National Electrical Manufacturers Association

The Association of Electrical Equipment
and Medical Imaging Manufacturers
www.nema.org

January 19, 2018

Dr. Walter G. Copan
Undersecretary of Commerce for Standards and Technology
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland 20899

RE: Comments of the National Electrical Manufacturers Association on the NIST Cybersecurity Framework Draft 2, Version 1.1

Dear Dr. Copan,

Thank you for providing the opportunity to submit comments in response to the National Institute of Standards and Technologies' Cybersecurity Framework Draft 2, Version 1.1, ("the Framework"). On behalf of the National Electrical Manufacturers Association (NEMA) and the NEMA Cybersecurity Council, I am pleased to provide the following comments on improving supply chain cybersecurity. We encourage you to list the below-referenced resource in Version 1.1 of the Framework.

The National Electrical Manufacturers Association represents nearly 350 electrical equipment and medical imaging manufacturers at the forefront of electrical safety, reliability, and efficiency. Our combined industries account for 360,000 American jobs in more than 7,000 facilities covering every state. Our industry produces $106 billion of shipments of electrical equipment and medical imaging technologies per year with $36 billion in exports.

NEMA supports NIST in its decision to provide enhanced guidance for supply chain risk management in the latest version of the Framework. NEMA and its Member companies understand their important role in strengthening the cybersecurity of the supply chain. We understand that a secure supply chain is essential and that cybersecurity aspects should be built into, not bolted onto, manufacturer's products. NEMA also understands that managing cybersecurity supply chain risk requires a collaborative effort and open lines of communication, both with end users as well as upstream suppliers. Furthermore, we recognize that other organizations, such as the North American Electric Reliability Corporation, are developing cybersecurity supply chain guidelines; NEMA supports general alignment in this area.

As a standards developing organization, NEMA advanced the supply chain security of our Member manufacturers' products in 2015 by developing an industry consensus whitepaper on cybersecurity supply chain best practices for manufacturers, "CPSP 1-2015: Supply Chain Best Practices." This report is publicly available online at http://www.nema.org/Standards/Pages/Supply-Chain-Best-Practices.aspx.

The document addresses supply chain integrity through four phases of a products life cycle:

1. **Manufacturing:** An analysis during manufacturing and assembly to detect and eliminate anomalies in the embedded components of the products supply chain;

2. **Delivery:** Tamper-proofing to ensure that the configurations of the manufactured devices have not been altered between the production line and the operating environment;

3. **Operation**: Ways that a manufactured device enables asset owners to comply with security requirements and necessities of the regulated environment; and

4. **End-of-Life**: Decommissioning and revocation processes to prevent compromised or obsolete devices from being used as a means to penetrate active security networks

NEMA believes that "CPSP 1-2015: Supply Chain Best Practices" maps well to the Supply Chain Risk Management Category (IDC.SC) described in Table 2 of Appendix A and requests that it be listed as an informative reference in each of the five subcategories (ID.SC-1 thru SC-5).

We thank you for the opportunity to provide this information. Should you have further questions, please contact Steve Griffith, Industry Director, at 703.841.3297 or steve.griffith@nema.org.

Respectfully,

Kyle Pitsor
Vice President, Government Relations