North American Transmission FORUM

Community Confidentiality Candor Commitment

Revision Process for the Energy Sector Supply Chain Risk Questionnaire and NATF Cyber Security Criteria for Suppliers

Version ~~1~~2.0
Document ID: 1304
Approval Date: ~~09/11/2020~~TBD

Versioning

Revision History

Version	Date	Description of Revision/Change
1.0	09/11/2020	Initial version
2.0 DRAFT	TBD	Added process step for notification of changes to ERO

Review and Update Requirements

- Review: every 3 years
- Update: as necessary

Contents

Introduction

Purpose

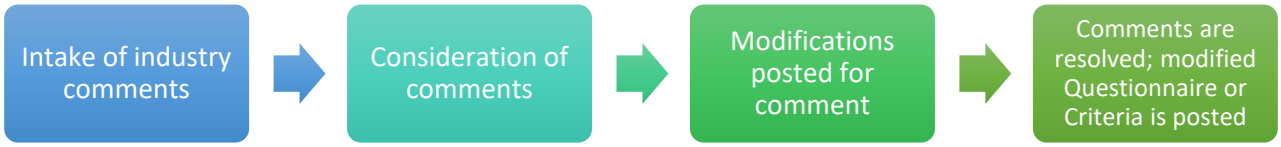
The purpose of this process is to facilitate the periodic reviews and modifications of the NATF Energy Sector Supply Chain Risk Questionnaire (Questionnaire) and the NATF Cyber Security Criteria for Suppliers (Criteria).[1] These living documents were developed for industry-wide use to drive consistency of information obtained from suppliers of bulk power system hardware, software and services.

Scope/Applicability

This procedure covers modifications and maintenance of the NATF Questionnaire and Criteria. Modifications are made with consideration of input from across industry and includes adding, deleting, or modifying individual questions in the 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.

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

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, suppliers, assessors, and other industry organizations (hereinafter "stakeholders"). 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 Questionnaire and the Criteria is to provide a consistent set of questions for entities to ask suppliers, it is optimal that the Questionnaire and the Criteria 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 supplier risks is being obtained
- Providing mapping to helpful security frameworks

Modifications to the NATF Questionnaire and Criteria 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. Entities will have 30 days to review and provide comments. Comments and concerns will be reviewed and addressed by the review team with assistance as needed from an advisory team. The revised Questionnaire and Criteria will be posted in May and communication (via a webinar or other form, as determined by the reviewed team) will be provided to industry.

Composition of the Review Team and Advisory Team

The review team consists of members from across industry, including members from the original development teams of the Questionnaire and Criteria. The number of organizations on the review team is not to exceed 25, although one organization may have more than one person attending. Active participation is required for a member to remain on the review team.

The review team will inform or consult with (at their option and depending upon the nature of the change determinations at issue) an advisory team and, as necessary, the Industry Organizations Team[2]. The advisory

[2] The Industry Organizations Team consists of representatives from industry trade organizations, forums, suppliers, third-party assessors and solution providers. Information on the Industry Organizations Team and its activities can be located on the NATF public website at: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

team is composed of additional members from the original development teams and the Industry Organizations Team. The advisory team is also not limited in the number of organizations or people that may participate, but active contribution is expected for a member to remain on the advisory team.

Industry Input

All industry input should be provided to NATF through supplychain@natf.net. Industry stakeholders are encouraged to provide any input that would reflect what information from the Questionnaire or Criteria they are using in their risk assessment or that they believe would be helpful in converging industry. Some specific examples of input include:

- Are the responses to all of the questions being considered in the risk assessment?
- Are some questions being used in the document more than others?
- Are there any questions that are not needed?
- Do any of the questions need modification?
- Are there any topic areas that are missing?
- Are the Criteria effective for measurement?

Consideration of Input and Modification of Questionnaire or Criteria

The Questionnaire and Criteria will be reviewed and updated annually in May as needed. Although the cadence for making changes is annual and mid-year changes are discouraged, if a change is one that should be made and the need for the change is urgent, or where the review team determines the change would be helpful to industry stakeholders, changes can be made at any time though out the year.

The review team will convene monthly to review any input received in the prior month~~,~~ and will conduct the annual reviews of the Questionnaire and Criteria in the January/February timeframe for potential updates and improvement opportunities.

Monthly reviews: The review team will meet once a month as needed to review industry inputs/suggestions for change and will decide whether the change should be made immediately or considered in the annual review.

Considerations for making change will include, but are not limited to:

- How urgent is the request?
- Should the change be made immediately or considered in the annual review?
- How broad is the request, i.e., how many industry entities would like to see the change?
- Could a current question be reworded/expanded to capture the concern?
- Does the question address an issue that supports a broader subsector (e.g., the gas industry)?
- Can a question be worded more generically to be applicable across subsectors?

The objective for the review team is to not increase the number of questions in the Questionnaire or, if possible, to reduce the number of questions while still capturing information needed to conduct risk assessments (not limited to compliance) and to add mappings to frameworks that the review and advisory teams determine are useful to a significant portion of entities.

Annual reviews: Any suggested changes that were not made throughout the course of the year but were deemed possible changes to make are reviewed by the review team during the annual review. The annual reviews will take place in the January/February timeframe.

Post review actions: After making their initial determination, both for the monthly determinations and the annual reviews, the review team will send a communication to the advisory team informing them of the review team's determination(s) and request, as needed based on the nature of the determinations, input from the advisory team.

Finally, the review team's determinations will be provided to the Industry Organization team for information and a high-level review for any fatal flaws.

Timing for Annual~~Updating~~ Updates to the Questionnaire

Once the review team has determined what changes, if any, should be made to the Questionnaire and Criteria through the review process~~, if any~~, the changes will be posted in a red-lined version of each document in early March for industry comments.

A notification of changes, if any, will also be sent to the Electric Reliability Organization (ERO) Enterprise as specified in the ERO Enterprise Endorsed Implementation Guidance for CIP-013 documents: NATF CIP-013 Implementation Guidance: Supply Chain Risk Management Plans and NATF CIP-013 Implementation Guidance: Using Independent Assessments of Vendors for comments and concerns that would jeopardize continued ERO Enterprise endorsement.

Entities and the ERO Enterprise will inform the review team if they have any comments or concerns within ~~have~~ 30 days ~~to review and provide comments~~. Comments and concerns, if any, will be reviewed and considered by the review team along with the advisory team and addressed, as necessary.

Finalizing Modifications: NATF Approvals and Communication to Industry Stakeholders

After the review team and the advisory team have reviewed and addressed any concerns raised by industry stakeholders in response to the posted redline, NATF will be asked to approve the modifications. This approval may be given by the NATF Board or the NATF CEO. In the event that the modifications are not approved, the process would be repeated, ~~-~~including reasons why it was not approved.

Finally, the revised Questionnaire and Criteria will be posted in May and communication or webinar, as determined necessary or helpful by the reviewed team, will be provided to industry.