

North American Transmission Forum External Newsletter

July 2021

NATF Posts Updated Supply Chain Documents for Industry

The “Supply Chain Security Assessment Model,” “NATF Supply Chain Security Criteria,” and “Energy Sector Supply Chain Risk Questionnaire” version 2.0 documents have been posted for industry use on the [Supply Chain Cyber Security Industry Coordination](#) page of the NATF public website. These postings reflect changes suggested by industry during the annual revision cycle.

Using the Assessment Model, Criteria, and Questionnaire

The five-step model provides a solid foundation for identifying, assessing, and mitigating supply chain risks; provides for inclusion of suppliers and solution providers depending upon each entity’s needs; and provides for flexibility of each entity’s implementation.

The criteria and questionnaire support the first three steps in the assessment model. The graphic to the right depicting the model provides a streamlined view of the process; however, it is important to review the detail for each of the steps so the intent of the model is not misconstrued and full value of the model can be realized. A full, yet concise, description is provided in the “Supply Chain Security Assessment Model,” and the basic actions for each step are provided here.



Supply Chain Security Assessment Model

Collect (and Validate) Information

Use existing means to obtain information regarding a supplier’s adherence to the NATF criteria or questionnaire:

- **Validated responses:** Obtain a certification (e.g., IEC 62443 or ISO 27001) or assessment (e.g., SOC 2 Type II) that maps to the criteria. *This would provide validated information.*
- **Supplier attestation (not validated):** Obtain a supplier-completed questionnaire or responses to the criteria. *This could be validated by a review of evidence or supporting certifications/assessments.*
- **Shared assessment:** Obtain an assessment conducted by another entity. *This may or may not be validated information.*

Collect additional information from public sources as necessary.

Evaluate the Information and Address Risks

Evaluate three levels, considering the product or service to be purchased: adherence, assurance, and ability to mitigate risks:

- **Supplier’s security posture:** Determine if the supplier’s level of adherence to the NATF criteria or questionnaire is appropriate for the product or service being purchased.

Open Distribution

Copyright © 2021 North American Transmission Forum. Not for sale or commercial use. All rights reserved.

- *Validation of information:* What level of assurance was provided for the accuracy of the supplier information and is the level of confidence provided appropriate for the product or service?
- *Mitigate identified risks:* Did the above two questions identify risks, and can those risks be mitigated or accepted?

Conduct Risk Assessment (of Supplier's Supply Chain Security)

- Based on the information obtained in the prior two steps, including any risk mitigations, conduct a supply chain security assessment for the supplier.

Note that the criteria and questionnaire are not “frameworks” in the same manner as security frameworks such as an IEC 62443, ISO 27001, or a SOC 2 Type II, among others. Those frameworks are audited by qualified third-party assessors, and suppliers receive either a certification or assessment report indicating their performance. Entities can use these security frameworks to validate information provided by the supplier.

When using a security framework audit or certification to validate supplier responses, an entity should verify that the certification or assessment report addresses all of questions or criteria needed to analyze risk for the purchase, which can be done by reviewing the report's statement of applicability. Mapping to selected security frameworks is provided in the NATF criteria.

Next Steps

The NATF continues to work externally on supply chain risk management with the Industry Organizations Team consisting of electric utilities, energy industry trade and forum representatives, suppliers, third-party assessors, and solution providers. The team has established goals to guide 2021 activities, including the following:

- Adoption of the NATF “Supplier Cyber Security Assessment Model”
- Monitoring of threat and governmental/regulatory landscapes

Central Repository/Library

As the industry adopts the assessment model, the need for additional assistance in obtaining validated supplier information has been identified. The NATF and the Industry Organizations Team are taking actions to help, exploring the development of a central repository for supplier information. The objective is to provide an affordable, easy-to-access library of information for suppliers to the electric industry. Entities will continue to have the ability to conduct a risk assessment for a potential supplier, identify risks and mitigations, and make a risk-informed purchase decision.

Regulatory Endorsement

The NATF, with support from the Industry Organizations Team, is working towards obtaining endorsement of the model, criteria, and questionnaire from the ERO Enterprise. The supply chain security assessment model is focused on security; however, obtaining assurance that the model provides a solid framework for compliance will provide additional confidence for adoption. These documents are examples of work that originated based on a request from the NERC Board of Trustees.¹

¹ In its August 2017 resolution adopting the supply chain standards, the NERC board of trustees requested NATF and other industry organizations to develop and share “best and leading practices in cyber security supply chain risk management, including procurement, specification, vendor requirements, and managing existing equipment activities.” (See [NERC Board of Trustees' Resolution](#))

Learn more about the Industry Organizations Team and projects supporting the 2021 goals at <https://www.natf.net/industry-initiatives/supply-chain-industry-coordination>

Response to U.S. Department of Energy (DOE) Request for Information (RFI)

The NATF submitted a response to the April 20, 2021, DOE RFI on “Ensuring the Continued Security of the United States Critical Electric Infrastructure.” The NATF’s response highlights that it is uniquely positioned and prepared to assist in protecting the security, integrity, and reliability of the bulk power system through the elimination of compromises introduced through supply chains, and references the long-standing, collaborative supply chain risk management efforts led by the NATF.

At a high level, the NATF recommended “...continued collaboration and coordination among governmental agencies and between the government and the private sector, measured use of clear prohibition orders if needed to address risks requiring immediate action, increased sharing of risk information identified by intelligence agencies, support for private sector collaboration (such as the NATF activities), and continued use of the existing regulatory framework.”

Responses to the RFI are posted on the DOE’s “Securing Critical Electric Infrastructure” web page: <https://www.energy.gov/oe/securing-critical-electric-infrastructure>.

Facility Ratings Practices Implementation

The NATF and members representing approximately 83% of the total transmission mileage at 100 kV and above in the United States and Canada continue work and reporting on enhancements to members’ facility ratings practices and processes, with guidance from the “NATF Facility Ratings Practices Document” developed by a team of subject-matter experts from NATF member companies.

The NATF periodically surveys its members to learn the extent to which NATF members have implemented and/or enhanced their facility ratings practices and processes. A summary report on overall member implementation status as of April 2021 will be provided by the NATF to NERC and regional entity leadership in August or September. Future updates are planned approximately every six months.

In addition, NATF staff participates in the joint Compliance and Certification Committee / Reliability and Security Technical Committee Facility Ratings Task Force (FRTF) to help ensure the NATF and FRTF efforts are complementary and not duplicative.

The “NATF Facility Ratings Practices Document”—published for members in mid-2020—provides guidance for establishing sustainable programs, processes, and internal controls to help ensure that facility ratings are accurate and that ratings for equipment and facilities are documented and communicated.

The NATF facility ratings practices are consistent with and align with practices and controls suggested by the ERO Enterprise in its November 2019 facility ratings problem statement and in reports and webinars presented by NERC and the regional entities.

For more information about the NATF, please visit www.natf.net.