North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

North American Transmission Forum, Inc.
9115 Harris Corners Parkway, Suite 350
Charlotte, NC 28269
(704) 945-1900

November 1, 2020

Dear Supplier:

This letter will give you:

- An explanation of supply chain importance to national security and utilities
- How this affects suppliers and next steps
- Invitations to attend an informational webinar:

  Suppliers: Responding to Requests for Cyber Security Information

This message is a follow up to the letter posted in March 2019 by the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection Committee (CIPC) Chair and the CIPC Supply Chain Working Group Chair informing you of upcoming regulatory requirements on supply chain risks. These federal requirements (the NERC supply chain standards[1]) went into effect on October 1, 2020. As a result, and pursuant to other governmental actions, you have likely been receiving requests from your customers and from third-party solution providers (companies offering services including collection and analysis of supplier data) for information on your supply chain cyber security practices.

The electric and gas utility industries are requesting information from you regarding your cyber security practices your company provides, with specific emphasis on your cyber security practices related to supply chain and the country of origin for major components of products or services. Many of these requests may be unique, requiring time and resources from your company to respond.

These requests will continue. There is an effort underway to make the responses to these requests easier by aligning utilities[2] on what information they need to request from suppliers. This non-commercial (no cost), industry-based effort has been developed through the Industries Organizations Team organized by the North American Transmission Forum (NATF) to assist utilities and suppliers evaluate supply chain cyber security risks.

> ***The only "ask" from you, as a supplier to utilities, is to be prepared with responses to requests for information from your customers and solution providers, if you choose to work with these vendors.***

[1] North American Electric Reliability Corporation (NERC) Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 (Supply Chain Standards) address cyber security supply chain risk management issues.

[2] Throughout this letter, "utility" or "utilities" refers to companies in the electric and gas industries with a need to procure products or services

To assist with this request, you are invited to attend a webinar that will provide detailed information on this alignment effort and will offer an opportunity for Q&A. There are two opportunities to attend this webinar:

- **Tuesday, December 1, 1pm-2pm ET**
- **Tuesday, January 12, 1pm-2pm ET**

This webinar will include presentations from representatives of utilities, trade organizations and suppliers. There is no cost to attend. You can get more information on this webinar, including registration information, on the North American Transmission Forum (NATF) website at:

https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

Why Suppliers' Supply Chain Cyber Security Postures are at the Forefront Now

You are seeing these requests due to:

- The North American Electric Reliability Corporation's (NERC's)[3] reliability standard CIP-013-1[4] that became effective on October 1, 2020
- The White House Executive Order 13920 *Securing the United States Bulk-Power System* issued on May 1, 2020[5]
- The Department of Energy (DOE) a Request for Information (RFI) related to Executive Order 13920 *Securing the United States Bulk-Power System* issued on July 8, 2020[6]
- A NERC *Recommendation to Industry: Supply Chain Risk III* (NERC Alert) issued on July 8, 2020[7]

The NERC CIP-013 Reliability Standard[8], one of the NERC supply chain standards, is a regulation that requires utilities with BES Cyber Systems to have supply chain cyber security risk management plan(s) in place for high and medium BES Cyber Systems. The standard addresses identified aspects of cyber security, and carries potential fines if utilities are found to be noncompliant. However, beyond a compliance aspect, the standard, the Executive Order, and subsequent RFIs have raised utilities' awareness of the importance of knowing their suppliers' supply chain cyber security postures, not only for electric reliability but also for national security reasons.

The NATF and Industry Organizations' Effort

This effort to streamline utilities' evaluations of suppliers' supply chain cyber security practices is being led by the North American Transmission Forum (NATF) organized Industry Organizations Team. This is a group of industry organizations, led by NATF, that are working diligently to assist utilities responding to the risks that

[3] https://www.nerc.com/Pages/default.aspx
[4] https://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States
[5] https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/. Additional information can be found at https://www.energy.gov/oe/bulkpowersystemexecutiveorder
[6] https://www.energy.gov/oe/articles/doe-office-electricity-issues-request-information-bulk-power-system-executive-order
[7] https://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx
[8] NERC CIP-013-1 is available at https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-013-1&title=Cyber%20Security%20-%20Supply%20Chain%20Risk%20Management&jurisdiction=United%20States

have been identified by the Executive Order and NERC Reliability Standards. The team is comprised of representatives from Trade Organizations and Forums, utilities of various sizes and organizational structures, suppliers, third-party assessors, and solution providers. A list of participating organizations has been included for you. Of note are the suppliers that have been involved, which include Hitachi-ABB, GE Grid Software Solutions, OSI, Siemens, Schneider Electric, and Schweitzer Engineering and the third-party solution providers, which include Asset to Vendor Network (A2V), EPRI, and UL. You can locate more information on this effort on the NATF's website at https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

This effort creates an effective and efficient method for utilities to identify any risks that may arise from a supplier's supply chain cyber security practices and provides for an opportunity for the utility and supplier to implement mitigations for these risks. Mitigating activities could be done by the utility, the supplier, or – in some instances where the risk to the bulk-power system is minimal – the risk may be accepted. It is a solution that avoids identifying "acceptable" suppliers. This solution helps entities to identify and address risks while continuing to work with their preferred suppliers.

To align industry on what information is necessary for utilities to obtain from suppliers, a set of 60 Criteria and a complementary Questionnaire have been developed that utilities can provide to you when they request information. These are living documents and will be refined as utilities have more experience with what information they use in their supplier risk assessment. There is no obligation or cost to utilities or suppliers to use these tools, which can be located on the NATF public website. Use of these tools:

- benefits suppliers, as it can reduce the number of questionnaires and unique requests you are receiving, and you can develop responses for these criteria and questions and have them available to provide upon request, and
- benefits utilities, as they will be requesting information that they need and use when conducting risk assessments and they can receive the information in a short timeframe.

Third-party solution providers may also be offering services to support you in demonstrating your cyber security practices/posture to your customers. These companies offer a range of beneficial services to utilities, including gathering information from suppliers and, with permission from a supplier, sharing this information with utilities, saving you time in responding to individual requests and streamlining information sharing.

Suppliers' Role

We are reaching out to you to:

- Provide you with awareness that utilities may be asking for you to provide responses to the Criteria and Questionnaire
- Ask that you prepare responses to the Criteria and Questionnaire to support your customers and future customers
- Encourage industry alignment by having the responses readily available
- Request that you continue to assist in driving industry alignment on information that is needed for utilities to conduct supplier risk assessments

Remember to Register Today

December 1, 2020

January 12, 2021

Thank you in advance for your support and consideration. You can reach out to supplychain@natf.net with any questions, and we hope to see you on the webinar!

Sincerely,

The Industry Organizations Team
supplychain@natf.net

Contributing Organizations for the Industry Organizations Collaboration Effort

This communication and the webinars are brought to you by the representatives designated with an (*) on behalf of the NATF and the Industry Organizations Team.

American Gas Association (AGA)*

American Public Power Association (APPA)*
Asset to Vendor Network – AEP (A2V)*

Canadian Electricity Association (CEA)*

Con Edison Working Group (ConEd)

Deloitte

Edison Electric Institute (EEI)*

- EEI Supply Chain Working Group

Electric Power Research Institute (EPRI)
Ernst & Young, LLP

GE Power

Hitachi ABB Power Grids

Industry Representatives on ERO Enterprise Committees

- NERC Compliance and Certification Committee (CCC)
- Reliability and Security Technical Committee (RSTC)
- NERC Supply Chain Working Group (SCWG)*

ISO/RTO Council
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)

- NATF Supply Chain Steering Team*
  - AEP
  - Ameren
  - Exelon
  - Duke Energy
  - Nebraska Public Power District
  - PJM Interconnection
  - Southern Company Services

OSI

PricewaterhouseCoopers (PwC)

Schneider Electric

Schweitzer Engineering Laboratories, Inc.

Siemens Industry, Inc.

Transmission Access Policy Study Group (TAPS)

UL*