of this document by the NATF and a revision history is set forth in the **Error! Reference source not found.** section of this document.

The "*Revision Process for the Energy Sector Supply Chain Risk ESSCR Questionnaire and NATF Cyber Security Criteria for Vendors*" (Revision Process) provides for an annual cycle to modify or update the NATF Criteria and ESSCR Questionnaire based on inputs from industry. Inputs are accepted from across industry, including entities, vendors, assessors, and other industry organizations, as well as ERO and Electricity Information Sharing and Analysis Center (E-ISAC) subject matter experts. The Revision Process includes posting changes for stakeholders' and the ERO Enterprise's review. Upon notification by NATF of a change, the ERO shall determine if any proposed change would jeopardize the ERO Enterprise's endorsement of this guidance and would inform the NATF of such concern to enable the concern to be addressed. The Revision Process and the ERO Enterprise review for continued endorsement ensures the criteria are kept current and relevant to address each of the security issues listed in Part 1.2 of Requirement R1 over time in a transparent manner.

The NATF Criteria, ESSCR Questionnaire, and Revision Process are posted and maintained on the NATF public website at https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

Appendix 1: Sources and Resources

The Model

The NATF Model, NATF Criteria, and ESSCR Questionnaire can be located on https://www.natf.net, under Industry Initiatives/Supply Chain Industry Coordination, at https://www.natf.net/industry-initiatives/supply-chain-industry-coordination,and individually at:

- The NATF Supply Chain Security Assessment Model
- The NATF Supply Chain Security Criteria
- The Energy Sector Supply Chain Risk ESSCR Questionnaire (Unformatted)
- The Energy Sector Supply Chain Risk ESSCR Questionnaire (Formatted)
- Revision Process for the Energy Sector Supply Chain Risk ESSCR Questionnaire and NATF Cyber Security Criteria for Suppliers

Resources

The NATF Supply Chain Industry Coordination webpage (https://www.natf.net/industry-initiatives/supply-chain-industry-coordination) also provides resources from Industry Organization Team trade organizations, entities, vendors, third-party assessors, and solution providers.

Documents
Trade Organizations
- APPA's Cyber Supply Chain Risk Management (external)
- EEI Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk V2 (external)
- NATF CIP-013-1 Implementation Guidance
- NATF Guidance for CIP-010-3 Software Integrity
- Advancing Supply Chain Security in Oil and Gas: An Industry Analysis (external)

Third-Party Assessors
- Understanding Third-Party Assessments

Solution Providers
- NATF Industry Collaboration: Using Solution Providers for Third-Party Risk Management

Presentations
Industry Organization Team and NATF
- Industry Organizations Aligned Approach for Supply Chain Cyber Security Webinar 02242020
- The Energy Sector Supply Chain Risk ESSCR Questionnaire Webinar 05192020
- Large Entity Use Case Webinar 06022020
- Large Entity Use Case Webinar - Exelon 09012020
- NATF Criteria and ESSCR Questionnaire Overview Use and Revision Process 10022020

- Identifying and Managing Potential Compromise of Network Interface Cards - NATF-RF-SERC Special Webinar 20201022
- Supply Chain Compliance Joint ERO and CCC Webinar 08072021 (Presentation | Streaming Webinar)
- ESSCR Questionnaire and Criteria Revisions Overview 03192021

Trade Organizations
- Securing Your Supply Chain – Designing and Implementing Supply Chain Security Programs – APPA 05082020
- APPA Cyber Supply Chain Risk Management Webinar hosted by MRO 09222021

Suppliers
- Suppliers Responding to Requests for Cyber Security Information 12012020
- Suppliers Responding to Requests for Cyber Security Information 01122021

Solution Providers
- Technical Assessment Methodology for Cyber Security - EPRI 10142020
- Solution Provider Webinar - EPRI 10142020

Support Products and Services

Suppliers
- PwC: Are you inundated with vendor management questionnaires? SOC 2 reporting can help

Third-Party Assessors
- Understanding Third-Party Assessments

Solution Providers
- NATF Industry Collaboration: Using Solution Providers for Third-Party Risk Management
- Asset to Vendor Network (A2V) Supplier & Product Assessment Database / Compliance Technology
- EPRI Technology Assessment Methodology (TAM) / Cyber Security Data Sheets (CSDS) for device and system supply chain risk assessment
- IHS Markit KY3P – Know Your Third Party / Third Party Risk Management
- NERC Supply Chain Working Group (SCWG) Security Guidelines
    - Cyber Security Risk Management Lifecycle
    - Procurement Language
    - Provenance
    - Risk Considerations for Open Source Software
    - Risks Related to Cloud Service Providers
    - Secure Equipment Delivery
    - Vendor Incident Response
    - Vendor Risk Management Lifecycle
- UL Supplier Cyber Trust Level