NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

March 6, 2019

Dear Electric Industry Vendor Community:

Re: Supply Chain Cyber Security Practices

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) directed the North American Electric Reliability Corporation (NERC) to develop or modify necessary Reliability Standards to address concerns that relate to supply chain risk management for industrial control system (ICS) hardware and software as well as computing and networking services associated with Bulk Electric System (BES) operations.[1] In October of 2018, FERC approved the Reliability Standards,[2] which will become effective on July 1, 2020.

This letter is intended to inform vendors to the electric utility industry of these new regulatory requirements and open a dialogue about the importance to electric utilities of working with their vendors to implement controls to manage supply chain security risks. Vendor products and services have a significant potential to impact the reliability of the BES. It is imperative that electric utilities work with their vendors to implement technical controls and processes to allow utilities to both meet their new regulatory obligations under NERC's Critical Infrastructure Protection (CIP) standards and to provide for a secure grid.

The electric utility industry is a vast ecosystem of asset owners, suppliers, service providers, stakeholders, and regulatory interests. Never before have we applied so much focus and efforts on security of the electric power grid and its related operations. The suppliers in this ecosystem play a crucial role by delivering innovative and reliable products and services that facilitate the reliable operation of the electric grid that we enjoy today. Without trusted suppliers working with asset (transmission and generation) owners and operators, the industry will struggle to increase or maintain reliability while directly addressing the ever-increasing security threats to the grid. Suppliers are working hard to address the concerns of supply chain security within the sector. This letter is to emphasize the need to continue that commitment as it will also help electric utilities address the new standards that require asset owners and operators to create and implement a supply chain risk management plan.

The electric utility industry is unique among the nation's critical infrastructure as the industry is subject to mandatory Reliability Standards, violations of which subject utilities to penalties. The Energy Policy Act of

[1] FERC Reliability Standard https://www.ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf , pg. 1
[2] NERC Reliability Standards CIP-013-1: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf; CIP-005-6: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-6.pdf; CIP-010-3: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-3.pdf

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

2005 granted FERC the authority to designate an Electric Reliability Organization, NERC, to develop and enforce mandatory Reliability Standards. Violations of Reliability Standards could lead to penalties and/or sanctions against entities, such as:

- Fines: $1000 to $1 million per day per violation
- Sanctions that impose limitations or restrictions on activities
- Remedial action directives designed to correct conditions, practices or other actions posing a threat to reliability

Facing significant penalties for noncompliance, electric utilities have developed compliance programs with reliability controls to ensure compliance obligations are met. As noted above, FERC approved a new standard requiring electric utilities to assess and mitigate supply chain risk. Regulated entities must evaluate the risk from their vendors and service providers prior to procuring certain products and services. Electric utilities must consider certain security issues in deciding which vendors and service providers to use so as to minimize their vulnerabilities to cyber security threats.

Similar to other industries, the electric utility industry is taking advantage of newer technologies from our vendors and service providers. As an example, in our not too distant past, we exclusively used mechanical relays to protect our transmission lines and generators. But these are being replaced by newer, faster relays providing better protection and much more information about the real-time operating system. Information in the past may have only been accessible at a remote substation and taken hours for a technician to physically drive a vehicle to the location. The same information today is now available within seconds. While the new technologies are more efficient and provide much better data, the new technology introduces cyber security risk from vulnerabilities and exploitation.

Suppliers, such as yourselves, have taken great strides to advance the security postures of their products and services. We have seen greater integration of intelligent features that facilitate automation and network connectivity. These efforts give our grid operations the flexibility to be deployed in many different models and achieve the efficient operation of utility grid and network operations. As such, we need the suppliers to continue to focus on the operational requirements that make their products viable and utility operations effective including cybersecurity controls. It is fundamental to the reliability and resiliency of utility operations that asset owners, asset operators and suppliers work together to address controls within their pervasive supply chains. Importantly, that work needs to efficiently mesh with the regulatory obligations utilities have with respect to the supply chain. Now it is time for the next step in this journey.

A strong partnership with suppliers is the only way to accomplish the task at hand. We want to maintain the innovation the suppliers have brought to the industry while integrating foundational cyber security controls into their products and services. Supply chain processes need to focus on ensuring that safe and reliable supply-side security concerns associated with technology integrations are addressed. This will require a level of cooperation and collaboration never before seen in our industry. Attached to this letter are examples of practices we encourage vendors to adopt and examples of practices that vendors should

consider discontinuing or minimizing, if possible. The items are provided as examples for your consideration and are not an all-inclusive list.

We are looking forward to addressing this challenge as a community, shoulder-to-shoulder with the suppliers, asset owners and operators, regulators, and stakeholders of the utility industry.

Sincerely,

Marc A. Child

Marc A. Child
Chair, Critical Infrastructure Protection Committee

Tony D. Eddleman

Tony D. Eddleman
Chair, CIPC Supply Chain Working Group

Attachment

Note: Examples provided below are not intended to be an all-inclusive list.

We encourage products and services that provide the following:

- Authoritative location of system updates, patches, executables, and or configuration files
- Digital signatures details - issued by, time/date signed and expiration date on all files (non-repudiation) - Provide hash codes for firmware and software application files
- Ability to provide traceability in the supply chain processes and supplier relationships (transparency - how can we determine the validity of the software and/or hardware)
- Delivered equipment is protected during transit by using tamper proof tape on packaging, seals on chassis hardware – secure transport
- Logging capabilities, vulnerability scan capability, Role Based Access Control (RBAC)
- Consideration for upgrades on equipment to maintain supported systems
- Technology considerations for open source and risk management - disclosure that it is embedded in systems
- Disclosure of system components from 3rd party manufacturers, including open source
- Secure Product Development Life-Cycle Process (Such as ISO27000 certification) or other supply chain certification
- Prompt notification of system or equipment compromises (examples provided below, but are not all inclusive)
  - Compromise of the Vendor's network that could have accessed a utility's system through a trusted connection
  - Compromise of a vendors trusted communication channels that may have been used to transmit malicious messages to a utility, such as phishing, vishing, or file transfer systems
  - Compromise of a vendors authorized remote access to a utilities network by a malicious actor
- Prompt notification of termination of a vendor employee who was granted access (physical or interactive) at the utility location
- Unique user name and password for remote access to systems
- Disclosure of known vulnerabilities in the system upon its delivery and mitigations applied or when patches will be provided for the vulnerability
- Disclose default accounts and passwords in the system
- Provide documentation baseline of ports and services with justification
- What, if any, programming/configuration accounts were used, and assurances they have been removed before the system is implemented at the utility

- What vulnerability assessments are used to assess the product or service, and provide the assessment findings
- Information on the systems logging capabilities, and capacity or methods to be scanned for vulnerabilities that will support ongoing detection of vulnerabilities
- Disclose use of 3rd party software libraries embedded in systems, including open source
- Maintain 3rd party software libraries embedded in systems with currently supported versions
- Clear designation as to whether a software update/patch is security related
  - Disclosure of the exact feature(s) affected by the vulnerability along with any mitigating measures
- Clear release date of security updates/patches
  - Clear indication of when the patch is made available to customers, not the internal release date

Action Item

We request suppliers review their practices in the following areas and discontinue or minimize, if possible:

- Hard coded or embedded passwords without the ability to change them and no complexity such as numbers only required
- Failing to secure backdoors to applications or systems after go-live
- Using unsupported systems without the ability to upgrade or patch