North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

NATF Cyber Security Supply Chain Criteria Application Guide

July 30, 2019

Introduction to the NATF Criteria

These NATF Criteria were developed to support the risk management strategies outlined in the NATF Cyber Security Supply Chain Risk Management Guidance (Guidance).[1] A suppliers' performance to the NATF Criteria is an indication of a supplier's cyber security practices when suppling products or services supporting reliable operation of the Bulk Electric System (BES), and are data inputs into an entity's risk analysis for the supplier.[2]

As outlined in the Guidance document, an entity's cyber security supply chain risk management will support informed purchase decisions from a supply chain cyber security perspective.

Organization of Criteria

The NATF Criteria is provided on a spreadsheet that contains several tabs:

- Confidentiality (also contains versioning information)
- Version 0 Information
- Organizational Information
- Supplier Criteria
- Acronyms and Definitions

Confidentiality

The confidentiality tab provides distribution restrictions per the NATF membership. It also provides versioning information, dates that specific versions became effective, and any notes associated with each version.

Version 0 Information

The version 0 tab provides specific points of information associated with the initial posting of the criteria.

Organizational Information

Organizational Information provides questions about suppliers that entities would benefit from knowing prior to starting a process to purchase from the supplier. It includes questions regarding a supplier's adherence to existing cyber security frameworks, which provides information about a supplier's cyber security practices in general, i.e. information regarding a supplier's cyber security practices broader than the industry specific criteria

[1] *NATF Cyber Security Supply Chain Risk Management Guidance,* version 1.0, PP 8-10 (June 2018).
[2] NERC CIP-013 R1 supply chain cyber security risk management plan(s) and other entity cyber security supply chain risk management plans.

on the next tab. This information is intended to supplement entities' purchasing teams' questions, questions contained in an entity's supplier on-boarding process, or an entity's initial questionnaire.

Supplier Criteria

The Supplier Criteria tab provides criteria to determine whether a supplier is conducting good security practices for the industry, and many are beyond what is required by the NERC supply chain standards.[3] Most are included in existing frameworks, but may contain an action that is more specific to the industry than what is required by the framework.

As this is criteria that is directly pertinent to supply chain cyber security for the BES, it does not encompass all good general cyber security actions. It would be important for an entity to understand if a supplier adheres to an existing cyber security framework(s) as a general practice. Whether or not the supplier adheres to an existing framework(s), and has third-party verifications conducted for that adherence, is included in the "Organizational Information" questions.

This tab of the spreadsheet maps the criteria to three existing frameworks as examples on how to determine whether an existing framework addresses the criteria. A supplier may use another existing framework, and an entity can use the spreadsheet as a tool to determine whether the framework encompasses the criteria.

As discussed below, there are several approaches an entity can take in considering a supplier's performance to an existing framework and to the Supplier Criteria.

Acronyms and Information

The acronyms and information tab provide definitions or explanations for terms used in the spreadsheet.

Application of the NATF Criteria

An entity may choose to require all suppliers it purchases BES products or services from to meet all of the NATF Criteria or it may determine to evaluate which criteria each of their suppliers needs to meet based the inherent risks of the entity and the product or service being purchased. Further, once an entity has determined which approach to use, it will then need to determine the level of assurance of the supplier's adherence to those criteria that it needs to acquire. These concepts will be explored further in future NATF supply chain projects.

BES Suppliers Meet All Criteria

In the first approach, where an entity has determined that all suppliers providing products or services for the BES must meet all of the NATF Criteria, some suppliers may be challenged to meet those high security practices. However, for the entity, because all products and services supplied have met that bar as well as the other considerations in the entity's cyber security supply chain risk management plan(s), there would be less need for risk documentation and, from a cyber security supply chain perspective, products or services may be interchangeable throughout the entity's system.

BES Suppliers Meet Criteria Based on Risk

In the second approach, where all suppliers providing products or services for the BES meet the criteria deemed necessary due to the combined risk of the entity and the product or service, entities have the ability to evaluate

[3] NERC Reliability Standard CIP-013-1 and modifications to Reliability Standards CIP-005-6 and CIP-010-3, have become known collectively as the "Supply Chain Standards". FERC approved the Supply Chain Standards on October 18, 2018. *See* Order No. 850, *Supply Chain Risk Management Reliability Standards*, 165 FERC ¶ 61,020, at P 30 (2018) ("Order No. 850").

suppliers' performance to each of the risk criteria and determine whether the suppliers' performance is acceptable or if not, whether the entity is willing to mitigate the supplier's cyber security supply chain risk. This approach provides entities with more flexibility as to which suppliers they purchase from. However, it also creates the need for to entities to document its risk determinations. Specifically, entities would want to develop a process for determining which criteria are necessary, capturing the supplier risk assessment results, its acceptance or rejection of the risk, and appropriate review/approval of the review effort. As a result of using this approach, products and services may not be interchangeable throughout the entity's system. For good security practices, the entity would want to track which products or services may be used for specific purposes and locations on its system. Further, the entity may be required to provide its documentation to support CIP-013-1 R1.1.

More information

The Guidance document provides a discussion[4] on various approaches an entity may take to develop its cyber security supply chain risk management strategy.[5] Four approaches are discussed – an Enterprise Strategy, a Supplier Strategy, an Asset Type Strategy, and a Hybrid Strategy.[6] Whichever approach an entity opts to use, the cyber security supply chain risk management plan(s) must be aligned with the entity's overall risk profile. Simply stated, each entity plan(s) considers the risk to the entity for the specific hardware, software, or services being acquired or used and is aligned to the entity's risk tolerance and cyber security policy. While considering appropriate risk exposure for the hardware, software, or service acquired, the entity considers specific cyber security criteria and known security frameworks implemented by the vendor.

Modifications or Updates to the NATF Criteria

As the criteria is used, additional insight or comments may be generated. The NATF Supply Chain Criteria team will continue to meet to review comments and a process will be developed to determine whether the criteria should be modified.

The findings and determinations from future projects may have an impact on the approaches listed above, in the Guidance document, and also in other NATF documents. These documents will either be modified or archived as determined appropriate based on the findings.

Sources for Additional Information

- The NATF Cyber Security Supply Chain Criteria for Suppliers Version 0
- NATF Cyber Security Supply Chain Risk Management Guidance
  - Available on the NATF website and the NERC website
- NATF CIP-013-1 Implementation Guidance
  - Available on the NATF website and the NERC website

[4] The Guidance document may be modified as more projects are completed related to cyber security supply chain risk management. "This is a dynamic and living document. The current content reflects a collection of best-practice inputs from NATF members. The challenges that C-SCRM aims to address will continue to evolve. The NATF intends that this document will help utilities assess and address cyber security supply chain risks and document evolving practices. We invite collaboration to promote supply chain risk management practices that promote Bulk Electric System reliability and resiliency." *Id.* at 7.

[5] *Id.* at 9-11.

[6] *Id.* at 9.