North American Transmission FORUM

Community Confidentiality Candor Commitment

Supplier Cyber Security Assessment Model

Disclaimer
This document was created by the North American Transmission Forum (NATF) to facilitate industry work to improve reliability and resiliency. The NATF reserves the right to make changes to the information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis. "North American Transmission Forum" and its associated logo are trademarks of NATF. Other product and brand names may be trademarks of their respective owners. This legend should not be removed from the document.

Version 1.0
Document ID: 1302
Approval Date: 01/31/2020

Versioning and Acknowledgments

Contributing Organizations

ABB Power Grids

American Public Power Association (APPA)

Con Edison Working Group (ConEd)

Edison Electric Institute (EEI)

Ernst & Young, LLP (E&Y)

GE Power

ISO/RTO Council (IRC)

KPMG

Large Public Power Council (LPPC)

National Rural Electric Cooperative Association (NRECA)

North American Energy Standards Board (NAESB)

North American Generator Forum (NAGF)

North American Transmission Forum (NATF)

OSI

Schneider Electric

Schweitzer Engineering Laboratories, Inc.

Siemens Industry, Inc.

Transmission Access Policy Group (TAPS)

With appreciation for the NATF Steering Team Members

- Ameren
- American Electric Power
- Duke Energy
- Exelon
- Nebraska Public Power District
- PJM
- PPL Electric Utilities
- Southern Company

Version History

Date	Version	Notes
1/31/2020	1.0	

Review and Update Requirements

- Update: as necessary
- Review: every year

Contents

1. Purpose

The purpose of the Supplier Cyber Security Assessment Model (Model) that has been endorsed by Industry Organizations[1] is to provide a streamlined, effective, and efficient industry-accepted approach for entities to evaluate supplier cyber security practices, which, if applied widely, will reduce the burden on suppliers, provide entities with more and better information, and improve cyber security. This evaluation will provide critical information for entities to consider when conducting risk assessments for potential suppliers of products and services.

The Model describes methods for purchasing entities to gain assurance a supplier is adhering to key supply chain cyber security practices as set forth in the NATF Cyber Security Supply Chain Criteria for Suppliers (the NATF Criteria). The purchasing entity can consider any identified risks in its risk assessment and determine whether the risk can be mitigated or accepted.

The overall objectives of this work were to 1) streamline common approaches to evaluating a supplier's cyber security practices, 2) provide for flexibility within the common approaches, 3) ensure the common approaches are scalable to include all suppliers and purchasing entities, and 4) while the focus is on good cyber security practices, if executed properly, the approaches will address requirements in the NERC supply chain related standards.

2. Scope

The scope of the Model addresses the first two steps in the supply chain cyber security risk assessment lifecycle (as shown in Figure 1), which provide information for purchasing entities to consider in their risk assessment.[2]

Figure 1: The Supply Chain Cyber Security Risk Assessment Lifecycle

The NATF, with inputs from the Industry Organizations, has created a Model that:

1. establishes criteria entities may use to evaluate supplier cyber security practices (the NATF Criteria);
2. suggests how entities obtain assurance of the supplier's adherence to the criteria.

---

[1] The team of Industry Organizations includes representatives from Industry Trade Organizations and Forums, NATF member utility representatives, key electric sector suppliers, and third-party assessors

[2] 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)

The Model and complementary products from other organizations provide tools for good cyber security practices that, executed properly, ensure compliance with the NERC supply chain reliability standards,[3] which become effective on July 1, 2020. Many of the criteria exceed what is required for compliance.

3. The Model

An overview of the Model, which uses existing sources of information to provide for a streamlined, effective and efficient process for entities' informed purchase decisions, is shown in Figure 2.

Figure 2. Overview of the Industry Organizations' Supplier Cyber Security Assessment Model

[3] 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."

Once an entity has determined it has a need to procure a product or service, the entity will determine a short list of suppliers to consider. The entity may have a history with all or some of these suppliers, and in some cases may even have a Master Services Agreement (MSA) with the supplier but will conduct a risk assessment in regard to the procurement of this specific product or service.

The Supplier's Adherence to the NATF Criteria

The Model uses the NATF Criteria as the basis for determining a supplier's cyber security practices. These criteria are a list of activities that are desirable cyber security practices. **This is not a Pass/Fail list and the criteria are not intended to be used in that manner.** The supplier should provide a potential purchasing entity with information on how they perform or could perform to each of the criteria and, depending upon how the information is provided, a level of assurance that the responses are accurate. The purchasing entity will determine if there are any of the supplier's cyber security practices that raise a concern (i.e., are a risk) and whether that risk can be mitigated or accepted.

Use Existing Means to Obtain Information Regarding Supplier's Adherence to the NATF Criteria

A purchasing entity will ask potential suppliers whether, and to what degree, the supplier adheres to the NATF Criteria. There are many ways that a supplier could respond with the information:

3.1 **By providing a report from an independent third-party assessor**

- The supplier could provide a certification to an existing security framework (e.g., IEC 62443, ISO 27001)[4]
- The supplier could provide its report from a qualified independent assessment or audit[5]

3.2 **By providing information themselves or from another source**

- A self-attestation response to the Supplier Cyber Security Assessment Questionnaire[6]
- Sharing an audit or assessment another purchaser had conducted
- Copies or sections from its procedures to supplement a certification report

3.3 **The supplier cannot or will not provide information. In these cases, a purchasing entity can**

- Investigate other external evaluations of the supplier (e.g., the DOD maturity ranking)
- Investigate other open or private sources to verify supplier's responses
- Use other verification methods such as reverse engineering or other testing

3.4 **The supplier may provide a combination of the above**

- Where one method wouldn't address all the specifics contained in the criteria, the supplier may use a combination of methods to report and verify its adherence to the NATF criteria

[4] See Appendix 1 for process detail

[5] See Appendix 2 for process detail

[6] A standardized questionnaire is being developed for industry use in conjunction with this Model.

Third-Party Assessments

The NATF Criteria are provided on a spreadsheet and are mapped to several existing security frameworks. This is not an all-inclusive list. The criteria are intentionally provided in this format so that an entity could use it to map the Criteria to an additional framework or certification. As entities add additional frameworks, their mapping could be included on the master NATF Criteria sheet to allow other entities to benefit from their work.

Evaluate the Information

Purchasing entities will evaluate the quality of the information received from the supplier and will use that in their risk assessment. Considerations include:

An evaluation of the supplier's adherence to the NATF Criteria. Does the supplier do all of the actions contained in the criteria or are there some actions that the supplier does partially? For any Criteria that are not fully conducted, the entity must determine whether the non-action constitutes a risk.

An evaluation of the level of assurance the supplier has provided for its responses.[7] 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 will need to ascertain whether it or the supplier could take actions or controls to mitigate any identified risks or are the risks could be accepted.

Document the Determinations

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

4. Conduct the Risk Assessment

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

- Financial
- Operational
- Supplier support levels
- Reputational

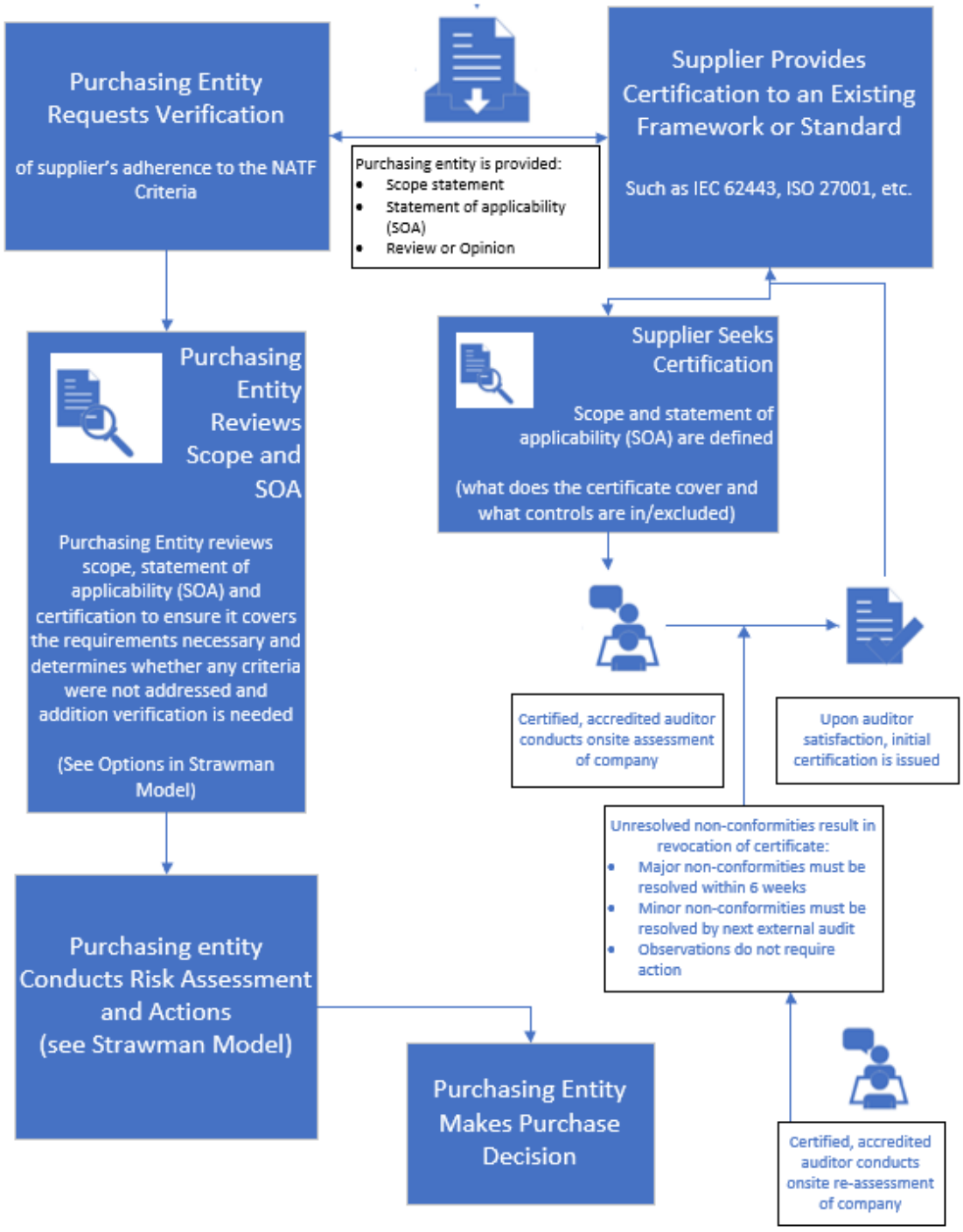
[7] See Appendix 3

- Regulatory
- Governmental cyber security information
- The entity's inherent risks
- The entity's risk appetite

5. Conclusion

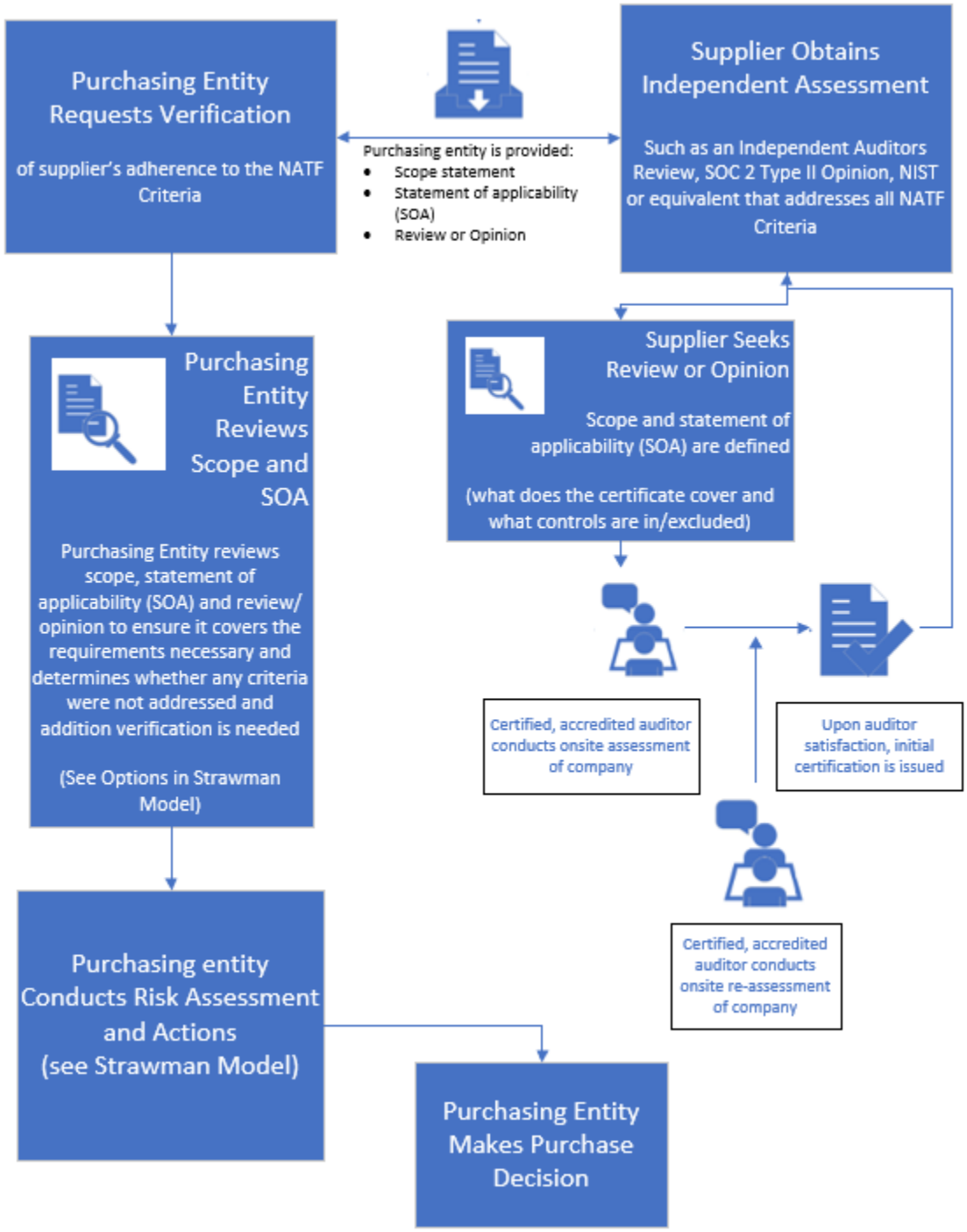
Entities can look to existing mechanisms to obtain information regarding suppliers' cyber security practices. The level of risk relating to a procurement of products or services that an entity is willing to assume may be based on a variety of factors and the potential impacts of each. At this time, the Supplier Cyber Security Assessment Model does not prescribe any method for an entity to make risk determinations—the Model takes advantage of existing formats to provide entities with a streamlined, effective and efficient source of information that each entity can use to make informed decisions.

Appendix 1: Certification to Existing Framework/Standard[8]



[8] Graphics reprinted with permission from GE Power

Appendix 2: Qualified Independent Assessment[9]



[9] Graphics reprinted with permission from GE Power