North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

To: NERC Board of Trustees (BOT)

From: Thomas J. Galloway, NATF President and CEO

Date: October 11, 2019

Subject: NATF Periodic Report to the NERC BOT (November 2019)

Attachments: NATF External Newsletter (October 2019)

The NATF interfaces with the industry as well as regulatory agencies on key reliability and resiliency topics to promote collaboration and continuous improvement. Some examples are highlighted below and two key topics (grid security emergencies and supply chain cyber security) are included in the attached October NATF external newsletter, which is also available on our public website: www.natf.net/news/newsletters.

Risk Mitigation

As reported previously, the NATF and NERC executed an updated memorandum of understanding in April 2019 to further advance collaboration and leverage respective and collective strengths to identify existing and emerging risks, prioritize actions, and implement mitigation strategies to advance the reliability, resilience, and security of the Bulk Power System. Based on recent discussions among NATF, NERC, and Regional Entity leadership, the NATF is pursuing mitigations for some priority emerging risks identified by the ERO, including facility ratings issues and supply chain cyber security risks.

Compliance Guidance Inputs

The NATF is noted as a "Pre-Qualified Organization" for developing ERO Implementation Guidance and has submitted a number of documents for endorsement. We have worked closely with NERC staff during the review process and appreciate the support provided.

We commend NERC for its recently issued survey ("Effectiveness and Enhancement Survey – Pre-Qualified Organizations and Standard Drafting Teams") to allow organizations such as ours to submit feedback on the compliance guidance process, as well as the survey to industry users on effectiveness and enhancement of the compliance guidance program. The NATF submitted inputs, and we look forward to continue working together on this important and beneficial initiative.

Open Distribution

North American Transmission Forum External Newsletter

October 2019

NATF Grid Security Emergency Work

Section 215A of the Federal Power Act, added via amendment by section 61003 of Public Law 114-94 (the Fixing America's Surface Transportation Act or "FAST Act"), gives the Secretary of Energy certain authorities to issue an emergency order following the President's written declaration of a "grid security emergency" (GSE) as defined in the statute:

> *The term 'grid security emergency' means the occurrence or imminent danger of—(A). . . a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event . . . and . . . disruption of the operation of such devices or networks, with significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure, as a result of such act or event; or (B) . . . a direct physical attack on critical electric infrastructure or on defense critical electric infrastructure; and . . . significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure as a result of such physical attack.*

The NATF Grid Security Emergency Team has been working on inputs to the Electricity Subsector Coordinating Council (ESSC) Steering Group and U.S. Department of Energy (DOE) related to GSEs. Topics include:

- Communication between the DOE and the electricity subsector after the declaration of a GSE
- Generation of a framework document detailing key GSE principles
- Families of prospective operational orders and pilot orders on specific topics
- Prospective waivers and other regulatory relief deemed beneficial during a GSE

In 2018, the team completed a document to address the geomagnetic disturbance (GMD) threat noted in the definition above. In 2019, the NATF team—supplemented by representatives of the DOE, National Security Council, NERC E-ISAC, and the Edison Electric Institute—completed an update to the report incorporating the other three threats (physical security, cyber security, and EMP) and recommending additional work on communications protocols.

The ESCC is leading a working group to develop form orders[1] to be used in the November 2019 GridEx V executive tabletop. This group will also work on an outline of the full set of form orders and associated decision-support tools to be developed in 2020. The NATF GSE team will serve as a key operational/technical resource in the development of these form orders. In addition, the team will be working with NERC and the DOE in 2020 on the implementation of communication protocols and capabilities, along with associated industry training.

[1] A form order would serve as a starting point for an actual order issued by the DOE secretary once the president declares a GSE

NATF Role in Mitigating Supply Chain Cyber Security Risks

Supply chain cyber security continues to receive much attention as a high-risk area, and NATF members are proactively developing solutions for entities in the industry to mitigate these risks. The NATF projects, both completed and in progress, as well as recommended products from other organizations, will assist members with tools for good cyber security practices as well as with compliance to the NERC supply chain reliability standards,[2] which become effective on July 1, 2020.

As the appropriate industry organization to develop leading practices for reliability, security, and resilience, the NATF has taken several actions to assist members with cyber security supply chain risk management, including implementation of the NERC Reliability Standards. The topic is complex, however, with many interrelated issues that affect entities, and is being addressed simultaneously by many organizations. To ensure NATF members have access to the most effective and efficient solutions, the NATF is developing solutions within the membership, determining which of those solutions provide maximum benefit to members by being shared openly, and collaborating with other industry segments that are also working to resolve security concerns.

NATF Guidance

In 2018, the NATF produced the "NATF Cyber Security Supply Chain Risk Management Guidance" (Management Guidance) and the "NATF CIP-013 Implementation Guidance" (Implementation Guidance). The Management Guidance describes best and leading practices for establishing and implementing a cyber security supply chain risk management plan, including procurement, specification, vendor requirements, and managing existing equipment activities.[3] The Implementation Guidance, which has been endorsed by the ERO as an acceptable example of how to meet compliance with the reliability standard, describes one way that a registered entity could comply with CIP-013-1 Requirement R1 and, subsequently, CIP-013-1 Requirement R2. These documents were approved for open distribution (i.e., publicly available) and are posted on the NATF and NERC websites:

- 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

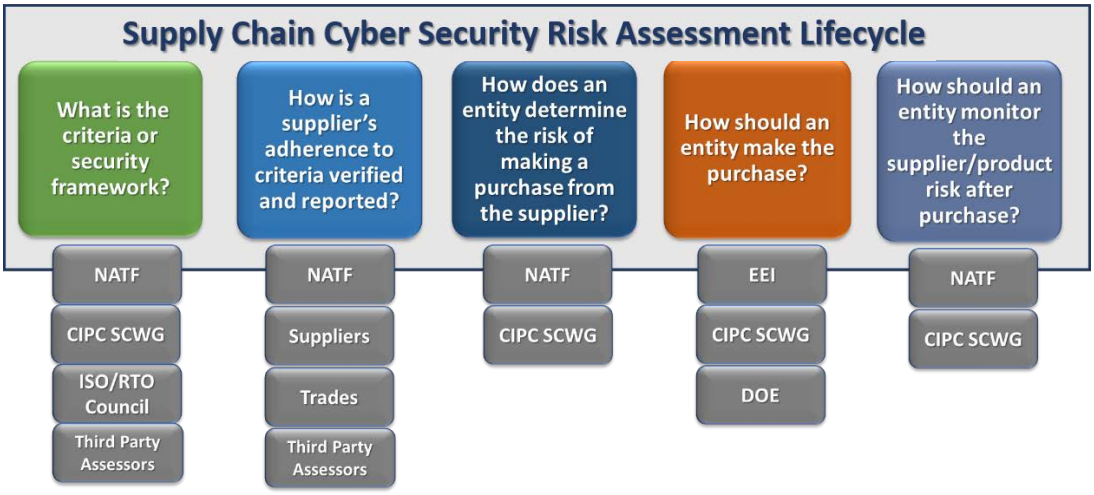
Products Mitigating Risk Throughout the Purchase Lifecycle

As the NATF began projects to support the concepts outlined in the Management Guidance document, members recognized projects being conducted by other organizations that addressed supply chain cyber security issues at various steps throughout the purchase lifecycle. As one example, the Edison Electric Institute (EEI) has developed (and posted publicly on its website) model procurement contract language that provides registered entities a consistent set of provisions to address CIP-013-1 security controls within their own respective

[2] In response to FERC's 2016 directive, NERC Reliability Standards Project 2016-03 Cyber Security Supply Chain Risk Management resulted in the development of the new Reliability Standard CIP-013-1 and modifications to Reliability Standards CIP-005-6 and CIP-010-3, which collectively have become known as the "supply chain standards." FERC approved the supply chain standards on October 18, 2018. Order No. 850, *Supply Chain Risk Management Reliability Standards*, 165 FERC ¶ 61,020, at P 30 (2018) ("Order No. 850").

[3] The Management Guidance document may be modified as more projects are completed related to cyber security supply chain risk management.

contractual forms. The model procurement contract language targets the processes required in CIP-013-1 Requirement R1.2 as well as supporting contract terms that address related information and data protection to strengthen cybersecurity overall. Legal, contracting, and compliance personnel from a number of NATF member companies contributed to the development of this product.



NATF members are also participating on the NERC Critical Infrastructure Protection Committee's (CIPC) Supply Chain Working Group teams to develop white papers that address various aspects of supply chain risks, and are continuing to work collaboratively with other organizations that are considering projects to address supply chain cyber security.

The NATF board and membership determined that NATF would be able to contribute to the industry's efforts by developing solutions in several areas throughout procurement lifecycle as shown in the illustration below.

NATF Supply Chain Cyber Security Criteria

Congruent with the overall NATF supply chain goals to achieve strong security assurance in an efficient and effective manner through convergence by industry on common approaches, NATF members approved NATF engagement and leadership in supply cyber security risk management through (1) the development and

implementation of cyber security criteria for suppliers and (2) a recommendation for NATF members to utilize the EEI procurement language as a basis for developing their own procurement language.

NATF member SMEs developed "NATF Cyber Security Supply Chain Criteria for Suppliers" (NATF Criteria) to assist entities in evaluating a supplier's cyber security supply chain risk. The NATF board determined that members have the potential to receive more benefit from sharing the NATF Criteria openly and voted to provide the criteria to industry, laying the foundation for streamlined cyber security solutions. The NATF Criteria are posted on the NATF's public website (www.natf.net/documents).

The NATF Criteria have also been provided to NERC and shared with the NERC CIPC. The NATF Criteria evaluates whether a supplier is conducting good cyber security practices for the industry, and many of the criteria are beyond what is required by the NERC supply chain standards. 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. A suppliers' performance to the NATF Criteria is an indication of a supplier's cyber security practices for Bulk Power System (BPS) / Bulk Electric System (BES) products or services, and a data input to an entity's risk analysis for the supplier,[4] which will support an entity's informed purchase decisions from a supply chain cyber security perspective.

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

Use of the NATF Criteria

As this is criteria that is directly pertinent to supply chain cyber security for the BPS/BES, it does not encompass all good general cyber security actions. It is important for an entity to understand if a supplier adheres to an existing cyber security framework or frameworks as a general practice. This consideration is included in the NATF Criteria.

Future NATF Supply Chain Projects

NATF members have approved the NATF to continue with several projects in a tiered approach:

Tier 1 – NATF Criteria and Proof of Concept Project

- Maintain criteria for supply chain products/services
- Conduct Proof of Concept project with EMS suppliers

Tier 2 – Common Reporting Format(s)

- Explore common format(s) to report a supplier's adherence to the NATF criteria
- Explore common response format(s) for initial supplier questionnaires

While the NATF cyber security supply chain projects have been developed to support supply chain cyber security, which is broader than what is required for NERC compliance, members (and the industry at large) have noted a need to have methods in place to determine supplier cyber security practices for supply chain prior to July 1, 2020, when the NERC supply chain Reliability Standards become enforceable. To meet that need, and to

[4] NERC CIP-013 R1 supply chain cyber security risk management plan(s) and other entity cyber security supply chain risk management plans.

give entities time to incorporate methods into their operating practices, the NATF is working to have solutions identified in the future projects developed by the end of 2019.

Proof of Concept Project

The initial Proof of Concept project will lay the foundation for, and grow into, the verification and common reporting projects:

- The verification project will evaluate the methods of verifying a supplier's adherence to criteria and the impact of a supplier's adherence to an existing cyber security framework.
- The common reporting project will investigate common reporting form(s) and whether common forms can streamline processes for entities, suppliers, auditors, and regulators.

The objective of the Proof of Concept project is to work with suppliers, third-party assessors/verifiers, and industry participants to brainstorm solutions that would enable entities in the electric industry to efficiently assess suppliers' cyber security controls and practices.

Impact of Future Projects

The findings and determinations from future projects may have an impact on the previously developed solutions in the guidance document and other NATF documents. These solutions and documents will either be modified or archived, as appropriate, based on the findings.

Workshops and Meetings

In addition to regular web conferences, NATF groups conduct periodic workshops and in-person meetings. Recent and upcoming activities include:

- Security Workshop (July)
- Operator Training (Train-the-Trainer) Workshop (August)
- Board and Members Meeting (September)
- Vegetation Management Workshop (October)
- Human Performance Improvement Workshop (October)
- EPM Substation Equipment and Asset Management Workshop (October)
- System Operations and Operations Tools Workshop (October)

Redacted Operating Experience Reports

Since our last newsletter, we have posted four reports to our public site for members and other utilities to use internally and share with their contractors to help improve safety, reliability, and resiliency.

***

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