National Electrical Manufacturers Association

Representing Electrical and Medical
Imaging Equipment Manufacturers
www.nema.org

January 11, 2016

Sarah McKinley
Office of External Affairs
Federal Energy Regulatory Commission (FERC)
202-502-8368
sarah.mckinley@ferc.gov

Re: NEMA Remarks for the FERC Technical Conference on Critical Infrastructure Protection Supply Chain Risk Management (Docket No. RM15-14-000)

Dear Sarah,

Thank you for the opportunity to participate as a panelist at the Commission's staff-led Technical Conference on Critical Infrastructure Protection Supply Chain Risk Management occurring on January 28, 2016.

NEMA is the association of electrical equipment and medical imaging manufacturers, founded in 1926 and headquartered in Arlington, Virginia. Our nearly 400 member companies manufacture a diverse set of products including power transmission and distribution equipment, lighting systems, factory automation and control systems, and medical diagnostic imaging systems.

Attached please find NEMA's remarks addressing Panel 3 on the agenda: Current Supply Chain Risk Management Practices and Collaborative Efforts.

Thank you for the opportunity to provide this information. Should you have further questions, do not hesitate to contact me directly at steve.griffith@nema.org or 703.841.3297.

Sincerely,

Steve Griffith
Industry Director

Enclosure: NEMA Remarks for the FERC Technical Conference on Critical Infrastructure Protection Supply Chain Risk Management (Docket No. RM15-14-000)

Remarks of the National Electrical Manufacturers Association (NEMA)
Steve Griffith, Industry Director

FERC Technical Conference on Critical Infrastructure Protection Supply Chain Risk Management (Docket No. RM15-14-000)

Good Afternoon Members of the Commission Staff. Thank you for the opportunity to participate as a panelist at the Technical Conference on Critical Infrastructure Protection Supply Chain Risk Management. My name is Steve Griffith and I'm an Industry Director representing the National Electrical Manufacturers Association (NEMA).

The National Electrical Manufacturers Association (NEMA) is the association of electrical equipment and medical imaging manufacturers, founded in 1926 and headquartered in Arlington, Virginia. Our nearly 400 member companies manufacture a diverse set of products including power transmission and distribution equipment, lighting systems, factory automation and control systems, and medical diagnostic imaging systems.

NEMA and its member companies interface with several of the 16 critical infrastructure sectors, energy being one of them. NEMA understands that a focused effort of its member companies is essential to support this critical infrastructure essential to national and economic security.

As the manufacturers of critical grid equipment, NEMA and NEMA member companies play an important role in strengthening the cybersecurity of the electric sector supply chain. NEMA and its manufacturing members understand that a secure supply chain is essential to a secure grid and that cybersecurity aspects should be built into, not bolted onto, manufacturers' products. They also understand that managing cybersecurity supply chain risk requires a collaborative effort and open lines of communication among electric utility companies and the manufacturers of critical electric grid systems and components—both hardware and software.

The Edison Electric Institute (EEI) and NEMA began discussions on shared cybersecurity principles focusing on the supply chain back in 2012. Supply chain disruption and compromise is a major concern for the electric utility industry. EEI and its member utilities recognized that addressing this concern would require collaboration with NEMA and electrical manufacturers—the companies that supply products and services to the electric utilities. There was a general consensus between EEI and NEMA that we could work together to manage supply chain cybersecurity risk.

NEMA took a further step toward improving the supply chain security of our member manufacturers' products in 2015. As a Standards Developing

Organization (SDO) NEMA worked to identify guidelines that electrical equipment manufacturers can implement during product development to minimize the possibility that bugs, malware, viruses or other exploits can be used to negatively impact product operation. On June 25, 2015, NEMA published an industry consensus white paper on cybersecurity supply chain best practices for manufacturers, "CPSP 1-2015: Supply Chain Best Practices." The report is available online at http://www.nema.org/supply-chain-best-practices. The document was well-received by manufacturers, utilities, policymakers, and the general public.

The document addresses United States supply chain integrity through four phases of a product's life cycle:

- **Manufacturing**: An analysis during manufacturing and assembly to detect and eliminate anomalies in the embedded components of the product's supply chain;
- **Delivery:** Tamper-proofing to ensure that the configurations of the manufactured devices have not been altered between the production line and the operating environment;
- **Operation:** Ways that a manufactured device enables asset owners to comply with security requirements and necessities of the regulated environment (Security Development Life Cycle);
- **End-of-life:** Decommissioning and revocation processes to prevent compromised or obsolete devices from being used as a means to penetrate active security networks.

As opposed to being an all-inclusive document, it is a representation of identified best practices that vendors can implement as they develop, manufacture, and deliver products as part of the supply chain. Here are some example recommendations from the document itself:

- In the manufacturing and assembly phase of the product it is suggested that manufacturers follow a documented purchasing process that gives preference to procuring components from only the original component manufacturers or their authorized suppliers. Manufacturers should also have in place some type of industry-recognized incoming inspection technique in order to discover counterfeit components before they become physically integrated into a product.
- In the tamper-proofing phase of the product at minimum, manufacturers should be required to use some type of tamper-resistant coating or seal for all hardware components. At the Operating System (O/S) layer, manufacturers should consider using an O/S with minimal kernel features and reduced application sets. Making the kernel harder to manipulate increases the integrity of the O/S component.
- In the Security Development Lifecycle phase of the product, at minimum, manufacturers should test their products or devices in order to validate

compliance with the security requirements and necessities of the regulated environment. Depending on the environment, third-party testing might be required.

- In the Decommissioning & Revocation phase of the product, at minimum, manufacturers should use purging/sanitization techniques to remove sensitive data from a system or storage device with the intent that the purged data cannot be reconstructed by any known technique.

NEMA and NEMA Member companies recognize that supply chain cybersecurity risks are constantly evolving, and we want to thank FERC for hosting this very important technical conference. NEMA looks forward to working with and being a resource for FERC, NERC, utilities, and other interested stakeholders in addressing supply chain risks and concerns within the energy sector.