North American Transmission Forum

NATF Supply Chain Security Assessment Model

Open Distribution for Supply Chain Materials

The NATF makes no and hereby disclaims all representations or warranties, either express or implied, relating to the content, including as to the accuracy or completeness of the information. No liability is assumed by the NATF for any damages arising directly or indirectly from the content or by the use or application thereof. Use of the content constitutes agreement to defend, indemnify, and hold the NATF harmless from and against all claims arising from such use.

Version 3.0
Document ID: 1302
Approval Date: 11/20/2024

Versioning and Acknowledgments

Version History

Date	Version	Notes
01/31/2020	1.0	
03/30/2020	1.1	Updated document with revised copyright
06/04/2021	2.0	Updated document content, figures, and appendices
10/23/2023	2.1	Corrected broken hyperlinks.
11/20/2024	3.0	Updated document figures, references, and formatting. Made revisions throughout to improve readability and avoid duplicating information proved in referenced documents.

Review and Update Requirements

- Review: every 5 years
- Update: as necessary

Contents

1. Purpose

The purpose of the Supply Chain Security Assessment Model (Model) is to provide a streamlined, effective, and efficient industry-accepted approach for entities to evaluate supplier supply chain security practices. The Model has been endorsed by representatives from energy industry trade organizations and forums, NATF member utility representatives, key electric sector suppliers, and third-party assessors, and is supported by solution providers. If applied widely, the Model will reduce the burden on suppliers, provide entities with more and better information, and improve supply chain security. The tools contained in the Model and supporting services offered by solution providers will provide critical information for entities to consider when conducting risk assessments for potential suppliers of products and services.

2. Scope

The scope of this document is the activities and processes that support the following Model objectives:

- Streamline common approaches to evaluating a supplier’s security practices
- Provide flexibility within common approaches
- Ensure the common approaches are scalable to include all suppliers and purchasing entities
- Focus on good supply chain security practices while addressing compliance requirements

3. Definitions

FERC

Federal Energy Regulatory Commission

NERC

North American Electric Reliability Corporation

Solution provider

An organization that collects and provides supplier information and may provide additional services to assist companies with supplier risk assessments.

IT

Information technology

OT

Operational technology

4. The Model

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. Further, the Model and complementary products from other organizations[1] provide tools that support good supply chain security practices. When executed properly and with a focus on security, the Model will assist entities with meeting the compliance requirements of the NERC supply chain reliability standards,[2] which became effective on October 1, 2020, and are revised from time to time.[3]

The five steps of the Model are depicted in Figure 1.

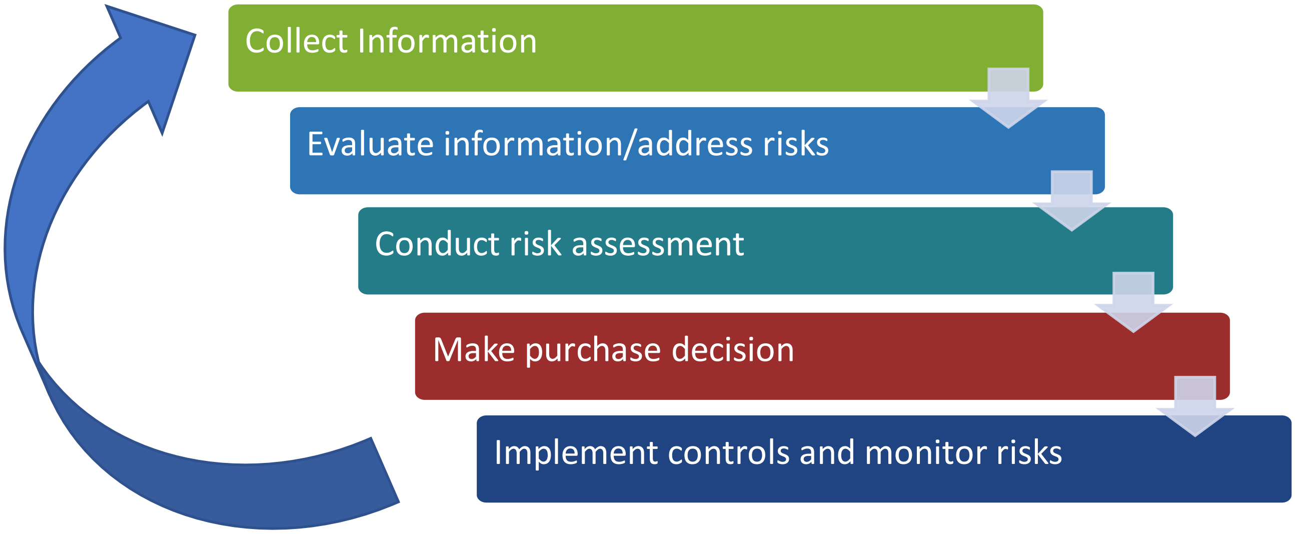
Collect Information
Evaluate information/address risks
Conduct risk assessment
Make purchase decision
Implement controls and monitor risks

Figure 1: The Supply Chain Security Assessment Model

5. The Five Steps of the Model

The five steps of the Model provide a strong foundation to mitigate supply chain risks by encapsulating the necessary actions and components of supply chain risk, without regard to whether the purchase is for IT, OT, software, firmware, hardware, equipment, components, or services. The actions contained within each step are outlined in the following sections.

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

[2] In response to FERC Order No. 829, NERC Reliability Standards Project 2016-03 Cyber Security Supply Chain Risk Management developed 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."

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

Step 1. Collect Information

The Model supports the use of the following tools for collecting information:

1. The NATF Supply Chain Security Criteria (NATF Criteria) can be used to collect information from a supplier or used as a basis for measuring a supplier's security posture/practices (i.e., a "best practice" list), and

2. the Energy Sector Supply Chain Risk Questionnaire (NATF Questionnaire) can be used to obtain more granular information on a supplier's supply chain risk performance.

Either tool can be used to collect information regarding the supplier's risk management at the supplier's corporate level, for a specific product or service, and/or at the development system level. These are not pass/fail tools; rather, they are designed to identify risks and provide an opportunity for mitigation.

Entities should provide the entire NATF Criteria and/or the entire NATF Questionnaire to a supplier. Likewise, suppliers should provide answers to all questions or criteria. Requesting responses in their entirety assists suppliers in recognizing these tools, having responses prepared, and thus being able to provide responses in a timely manner. The entity can determine which responses they use in their risk assessments based on the supplier and the risk of the product or service being procured. When entities have additional questions, or need a question modified, those may be provided to the supplier as an addendum to the NATF Questionnaire or Criteria.

Entities should obtain information from, or about, suppliers and verify that the information is accurate. The information received from or about a supplier may be verified in several ways:

The supplier could provide a security framework report from a qualified independent third-party

This would include either a certification to, or assessment of, a supplier's performance to a security framework from a qualified auditor or assessor. 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. Examples include:

- *Certification* - The supplier could provide a certification to an existing security framework (e.g., IEC 62443, ISO 27001)
- *Independent assessment or audit* - The supplier could provide its report from an independent assessment (e.g., SOC2) or audit by a qualified auditor or assessor

Mapping is provided to selected security frameworks in the NATF Criteria and Questionnaire.

Entity could procure a report from an independent third party

This would include either a report or audit conducted by a third-party professional organization or entity. The receiving entity should verify that the information collected addresses all the questions or criteria needed to analyze risk for the purchase and should understand how the accuracy of the information was verified by the third party. Examples include:

- *Solution Provider* – The entity may procure information and verification through a solution provider that specializes in analyzing and evaluating suppliers.

- *Sharing prior purchaser audit* – The entity may rely on an audit or assessment another purchaser had conducted previously that could be obtained from the prior purchaser/entity, from the supplier, or from a solution provider

The supplier could provide verification of accuracy with the information

This would consist of a self-attested response to the NATF Criteria or Questionnaire with supporting evidence that the purchasing entity could review.

If the supplier cannot or will not provide information, a purchasing entity can seek information from other sources

- Investigate other external evaluations of the supplier (e.g., a Department of Defense maturity ranking)
- Investigate open or private sources to verify supplier's responses, including suppliers' security policy statements or trust-center webpages, financial reporting services, references from other entities that purchase from the supplier, etc.
- Use other verification methods, such as hardware, firmware and software security assessments or testing

When evaluating a third-party assessment of any kind, it is imperative to understand the scope of the evaluation as well as to validate the assessor's qualifications. These concerns, including others, are explored in the ERO Enterprise-endorsed implementation guidance, *NATF CIP-013 Implementation Guidance: Using Independent Assessments of Vendors*[4].

Mapping to Third-Party Certifications and Assessments/Audits

The NATF Criteria and Questionnaire are provided on a spreadsheet and are mapped to several existing security frameworks. This is not an all-inclusive list. The mappings are intentionally provided in this format so that an entity may map to an additional security framework or certification. A critical observation would be to first see which elements are not addressed by the security frameworks already mapped, and then use other methods (which may include referencing an additional security framework) to verify the suppliers' performance to those remaining elements.

Step 2. Evaluate the Information/Address Risks

When evaluating the information collected, an entity can determine:

1. Whether the level of the supplier's adherence to the NATF Criteria or the responses to the Questionnaire identify any risks pertinent to the product or service being purchased

2. Whether the level of assurance or verification of the accuracy of the supplier information is sufficient for the product or service being purchased

3. Whether any identified risks could be mitigated by the supplier or the entity, or if the risk could be accepted.

[4] https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/natf-cip-013-using-independent-assessments-of-vendors.pdf

The purchasing entity can determine, based on the information and assurance provided, if any of the supplier's security practices raise a concern (i.e., are a risk) and whether that risk can be mitigated or accepted. Considerations include:

An evaluation of the supplier's adherence to the NATF Criteria and/or response to the Questionnaire
Does the supplier fully conduct all the pertinent actions contained in the Criteria and/or Questionnaire or are there some pertinent actions that the supplier conducts partially? For any pertinent actions that are not fully conducted, the entity can determine whether the non-action constitutes a risk.

An evaluation of the level of assurance the supplier has provided for its responses
Was the supplier able to provide the purchasing entity with assurance that it performs as reported? Depending upon the potential impact the specific product or service could have on the Bulk Power System, the purchasing entity may require more assurance.

An evaluation of the significance of any identified risks and how they could be addressed
The purchasing entity can ascertain whether it or the supplier could take actions or implement controls to mitigate any identified risks or if the risks can be accepted.

Mitigation of Risks

Identified risks are evaluated for potential mitigations that would result in a lower residual risk or an elimination of the risk. Mitigations could be implemented by the supplier or by the entity. In some cases, the risk may be such that it can be accepted. Through entities and suppliers 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:

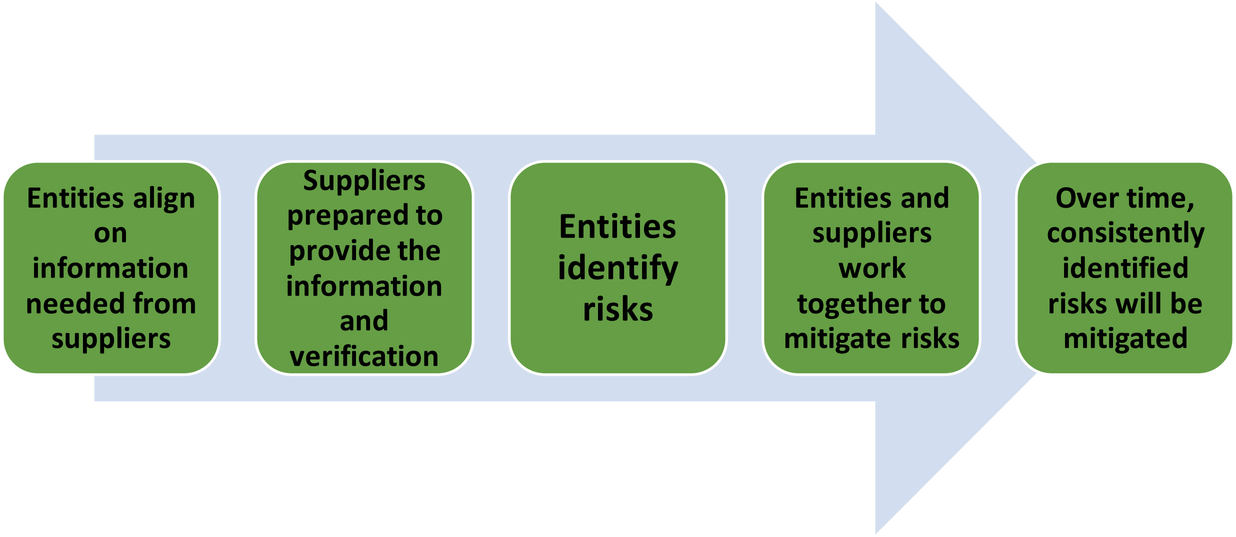
Entities align on information needed from suppliers
Suppliers prepared to provide the information and verification
Entities identify risks
Entities and suppliers work together to mitigate risks
Over time, consistently identified risks will be mitigated

Figure 2: Vision for Alignment

Document the Determinations

Maintaining the supplier's responses and documenting the evaluations helps the purchasing entity to monitor risks after the purchase as well as demonstrate compliance.

Step 3. Conduct the Risk Assessment

1. The entity should have a methodology to perform supplier risk assessments.
2. The entity should document the results of risk assessments.

The entity then conducts a risk assessment to determine which suppliers could provide the desired product or service with the least amount of residual risk. There are a variety of methods that could be used to conduct a risk assessment. Some entities use the suppliers' responses to the criteria in a staged approach, or gates, determining which criteria are the most critical for the product or service and assessing supplier risk in phases. Other entities use a rating and ranking methodology, and some use a combination of both.

The entity's risk assessment process determines the risk that could derive from a procurement, with input from sources such as the NATF Criteria, NATF Questionnaire, certifications to existing frameworks/standards, independent assessments/audits from qualified third-parties, open-source information, shared entity assessments, other data sources, or a combination of these sources. Supplier answers to specific criteria or questions may or may not prevent the entity from procuring a product from the supplier. The information from these various sources, as available, should be viewed as input to the risk assessment process documented by each entity, and is not intended as a checklist of items that require mitigation. The entity's risk assessment process should identify risk and provide an opportunity for any mitigation the entity deems appropriate.

Step 4. Make Purchase Decision

1. Develop a cross-functional process to include the information from the supplier risk assessment in the entity's purchase procedure.
2. Consider other entity-identified factors and the entity's risk appetite in supplier selection.
3. Evaluate whether implemented or agreed upon mitigations can be supported by contractual terms and conditions before entering into a purchase agreement or contract.

The results from the supply chain risk assessment, including consideration of any mitigations that need to be implemented and monitored, are one input into the entity's procurement process. Depending upon the nature of the mitigations and the risk associated with a failure of the mitigations, entities may include terms and conditions to support the mitigation activities in procurement contracts or purchase order terms and conditions.

The information obtained through this Model does not dictate purchasing decisions for the purchasing entity; rather it provides risk information to consider and weigh along with other factors. This Model does not address what factors a purchasing entity should consider (and which may vary by purchase) or how the entity should weigh their considerations. These factors may include, among others:

- Financial
- Operational
- Supplier support levels

- Reputational
- Regulatory requirements
- The entity's inherent risks
- The entity's risk appetite
- Other information or factors as determined by the entity

Cross-Functional Process

Cross-functional processes are required for the supplier risk evaluation, mitigation, the development of contractual terms and conditions, procurement, and monitoring. Often there is not a single responsible department, so entities should develop controls to ensure processes are implemented as intended across multiple functions.

Step 5. Implement Controls and Monitor Risks

> The entity should have a plan to monitor:
>
> 1. Risks and controls associated with the purchase throughout the lifecycle of the products or services.
>
> 2. The supplier for any changes that could affect products or services (e.g., corporate changes or changes to the supplier's supply chain) as well as for any breaches or compromises.

Supply chain risk is not limited to the purchase, completion of the service, or the installation of the product, and needs to be monitored through the lifecycle of the product or service purchased. A supplier's supply chain security posture can be dynamic, requiring an entity to have controls in place and monitor risks.

Controls and Monitoring Risk

Any mitigations that have been implemented need to be monitored to ensure that the mitigating actions remain effective, and the purchased product or service should be evaluated for any changes in risk resulting from implementation. In addition, new supply chain risks (such as concerns regarding a country of origin) may arise, and an 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.

Review of Supplier Risk Assessment

How often an entity reviews or refreshes a supplier's risk assessment may be approached differently depending upon the supplier, whether or how the supplier is being monitored for purchased products or services, or whether the supplier is being considered for a new purchase. Entities may conduct supplier monitoring themselves or may employ a solution provider to conduct continuous monitoring.

6. Conclusion

Supply chain exploitation is not just a potential risk but has become reality. Now more than ever, industry needs to take actions to prevent attacks and breaches, be knowledgeable of breaches that have occurred, and know how to identify if a compromise has affected its systems. The NATF in conjunction with industry has developed this Supply Chain Security Assessment Model to encapsulate the necessary actions and components for supply chain risks.

The Model can assist entities in management of supply chain risks. It takes advantage of existing methods to provide entities with a streamlined, effective, and efficient approach while providing flexibility for each entity's implementation. Entities can build upon this Model as they mature in their processes and as new aspects of supply chain risk are identified. This Model is available for industry stakeholders and adoption of the Model will provide entities with a strong foundation to address supply chain security.

7. Related Documents

The following documents and resources are provided for additional guidance:

- NATF Supply Chain Industry Coordination website and resources
  - https://www.natf.net/industry-initiatives/supply-chain-industry-coordination/
- NERC Supply Chain Working Group (SCWG) supply chain security guidelines
  - https://www.nerc.com/comm/RSTC/Pages/SCWG.aspx
  - Available guidelines cover topics such as Cloud Computing, Open-Source Software, Vendor Incident Response, Supply Chain Provenance, and more.
- American Public Power Association (APPA): *Cyber Supply Chain Risk Management*
  - https://www.publicpower.org/resource/cyber-supply-chain-risk-management
- Edison Electric Institute (EEI): *Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk*
  - https://www.eei.org/-/media/Project/EEI/Documents/Issues-and-Policy/Model--Procurement-Contract.pdf