North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

North American Transmission Forum Responses to The Department of Energy's Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure

VIA EMAIL
ElectricSystemEO@hq.doe.gov

June 7, 2021

The North American Transmission Forum (NATF) staff respectfully submits the following comments in response to the April 20, 2021, Department of Energy (DOE) request for information (RFI) on "Ensuring the Continued Security of the United States Critical Electric Infrastructure."

The NATF is uniquely positioned and prepared to assist in protecting the security, integrity, and reliability of the United States bulk power system through the elimination of compromises introduced through supply chains. Over the last several years, in collaboration with industry, suppliers, third-party assessors, and organizations that provide supporting products or services, the NATF has developed the "Supply Chain Security Assessment Model" (Model). The Model provides a strong framework for entities to identify, mitigate, and monitor supply chain risks. This is a streamlined, effective, and efficient industry-accepted approach for entities to evaluate supplier security practices. Any specific protections identified through DOE's efforts can be incorporated into the Model.

The Model has been endorsed by the NATF-led Industry Organizations Team[1] and, if applied widely, will create consistency in supplier information requests, provide entities with necessary information, and improve supply chain security. The tools contained in the Model, including the "NATF Supply Chain Security Criteria" (NATF Criteria) and the "Energy Subsector Supply Chain Risk Questionnaire" (Questionnaire), and supporting tools and services offered by other industry organizations and solution providers, provide critical information for entities to consider when conducting risk assessments for potential suppliers of products and services.

In addition to incorporating DOE solutions into the Model, the NATF can provide implementation support through four activities:

- Coordinating electric industry organizations, suppliers, and third-party assessors on supply chain initiatives and solutions.

[1] The NATF-led "Industry Organizations Team" includes representatives from energy industry trade organizations and forums, NATF member utility representatives, key electric sector suppliers, and third-party assessors. A list of participants on the Industry Organizations Team is located on the NATF public website at: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination/contributing-organizations.

- Providing entities that procure bulk-power system equipment with tools to obtain relevant information from suppliers.
- Obtaining detailed information or trends from NATF members and providing anonymized summaries.
- Working with members to identify and implement relevant superior practices.

The NATF staff offer the responses below to DOE's RFI. The responses are categorized by section. As overarching comments, the NATF recommends continued collaboration and coordination among governmental agencies and between the government and the private sector, measured use of clear prohibition orders if needed to address risks requiring immediate action, increased sharing of risk information identified by intelligence agencies, support for private sector collaboration (such as the NATF activities), and continued use of the existing regulatory framework.

Development of a Long-Term Strategy

The NATF staff recommends the development of a long-term strategy take into consideration the prevention of risks stemming from multiple sources, including immediate national security risks, such as those from foreign adversaries, as well as other supply chain risks, such as those driven by criminal activity. Further, the NATF encourages drawing upon the expertise of industry, suppliers, third-party assessors, and solution providers to develop or participate in the development of solutions and/or guidance.

The NATF staff proposes the following for the development of a long-term strategy.

Collaborate

1. **Collaborate with other agencies.** The NATF fully supports and applauds the DOE's collaboration and consultation with other agencies and recommends this continue to an even greater extent. Streamlined, unified information and direction across federal government branches and agencies would allow states, Indian Tribes, local government, industry, and suppliers to act in a cohesive manner. The NATF adopted this model for its supply chain security activities and has organized the Industry Organizations Team to bring the industry trade organizations and forums (electric and gas), suppliers, third-party assessors, and solution providers together to develop and share approaches to supply chain security.

2. **Collaborate with suppliers.** Suppliers are the first line of defense in identifying compromises. The DOE can encourage government-supplier-industry collaboration and provide funding for projects to assist suppliers, such as the playbook pilots now being conducted with the national labs. Suppliers will incur additional costs to implement additional security measures, and the DOE can consider national security funding for suppliers, especially small and medium suppliers. Additionally, some suppliers may not be as advanced in their cyber security postures, and the DOE can provide education, training, and other resources to assist suppliers' security maturation.

3. **Support existing collaboration mechanisms to create alignment.** Support existing industry efforts to define the information necessary to conduct a supply chain security assessment of a supplier, identify risks, determine where mitigation is possible, and monitor controls for mitigation. Continued alignment efforts, along with the increasing sophistication in technologies to detect compromises or mitigate risks, and the continued focus on controls and monitoring, will have a long-term effect of mitigating repetitive

or systemic risks as depicted by figure 1 below.

Figure 1. Vision for the Long-Term Benefits of Alignment

4. **Collaborate with regulators and work within existing regulatory mechanisms.** In lieu of prohibitions, as suggested below in item 6: *Communicate urgency*, utilize the risk-based assessment regime that is required by existing regulations and supported by several years of industry development to address supply chain risks.

Communicate

5. **Communicate identified risks.** Entities in the electric utility industry and suppliers do not have access to the intelligence agencies' knowledge. The DOE should communicate risks that the intelligence agencies have identified and determined require action from entities or suppliers. The DOE should work with prospective recipients of the information (industry, states, tribal, and local government) and potential issuers of the information to develop communication mechanisms.

6. **Communicate urgency.** Communicate whether the risk is (1) of an urgent nature, which may require issuance of a prohibition or executive order (or possibly a NERC Alert) to compel immediate action for national security; (2) such that communication of the risk would be sufficient to compel industry action until the risk can be addressed through the development of a reliability standard, or (3) such that entities could be educated on the risk and respond without the need for a reliability standard.

   The DOE saw evidence of industry and suppliers' desire for communication during the DOE webinars held for the 2020 RFI, as the attendance overwhelmed the webinar's capabilities.

   When determining and communicating the necessary urgency for actions, the DOE should consider entities' abilities to respond when required actions involve existing deployed equipment. Urgent actions for deployed equipment can create reliability risks and operational cost. It takes time to take deployed equipment out of service and replace with something that does not pose a risk. These issues are reduced when actions involve future procurements.

7. **Communicate risk parameters.** Provide sufficient information for risk-based implementation, either by equipment type, location, or facilities, or communicate that the risk is too substantive to allow for risk-based implementation.

Provide Resources – Tools and Funding

8. **Support private-governmental development of tools and resources**. Support the development of tools that support supply chain risk identification or detection.

    a. **A single repository for suppliers' security information**. Provide and fund a single location to house suppliers' security information, including supplier responses to the NATF Criteria and Questionnaire, third-party assessor verifications, prior audits conducted by supplier customers, and other risk information. The DOE should seek support from industry, suppliers, third-party assessors, and solution providers. The NATF could support this effort by continuing to identify and align industry on what information is needed to conduct risk assessments.

    b. **Supplier ratings.** Provide and maintain, in conjunction with the intelligence agencies, a list of suppliers that have been determined to be exemplary in supply chain security (whitelist) and, where applicable, a list of suppliers with known connections to nation-state adversaries or criminal supply chain activity (blacklist). The whitelist would not be an all-inclusive list that entities should use; rather, it would designate suppliers that have demonstrated superior security postures. Entities would be able to continue to conduct risk assessments and implement risk mitigations for suppliers of their choice. This information could be communicated via the mechanisms described in item 5: *Communicate identified risks* and be made available in the single repository. These "supplier ratings" would also be an initial consideration in the NATF Model prior to an entity conducting a risk assessment for a supplier.

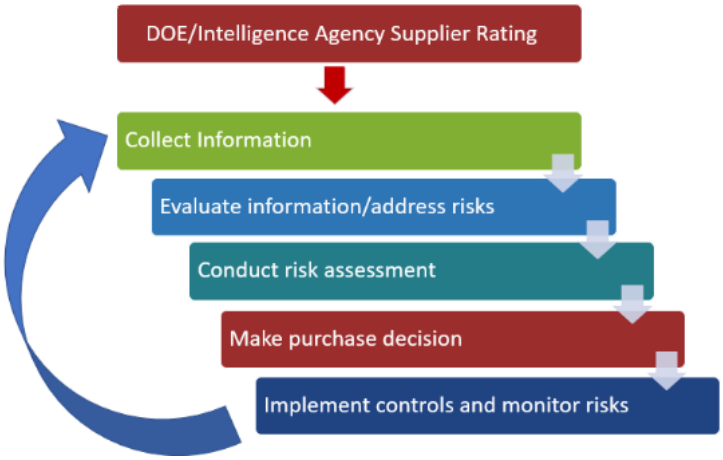

Figure 2. The NATF Model Steps with Supplier Ratings

    c. **Risk identification and risk assessment products.** Provide resources and funding to support the development of risk assessment products, such as supplier testing playbooks and bills of materials (BOMs), including digital, software, and hardware BOMs, as well as other efforts that can support risk identification.

9. **Cost recovery.** Where industry's response includes actions that will incur additional costs for an entity, including replacement of equipment already installed on the system or held in inventory, the DOE should work with state, tribal, and local governments to ensure time-sensitive cost recovery.

Prohibition Authority

The suspension of Executive Order 13920 *Executive Order on Securing the United States Bulk-Power System* and the revocation of the December 2020 prohibition order has provided an opportunity for an assessment of effective and practical ways to accomplish the security goals of the original order. In considering whether to issue a replacement prohibition order, the DOE can consider whether industry action to address the risks of supply chain compromise from foreign adversaries must be compelled by authority and whether industry has the ability to respond to such prohibition orders.

If it is determined that a replacement prohibition order is necessary to compel industry action or act as a signal of the criticality of the actions, the NATF staff proposes the following considerations for supply chain controls.

1. **Clarity of scope and responsibility (facilities and entities):** Orders or rules to implement supply chain controls need to clearly:
    a. *define which facilities are subject to those controls;*
    b. *specify which entities are responsible for applying the controls; and*
    c. *consider joint ownership of facilities.*

    When controls are to be applied to a subset of the electrical system, the implementation language should consider that facilities subject to the controls may be owned by more than one utility. Diverse ownership can create difficulty when the facilities are not identified through public, bright-line criteria.

2. **Clarity of scope (breadth).** The equipment types subject to supply chain controls should be clearly specified by the language of orders or rules that implement those controls.

    While language specifying primary equipment (e.g., transformers, breakers, reactors, and capacitors) is relatively easily to interpret, the meaning of such terms as "…software, firmware, and digital components that control the operation of Regulated equipment" is less clear.

3. **Clarity of scope (depth).** The types of equipment components subject to supply chain controls should be clearly specified by the language of orders or rules that implement those controls.

    Primary equipment of the types covered by EO 13920 is built by original equipment manufacturers (OEM) using components manufactured by the OEM and by others. Some components are complex electronic devices built using a variety of different types of sub-components. Sub-components vary in complexity from passive resistors and diodes to memory devices and processors. Terms like "digital components" leave room for interpretation as to the depth of the intended controls.

4. **Origin.** Orders or rules that implement supply chain controls need to specify how responsible utilities are to determine which persons and entities are of concern.

    It is possible to determine location of manufacture of equipment and apply supply chain controls as required. However, when equipment is manufactured outside an adversarial country, it may be difficult to discover relationships that could constitute prohibited ownership, control, or jurisdiction over persons or entities involved in the design, development, manufacture, or supply of equipment.

5. **Timing.** Orders or rules that implement supply chain controls should be clear as to the timing or status of equipment purchases that are subject to the controls.

Orders or rules that implement supply chain controls need to specify whether controls apply in the following situations:

- Purchases where contracts have been signed but transactions have not occurred.
- Situations when there are existing contracts for automatic periodic replenishment of equipment or components.

6. **Use of like-for-like replacements:** ***Orders or rules that implement supply chain controls need to be clear about the expectations for replacement of failed equipment and the use of inventory equipment.***

   Orders or rules that implement supply chain controls need to consider the potential reliability impact of restrictions on the replacement of failed equipment with identical or substantially similar equipment from existing "warehouse" spares or in-service equipment. For example, repairing equipment using existing spares may create little or no additional cyber risk when compared to the risk prior to the failure, while these repairs would avoid the reliability risks of leaving the equipment out of service.

7. **Cost recovery:** ***Orders or rules that implement supply chain controls need to provide a mechanism and funding for cost recovery.***

   As for long-term strategy, cost recovery should be considered for mandated actions. Orders or rules that implement supply chain controls need to acknowledge that responsible entities may seek to recover the cost of implementing these controls. Such costs may include, but are not limited to, internal costs of implementing and administering processes necessary to comply, external costs of ensuring that suppliers perform due diligence and provide certifications and evidence, costs of developing new sources of supply, or the cost of loss of use of assets due to restrictions that prevent the utility from implementing existing spares strategies for major equipment.

8. **Entity access to information:** ***Orders or rules that implement supply chain controls need to consider entities' ability to access information and the effectiveness of actions to identify and address risk.***

   Orders or rules that implement supply chain controls, such as those identified in EO 13920, should consider that responsible entities may have limited access to the information needed to comply, and suppliers may have difficulty providing this information. Rules that require suppliers to share information should consider the type and amount of information suppliers would share, the ability of responsible entities to analyze the information such that it is actionable, and the expected response.

The NATF appreciates the opportunity to provide comments on these issues. Over time, responsible entities, suppliers, and government could work together to determine effective ways to address supply chain risks. This may include sharing of data on foreign ownership, control, or influence, as well as entities' consideration of supplier controls and testing to mitigate risk. Solutions, whether in the form of a prohibition order or as part of the long-term strategy, should clearly meet the objective of reducing risk while considering the ability for responsible entities and suppliers to implement the solutions.

The NATF activities align with DOE's goals to protect national security. Given its unique position within the industry, the NATF is poised and available to support the implementation efforts. Thank you in advance for your consideration of these comments.

Respectfully submitted,

/s/ Thomas J. Galloway Sr.

Thomas J. Galloway Sr.
President and Chief Executive Officer
North American Transmission Forum
9115 Harris Corners Parkway, Suite 350
Charlotte, NC 28269