NEMA

National Electrical Manufacturers Association

TESTIMONY OF

KYLE PITSOR
VICE PRESIDENT, GOVERNMENT RELATIONS
NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)

HEARING ON
DOE MODERNIZATION: LEGISLATION ADDRESSING
CYBERSECURITY AND EMERGENCY RESPONSE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON ENERGY

MARCH 14, 2018

SUMMARY OF TESTIMONY

Manufacturers are developing and following cybersecurity best practices. NEMA has published two industry-developed cybersecurity documents detailing best practices for electrical manufacturers, "NEMA CPSP 1-2015: Supply Chain Best Practices,"[1] and "NEMA CPSP 2-2018, Cyber Hygiene."[2] Government agencies should rely on industry-developed standards and documents, where available and applicable.

Government and private industry should work together to address security challenges. NEMA supports collaboration between the private sector and the Department of Energy, the National Institute of Standards and Technology, the Department of Homeland Security, and other federal and state agencies to promote cybersecurity best practices.

Electrical manufacturers support voluntary cybersecurity evaluation of products used in the transmission, distribution, storage, and end-use of electricity. Manufacturers and electricity companies should be involved in establishing the criteria for any such program via an open and transparent process.

NEMA supports the concepts included in the *Enhancing Grid Security through Public-Private Partnerships Act*. We encourage the Committee to broaden the list of outage indices in Section 4(b) to include Momentary Average Interruption Frequency Index (MAIFI), the average number of momentary power interruptions experienced by a utility customer in a given year. Momentary outages cost U.S. electricity customers $60 billion in 2014.

[1] Available online at http://www.nema.org/supply-chain-best-practices
[2] Available May 2018 at http://www.nema.org

Chairman Upton, Ranking Member Rush, and Members of the Subcommittee:

Thank you for the opportunity to testify in front of you today on such an important topic—the physical and cybersecurity of our nation's electric system.

My name is Kyle Pitsor, and I am the Vice President of Government Relations at the National Electrical Manufacturers Association (NEMA). NEMA is a trade association representing nearly 350 electrical equipment and medical imaging manufacturers that make safe, reliable, and efficient products and systems. Our combined industries account for 360,000 American jobs in more than 7,000 facilities covering every state. Our industry produces $106 billion shipments of electrical equipment and medical imaging technologies per year with $36 billion exports.

NEMA and its Member companies provide products and systems for use in several infrastructure sectors, energy being one of them. We understand that a focused effort by our manufacturers is required to support the electrical infrastructure essential to national and economic security. However, the responsibility for protecting our nation's electric grid must be shared among the private sector, end-users, and government agencies like the Department of Energy, Department of Homeland Security, and the Department of Commerce's National Institute of Standards and Technology.

NEMA and our Member manufacturers have made cybersecurity a top priority. As the manufacturers of essential grid equipment, NEMA companies are a key line of defense against both physical- and cyber-attacks on the electricity transmission and distribution system. We understand that a secure product supply chain is inherent to a secure grid, and that cybersecurity aspects should be built into, not bolted onto, manufacturers' products whenever possible. Manufacturers also understand that managing cybersecurity supply chain risk requires a collaborative effort and open lines of communication among electric utility companies, federal, state, and local governments, and the suppliers of the full spectrum of electric grid systems and components—both hardware and software.

I would like to mention briefly some of the industry-wide efforts NEMA and its Members have pursued to establish best practices for supply chain and manufacturers' cybersecurity hygiene. I will then make a few comments on the *Cyber Sense Act* (H.R. 5239) and the *Enhancing Grid Security through Public-Private Partnerships Act* (H.R. 5240) under consideration today.

Manufacturers are developing and following best practices

NEMA, as a standards development organization, has been discussing mutually shared cybersecurity principles with our partners in the electric utility industry for almost a decade. Supply chain disruption and compromise are major concerns for the electric utility industry, and both electric utilities and manufacturers recognize that addressing these concerns requires close collaboration.

Supply Chain Security

In 2015, the electrical industry took a step toward improving the supply chain security of manufacturers' products by publishing a technical best practices document that laid out the steps for securing supply chains. NEMA convened industry experts to identify technical guidelines that electrical equipment manufacturers can implement during product development to minimize the possibility that bugs, malware, viruses or other exploits could be used to negatively impact product operation. On June 25, 2015, NEMA published a white paper on cybersecurity supply chain best practices for manufacturers, “NEMA CPSP 1-2015: Supply Chain Best Practices.” The report is available online at http://www.nema.org/supply-chain-best-practices.

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

- **Manufacturing**: 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**: Methods by which a manufactured device enables asset owners to comply with security requirements and necessities of the regulated environment;
- **End-of-life**: Decommissioning and revocation processes to prevent compromised or obsolete devices from being used as a means to penetrate active security networks.

U.S. manufacturers are implementing the recommendations included in this report to protect their supply chains from, among other things, counterfeit, re-labeled, used, and grey market products that could cause security and safety risks.[3]

Cybersecurity Hygiene

On March 7, 2018, NEMA Members approved a new technical document, “NEMA CPSP 2-2018, Cyber Hygiene,” detailing industry best practice cyber hygiene principles for electrical manufacturers to implement in their manufacturing and engineering processes.[4] The guideline

[3] http://www.eaton.com/Eaton/ProductsServices/Electrical/ThoughtLeadership/Anti-Counterfeiting/index.htm#tabs-2

[4] This document will be published in May 2018, and will be available for download at www.nema.org

document addresses raising a manufacturer’s level of cybersecurity sophistication by following seven fundamental principles:

- **Segmenting networks**: Designing data networks that logically and/or physically separate manufacturing systems’ data flows from business or public networks;
- **Understanding data types and flows**: Understanding what data should flow through a network, where that data typically goes, and what or who should have access to it;
- **Monitoring devices and systems**: Providing the ability to monitor the health and security of devices and systems using existing, well-known, standard software protocols;
- **User management**: Restricting access to networks to only properly authenticated and authorized users;
- **Hardening devices**: Identifying potential threats and protecting hardware from unauthorized access (e.g., by removing unnecessary software from computers, encrypting confidential and sensitive data, etc.);
- **Updating devices**: Regularly patching and updating devices to protect against evolving vulnerabilities; and
- **Providing a recovery plan and/or escalation process**: Developing a plan to follow in the event that a vulnerability is identified, including incident detection and recording, classification and initial support, investigation and diagnosis, resolution and recovery, incident closure, monitoring the progress of the incident resolution, and a communication plan to inform affected parties about the status of the resolution.

Government and private industry should work together to address challenges

While industry is moving forward with a focus on cyber-security, there are opportunities for the private sector and government to work together.

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* is an example of a successful collaboration between industry and government to develop a voluntary, flexible framework to promote cybersecurity protection for multiple types of infrastructure, including the electric grid.[5] The NIST *Framework* should be referenced by the Department of Energy and other agencies as they work with private industry to promote cybersecurity best practices. It is important that the Department of Energy not reinvent or duplicate the tremendous work already accomplished by NIST; rather, DOE should collaborate with NIST to promote cybersecurity in the energy sector.

Electricity Information Sharing and Analysis Center (E-ISAC)

Another opportunity for public-private cooperation is to allow representation from electric grid equipment manufacturers as full participants in the Electricity Information Sharing and Analysis Center (E-ISAC), managed by the North American Electric Reliability Corporation. The E-ISAC is the principal information- and analysis-sharing gateway for the electricity industry.[6]

[5] https://www.nist.gov/cyberframework
[6] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf

Cyber Sense Act* and *Enhancing Grid Security through Public-Private Partnerships Act

With the above-mentioned industry-developed and -supported cybersecurity best practices in mind, I will make a few comments on two of the bills under consideration today—the *Cyber Sense Act* and the *Enhancing Grid Security through Public-Private Partnerships Act*.

Cyber Sense Act (H.R. 5239)

NEMA Member manufacturers support voluntary cybersecurity evaluation of products used in the transmission, distribution, storage, and end-use of electricity. Not doing so could permit unsecure equipment to be installed, potentially compromising the electric system. However, the specific requirements of any such program need to be carefully designed in close collaboration with manufacturers. We recommend that any cybersecurity evaluation program abide by the following principles:

- Evaluation procedures and requirements should be developed via an open and transparent process with sufficient opportunity for participation and input from the private sector, including electrical manufacturers and electric utilities;
- Electric grid product manufacturers and approved third-parties should be permitted to conduct Cyber Sense evaluation, in accordance with agreed upon evaluation procedures;
- Evaluation procedures and requirements should rely on industry-developed standards and best practices where available and applicable;
- Procedures should avoid reliance on "single point of time" evaluation as a primary determining factor, as the nature of these risks are constantly changing and the

previously described best practices outline continuously evolving system features that require continuous commissioning and patching;

- Sensitive information should be handled with appropriate care to prevent premature or unauthorized disclosure, including system attributes as well as the details of the specific evaluation requirements and information of the results beyond a summary; any disclosure of these types of details undermines the process by providing what could amount to a roadmap for entities attempting to negatively impact the system;
- The scope of the program should be clear and the products to be tested should be decided upon with industry participation;
- The program should account for how products are intended to be installed and operated (e.g., some products are intended to be installed behind layers of security, a concept referred to as “defense-in-depth,” and it would be inappropriate to test those products in the same manner as products that are intended to connect directly to the public internet);
- The program should account for the fact that once products are sold, manufacturers often don’t know where their products are put into use, how they have been installed, or how they are being operated; asset owners should maintain a system for tracking products;
- Upon the discovery of any vulnerability, manufacturers should be immediately notified and provided an opportunity review the findings and provide feedback to the Department of Energy;

Enhancing Grid Security through Public-Private Partnerships Act (H.R. 5240)

NEMA supports the concepts included in the *Enhancing Grid Security through Public-Private Partnerships Act*.

With respect to Section 2, "Program to Promote and Advance Physical Security and Cybersecurity of Electric Utilities," NEMA agrees that voluntary technical assistance efforts should be available to provide electric utilities with information and resources to effectively prepare for and combat both physical and cybersecurity threats. We also agree that this technical assistance should be provided in close collaboration with state governments and public utility regulatory commissions, as well as with equipment manufacturers. Including manufacturers in training and technical assistance efforts will ensure that products are installed and maintained as intended to limit the risk of a cyberattack resulting from possible improper use of a product.

NEMA also supports the recommendations included in Section 3, "Report on Cybersecurity and Distribution Systems," and Section 4, "Electricity Interruption Information." One additional outage index that should be included in Section 4(b) is Momentary Average Interruption Frequency Index (MAIFI). MAIFI is the average number of momentary (< 5 minutes) power interruptions experienced by a utility customer in a given year. Momentary outages cost U.S. electricity customers $60 billion in 2014, accounting for more than half the cost of all power outages.[7] Certain electrical equipment is sensitive to fluctuations in electricity voltage and frequency, which can cause significant disruptions for customers.[8] For example, some owners of distributed generation resources (like rooftop solar photovoltaic systems) have reported that their systems periodically shut off as a precaution when the system inverter senses

[7] http://grouper.ieee.org/groups/td/dist/sd/doc/2016-09-02%20LBNL%202016%20Updated%20Estimate-Nat%20Cost%20of%20Pwr%20Interruptions%20to%20Elec%20Custs-Joe%20Eto.pdf

[8] http://www.elp.com/articles/powergrid_international/print/volume-20/issue-6/features/utility-industry-targets-growing-concern-momentary-outages.html

voltage and frequency disruptions on the grid; while inverter manufacturers are working on systems that can safely “ride through” these disruptions, a better solution would be to decrease these momentary grid disruptions.[9,10] In industrial applications, momentary outages and voltage/frequency fluctuations can impact the performance of electric motors, necessitating the need to restart industrial processes, which results in expensive downtime. Additionally, with more people working from home, momentary outages are also having an impact on teleworkers; without the protection of an uninterruptible power supply, computers might shut down while teleworkers are editing documents, for example.

Conclusion

NEMA and NEMA Member companies recognize that cybersecurity risks are constantly evolving, and we want to thank the Committee for hosting this very important hearing. As you move forward in considering these bills, we urge you to ensure that manufacturers and electric utilities are consulted start-to-finish, and that industry best practices and standards are used wherever feasible. NEMA looks forward to working with and being a resource for the Committee as you continue your work to address cybersecurity concerns within the energy sector.

Thank you for your attention, and I look forward to answering any questions you might have concerning my testimony.

[9] https://www.ferc.gov/whats-new/comm-meet/2016/072116/E-11.pdf

[10] http://www3.dps.ny.gov/W/PSCWeb.nsf/96f0fec0b45a3c6485257688006a701a/def2bf0a236b946f85257f71006ac98e/$FILE/EPRI%20Fact%20Sheet.pdf