North American Transmission FORUM

*Community Confidentiality Candor Commitment*

**ERO Enterprise Endorsed Implementation Guidance**

# NATF CIP-013 Implementation Guidance: Using Independent Assessments of Vendors



Version 3.0
Document ID: 1097
Approval Date: 01/28/2022

# Versioning

## Version History

| Date | Version | Notes |
|---|---|---|
| 06/20/2018 | 1.0 | Initial version. |
| 04/03/2019 | 2.0 | Revised to address comments from ERO review team. Added independent assessor qualifications, scope of review, and clarification of process steps and documentation. Endorsed by ERO Enterprise. |
| 01/28/2022 | 3.0 | Updated to include CIP-013-2 and to incorporate the NATF Criteria, ESSCR Questionnaire, and Revision Process, as defined in the document. |

## Review and Update Requirements

- Review: every 5 years
- Update: as necessary

# Contents

# 1. Introduction

NERC's 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."[1] This NATF Implementation Guidance document describes one way that a Responsible Entity could comply with CIP-013-1 and CIP-013-2 Requirements R1 and R2. Throughout this document, CIP-013-1 and CIP-013-2 will be referred to as "CIP-013."

## Reliance on Independent Assessments of Vendors as an Acceptable Means of Identifying and Assessing Vendor Risk

The ERO has endorsed the practice of a Responsible Entity obtaining an independent assessment of the vendor's production of 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"), and/or related services as a means of complying with CIP-013.[2] The ERO Enterprise-endorsed "*CIP-013-1 Supply Chain Risk Management Plans (2016-03 SDT),"* developed by the CIP-013 drafting team, recommends that a Responsible Entity's risk assessment process identify and assess potential cyber security risks including "potential risks based on the vendor's risk management controls." Responsible Entities may consider assessing vendor risk-management controls by obtaining a "summary of any internal or independent cyber security testing performed on the vendor products to ensure secure and reliable operations."[3]

Responsible Entities that review independent assessments of vendors also build on the ERO-endorsed practice of relying on the "work of others" as a means of supporting reasonable assurance that defined reliability and security objectives are being met by vendors. The "*ERO Enterprise Guide for Internal Controls*"[4] promotes ERO Compliance Enforcement Authorities evaluating the independence, capabilities, and competencies of the "work of others" (i.e., disinterested third parties or departments that are independent from the department performing a reliability function) for purposes of compliance monitoring.[5]

Just as the ERO may rely on the "work of others" to assist in determining how to monitor a registered entity's compliance, Responsible Entities, in the context of managing their supply chain risk, may rely on qualified independent assessments of a vendor's risk-management controls to demonstrate that they have assessed cyber security risks associated with the CIP-013 Applicable Systems' products and services provided by the vendor.

The steps described below build on the "*CIP-013-1 Supply Chain Risk Management Plans (2016-03 SDT)*" to provide clarity on how the Responsible Entity may meet the obligations in both Requirement R1 and R2 when

[1] NERC Compliance Guidance Policy, November 5, 2015, *available at:* https://www.nerc.com/pa/comp/Resources/ResourcesDL/Compliance_Guidance_Policy_FINAL_Board_Accepted_Nov_5_2015.pdf

[2] NERC Reliability Standards' One Stop Shop, *available at:* https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx.

[3] CIP-013-1 Supply Chain Risk Management Plans (2016-03 SDT) at p 4 (June 2017), *available at:* https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-013-1-R1%20Implementation%20Guidance.pdf.

[4] http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Guide_for_Internal_Controls_Final12212016.pdf

[5] *Id.* at Section 2.2.2.

using an independent assessment but do not obligate a Responsible Entity to choose an independent assessment under any particular set of circumstances.

# 2. Using Independent Assessments of Vendors

## When Developing the Cyber Security Supply Chain Risk Management Plan, the Responsible Entity Describes Option for Relying on Independent Assessment (CIP-013 R1)

The Responsible Entity develops its supply chain cyber security risk management plan(s) to address CIP-013 requirements. The plan includes the Responsible Entity's process for assessing risk in procuring and installing CIP-013 Applicable Systems and transitioning from one vendor to another vendor. To incorporate reliance on independent assessments of vendors, a Responsible Entity's cyber security supply chain risk management plan, as required in CIP-013 Requirement R1, describes the Responsible Entity's process to:

1. Ask vendors to provide a third-party independent assessment (including a description of the methodology for performing that assessment), from an auditor.[6] 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.
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.
3. Evaluate the scope and the results of the third-party independent assessment.
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 that addresses each of the security issues listed in Part 1.2 of Requirement R1.

## Using an Independent Assessment as a Means for Implementing the Supply Chain Cyber Security Risk Management Plan (CIP-013 R2)

For those CIP-013 Applicable Systems and/or related services for which the Responsible Entity has determined that it is appropriate to obtain an independent assessment, the Responsible Entity may show that it implemented its plan as required in CIP-013 Requirement R2 through documenting that it:

[6] Auditors providing independent assessments have appropriate credentials to provide such an assessment. For examples of appropriate certifications, see pages 134 – 137 of https://www.nerc.com/pa/comp/ERO%20Enterprise%20Compliance%20Auditor%20Manual%20DL/NERC_Compliance%20Monitoring%20and%20Enforcement%20Manual_v4_0.pdf for example qualifications. Other examples of relevant credentials include Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA), and similar security and controls auditing certifications.

1. Asked for and received a third-party independent assessment and documented its conclusion that the independent assessor was appropriately qualified.
2. Reviewed and confirmed (such as by using a predefined checklist) that the results of the third-party independent assessment address the topics in CIP-013 Requirement R1, Part 1.2.

   **Attachment A:** The NATF Supply Chain Security Criteria (NATF Criteria), described in Attachment A, provides industry- and vendor-vetted criteria that a Responsible Entity can utilize to measure a vendor's security posture, and includes criteria to address all of the topics in CIP-013 Requirement R1, Part 1.2. The Energy Sector Supply Chain Risk Questionnaire (ESSCR Questionnaire) provides questions to assist Responsible Entities in obtaining necessary information to use in the evaluations. The NATF Criteria includes a mapping of known security frameworks that address the security topics specified in CIP-013 Requirement R1, Part 1.2.

   Either or both tools can be used to collect information regarding the vendor's risk management at the corporate level, for a specific product or service, and/or at the development system level.[7] Responsible Entities obtain responses from the NATF Criteria and/or ESSCR Questionnaire that the Responsible Entity has determined are necessary to consider in its 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 provided in Requirement R1, Part 1.2 in the risk assessment.

   **Attachment B:** The "*Revision Process for the Energy Sector Supply Chain Risk Questionnaire and NATF Cyber Security Criteria for Vendors*" (Revision Process), described in Attachment B, provides an annual cycle to modify or update the NATF Criteria and ESSCR Questionnaire based on inputs from industry stakeholders. Inputs are accepted from across industry, including entities, vendors, assessors, and other industry organizations, as well as ERO and E-ISAC subject matter experts. The Revision Process ensures the criteria are kept current and relevant to address each of the security issues listed in Requirement R1, Part 1.2 and to do so 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.
3. Reviewed and evaluated the results of the third- party independent assessment to confirm that vendor and/or Responsible Entity actions and security controls mitigate the cyber security risks to procure the CIP-013 Applicable Systems. This step includes using the third-party independent assessment to inform the actions the Responsible Entity takes to address the security issues listed in Part 1.2 of Requirement R1.

As the Responsible Entity is ultimately responsible for compliance with the supply chain cyber security standards, the Responsible Entity maintains evidence to demonstrate its compliance to CIP-013, including documentation of its supply chain cyber security risk management plan and completion of recurring reviews as well as use of its supply chain cyber security risk management plan. Use includes identifying risks, risk assessment conclusions, and mitigating actions and status.

[7] 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 Suppliers* (Revision Process), which is an open process for industry stakeholders and also provides for vetting by the ERO and E-ISAC.

# 3. 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 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 E-ISAC subject matter experts. The Revision Process includes posting changes for stakeholder and the ERO Enterprise review. Upon notification by NATF of a change, the ERO shall determine if any proposed change would jeopardize the ERO Enterprise 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 ensure 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 A – NATF Criteria and ESSCR Questionnaire

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. 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. Different approaches exist to address each action step, and 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[8] 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.[9,10] The five steps of the NATF Model are depicted below in Figure 1. 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.


Figure 1: The NATF Supply Chain Security Assessment Model

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

- The NATF Supply Chain Security Assessment Model

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

[9] In response to FERC Order No. 829, NERC Reliability Standards Project 2016-03 Cyber Security Supply Chain Risk Management developed new Reliability Standard CIP-013-1 and modified Reliability Standards CIP-005-6 and CIP-010-3, which collectively have become known as the "supply chain standards."

[10] 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.

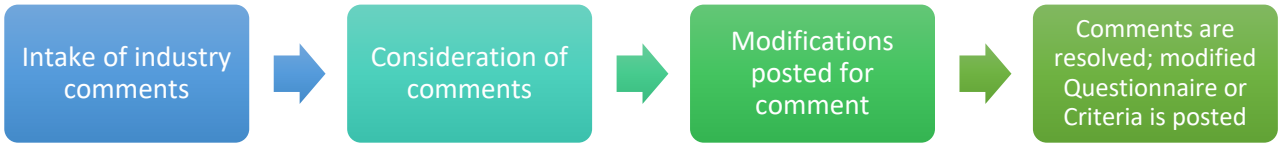
- The NATF Supply Chain Security Criteria
- The Energy Sector Supply Chain Risk Questionnaire (Unformatted)
- The Energy Sector Supply Chain Risk Questionnaire (Formatted)

# Appendix B – NATF Criteria and ESSCR Questionnaire Review and Update Process

The purpose of the Revision Process is to facilitate the periodic reviews and modifications of the NATF Criteria and the ESSCR Questionnaire.[11] These living documents were developed for industry-wide use to drive consistency of information obtained from vendors of bulk power system hardware, software, and services.

This procedure covers modifications and maintenance of the NATF Criteria and the ESSCR Questionnaire. Modifications are made with consideration of input from across industry, including entities, vendors, assessors, and other industry organizations, as well as ERO and E-ISAC subject matter experts, and includes adding, deleting, or modifying individual questions in the ESSCR Questionnaire or individual criterion in the Criteria as well as adding, deleting, or modifying mappings to security frameworks (e.g., SOC2, ISO27001, etc.). This process involves NATF members and non-NATF members, so is not governed by NATF confidentiality policies.

## Summary of Major Steps




## Process Overview

The process provides for an annual cycle to modify or update the Questionnaire and Criteria based on inputs from industry. Inputs are accepted from across industry, including entities, vendors, assessors, and other industry organizations, as well as the ERO Enterprise and E-ISAC. The process provides for modifications or updates that are more urgent and includes a monthly review of industry inputs to identify and address those modifications or updates. As the purpose of the NATF Criteria and the ESSCR Questionnaire is to provide a consistent set of questions for entities to ask vendors, it is optimal that the NATF Criteria and the ESSCR Questionnaire remain as stable as possible. However, in driving industry convergence on the use of these tools, industry inputs can assist with:

- Reducing the number of questions in the Questionnaire
- Ensuring that all necessary information needed to evaluate vendor risks is being obtained
- Providing mapping to helpful security frameworks

Modifications to the NATF Criteria and the ESSCR Questionnaire will be considered simultaneously to keep the documents aligned. This includes instances where the same modification would need to be made in both documents, such as an update for mappings to security frameworks, as well as instances where a revision to one of the documents would have an impact on and be the impetus for a different change in the other document. The Questionnaire and Criteria review team will post potential changes to the Questionnaire and Criteria in early March of each year.

The Revision Process can be located on NATF.net under Industry Initiatives/Supply Chain Industry Coordination.

[11] The Questionnaire and Criteria are available at https://www.natf.net/industry-initiatives/supply-chain-industry-coordination