The association of electrical equipment
and medical imaging manufacturers
www.nema.org

National Electrical Manufacturers Association

June 7, 2021

Submitted via email to: ElectricSystemEO@hq.doe.gov

Michael Coe
Director, Energy Resilience Division of the Office of Electricity
U.S. Department of Energy
Mailstop OE-20, Room 8H-033
1000 Independence Avenue, SW
Washington, DC 20585

Re: Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure (86 Fed. Reg. 21309)

Dear Mr. Coe:

The National Electrical Manufacturers Association (NEMA) is the leading U.S. trade group representing electrical equipment and medical imaging manufacturers, which are at the forefront of electrical safety, reliability, and efficiency. Our nearly 325 Member companies provide a range of products used in buildings, industrial facilities and by utilities, transportation departments and hospitals. Collectively our membership provides some 370,000 American manufacturing jobs in more than 6,100 facilities, with worldwide industry sales exceeding $140 billion.[1]

On January 20, 2021, Executive Order 13990, "Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis" (E.O. 13990), suspended EO 13920 for 90 days and directed the Department of Energy (DOE or Department) to consider whether to recommend that a replacement Executive Order be issued. In response to the EO, in April 2021, DOE issued the "Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure."[2]

In the RFI, DOE states that the Department wishes to "appropriately balance national security, economic, and administrability considerations"[3] by seeking input from "electric utilities, academia, research laboratories, government agencies, and *other stakeholders* [emphasis added]."

[1] For more information, please visit: https://www.nema.org/.

[2] "Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure," 86 Fed. Reg. 21309 (April 22, 2021), https://www.federalregister.gov/documents/2021/04/22/2021-08482/notice-of-request-for-information-rfi-on-ensuring-the-continued-security-of-the-united-states.

[3] *Id.*

While we commend the DOE in its efforts to engage affected parties, NEMA must point out that despite our multiple past requests to be recognized as an essential part of this process, NEMA Member companies continue to fall into the "other stakeholders" category. We find it incomprehensible that NEMA Member companies have not been formally consulted as the Department considers new and effective measures to secure the grid, despite being the essential manufacturers of critical energy infrastructure that is produced for hundreds of North American utilities as well as other Department of Homeland Security-defined Critical Infrastructure Sectors, including Government Facilities and the Defense Industrial Base.

NEMA Members are longstanding and active manufacturers of many of the products comprising "bulk-power system electric equipment" as defined in Executive Order (EO) 13920,[4] including: capacitors, transformers and voltage regulators, metering equipment, reclosers and switchgear, protective relays, and substation safety and control systems.

To achieve the Department's stated goals to identify opportunities to "institutionalize change, increase awareness, and strengthen protections against high risk electric equipment transactions by foreign adversaries,"[5] DOE must provide better opportunities for NEMA Members, an essential part of the system, to have formal opportunities to provide input given the crucial importance of securing the U.S. electricity network.

Summary of NEMA Comments

1. DOE Must Establish a New Council
2. DOE Must Use Existing Standards
3. DOE Should Rely on NEMA Cybersecurity Supply Chain Practices
4. NEMA Responses to the RFI Questions

DOE Must Establish a New Council

NEMA urges DOE to establish a formal pathway for BPS equipment manufacturers to advise and exchange information with the US Government in matters related to security of the electric system, including procurement of electrical equipment. Such a pathway could be created through a new Cybersecurity and Infrastructure Security Agency (CISA) subsector coordinating council under the existing Energy Sector Council. The current charters for the Energy Sector Council and its Subsector Councils do not allow vendor and manufacturer participation.

DOE Must Use Existing Standards

DOE should integrate and rely upon preexisting sector specific efforts and industry Standards to the maximum extent practical in the development of any final rule. By leveraging these

[4] Executive Order 13920 issued May 1, 2020, titled ''Securing the United States Bulk-Power System,'' https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system

[5] "Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure," 86 Fed. Reg. 21309 (April 22, 2021), https://www.federalregister.gov/documents/2021/04/22/2021-08482/notice-of-request-for-information-rfi-on-ensuring-the-continued-security-of-the-united-states.

preexisting activities, a final rule will support an efficient compliance architecture and prevent unintended conflicts between the rule and already applicable efforts, technical Standards and certifications being used in the BPS market. Indeed, NEMA Members that manufacture equipment for the Bulk Power System follow all federally mandated cyber security Standards. In many cases, our Members have voluntarily adopted cyber security recommendations and/or guidelines from the Federal Government and/or Standards from independent Standards Development Organizations. Finally, our Members work closely with utilities who operate in the Bulk Power System to ensure that the equipment facilitates customer compliance with all applicable cyber security practices. While by no means complete, a brief list of these Standards, guidelines and recommendations are listed here:

- North American Electric Reliable Corporation Critical Infrastructure Protection (NERC CIP) Standards: These federally mandated Standards establish requirements for a broad spectrum of BPS utility operations and assets, ranging from security management (CIP-003-8 and CIP 007-6) to information protection (CIP-011-2). Recently, NERC published CIP-013-1 for Supply Chain Risk Management, which has relevance to Executive Order 13920. As first-tier suppliers to the Bulk Power System, NEMA Members play a primary role in their customers' supply chains and accordingly will play an integral part in compliance with these requirements.

- National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity: Created by way of response to Executive Order 1363, Improving Critical Infrastructure Cybersecurity, NIST developed this voluntary Framework of Standards, guidelines and practices to "foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders." Because the Framework is applicable beyond electric utilities, many NEMA Members have incorporated its principles into their own internal operating procedures.

    - NIST SP 800-82 "Guide to Industrial Control Systems Security": This document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

      A revision of this is currently being proposed to provide alignment to other relevant control system cybersecurity standards and recommended practices. Items being considered for this revision that are relevant include: an expansion of its scope to control systems in general, application of new cybersecurity capabilities in control system environments, and development of guidance specific to small and medium-sized control system owners and operators.

- NIST SP 800-53 Rev 5 "Security and Privacy Controls for Information Systems and Organizations": This document defines the Standards and guidelines for federal agencies to architect and manage their information security systems. It was established to provide guidance for the protection of agencies and citizen's private data and addresses diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines.

- NIST IR 8276 "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry": Although not a Standard, this document provides general guidance on cyber-related supply chain issues, including an extensive set of cyber supply chain risk management (C-SCRM) key guidelines that focus on processes, practices, and tools that have been adopted by industry.

- NIST Internal/Interagency Report (NISTIR) 7628 Guidelines for Smart Grid Cybersecurity: Presents an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their specific combinations of Smart Grid-related characteristics, risks, and vulnerabilities. It is applicable to utilities and their vendors.

- U.S. Department of Energy (DoE) Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) provides a mechanism that helps organizations evaluate, prioritize, and improve cybersecurity capabilities. A voluntary guide, ES-C2M2 allows implementing organizations to self-evaluate their cyber-security practices and track them against referenced industry best practices.

- DoE Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline is intended to enable utilities to apply effective and efficient risk management processes and tailor them to meet their organizational requirements.

- International Electrotechnical Commission (IEC)

    - IEC 62443: A series of Standards including technical reports to secure Industrial Automation and Control Systems (IACS). It provides a systematic and practical approach to cybersecurity for industrial control systems. These Standards provide a flexible framework to address and mitigate security vulnerabilities in IACSs. Every stage and aspect of cybersecurity is covered, from risk assessment through operations.

    - IEC 62351: Is the current Standard for security in energy management systems and associated data exchange. It describes measures to comply with the four major requirements for secure data communications and data processing: confidentiality, data integrity, authentication, and non-repudiation.

- International Organization for Standardization (ISO)
    - ISO/IEC 15408: Establishes the general concepts and principles of IT security evaluation.
    - ISO 20071 Information Security Management: This is a specification for an information security management system which provides "a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system."
    - ISO 27002 "Information technology - Security techniques": Code of practice for information security controls describes a comprehensive set of information security control objectives and generally accepted security controls to obtain them.
    - ISO/IEC 27019:2017 "Information Technology - Security Techniques - Information Security Controls For The Energy Utility Industry": Provides guidance based on ISO/IEC 27002:2013 applied to process control systems used by the energy utility industry for controlling and monitoring the production or generation, transmission, storage and distribution of electric power, gas, oil and heat, and for the control of associated supporting processes.

The above list comprises an indication of the measures BPS equipment suppliers already undertake. Any further regulations stemming from the EO should strive to fully utilize these existing Standards, guidelines, and recommendations.

DOE Should Rely on NEMA Cybersecurity Supply Chain Practices

In addition to existing sector specific efforts and industry Standards, DOE should consider whether and to what extent the work that NEMA Members have already done with respect to industry cybersecurity supply chain best practices can be utilized in the development of any rule. As manufacturers of BPS equipment, NEMA Member companies play an indispensable role in strengthening the cybersecurity of the electric sector supply chain. The below documents comprise a series of viable recommendations for all BPS equipment manufacturers to ensure that cybersecurity is built into, not bolted onto, their equipment. Managing cybersecurity supply chain risk requires a collaborative effort and open lines of communication among BPS owners and operators, the manufacturers of electric grid systems and components—both hardware and software—and the US Government. To that end, NEMA would welcome an opportunity to discuss further how the principles and practices outlined in these documents might inform DOE deliberations.

Two specific examples of NEMA best practice documents (supply chain and cyber hygiene) are provided below.

Supply Chain Best Practices. NEMA CPSP 1-2021

"Supply Chain Best Practices. NEMA CPSP 1-2021" is a document that identifies a recommended set of best practices and 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."[6] The document addresses US supply chain integrity through four phases of a product's life cycle:

1. Manufacturing: An analysis during manufacturing and assembly to detect and eliminate anomalies in the embedded components of the product's 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. Operational Compliance: 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 to penetrate active security networks.

This document is representative of identified best practices that vendors can implement as they develop, manufacture, and deliver products as part of the supply chain. Here are some examples of recommendations from the document itself:

- In the manufacturing and assembly phase of the product manufacturers should 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 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 operational compliance phase of the product, at minimum, manufacturers should test their products or devices at a regular frequency to validate compliance with the security requirements and necessities of the regulated environment. Depending on the environment, testing via an independent in-house party or even an external accredited testing lab is a best practice.

[6] Supply Chain Best Practices (NEMA CPSP 1-2021), https://www.nema.org/standards/view/supply-chain-best-practices.

- In the decommissioning and revocation phase of the product, at minimum, manufacturers should use purging and 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 method.

As counterfeit components are often included in the discussions with securing the supply chain, the document also provides practical recommendations on how manufacturers should:

- Follow a documented purchasing process that gives preference to procuring components from only the original component manufacturers or their authorized suppliers.

- Have in place some type of industry-recognized incoming inspection technique to discover counterfeit components before they become physically integrated into a product.

- Have a system in place to track disposition of components if counterfeit detection occurs after a device has been shipped to facilitate a recall.

Cyber Hygiene Best Practices

With the trend of interconnected BPS equipment and systems that NEMA Members manufacture, NEMA also published two companion Cyber Hygiene Best Practice documents. These best practices are applicable to manufacturing facilities and engineering processes (CPSP 2- 2018 "Cyber Hygiene Best Practices), and how end-users and customers can work with their respective manufacturers to improve the customer's level of cybersecurity (CPSP 3-2019 "Cyber Hygiene Best Practices Part 2") The cyber hygiene guidelines described in the documents focus on people, processes, and products and follow seven fundamental principles:

1. Segmenting networks: A principle that focuses on the practice of splitting a computer network into sub-networks (also called zones), each being its own network segment. This provides the capability to segment zones with differing security requirements.

2. Understanding data types and flow: A principle that focuses on understanding the applications and network protocols being deployed within a product.

3. Monitoring devices and systems: A principle that focuses on the capability to monitor devices and systems for potential security incidents or anomalies.

4. User management: A principle that provides user management capabilities to intelligently control access to their computer networks. Typically covers the following four areas: administration, authentication, authorization, and audit.

5. Hardening devices: A principle that focuses on techniques to eliminate vulnerabilities and disabling nonessential device-based services and capabilities.

6. Updating devices: A principle that focuses on procedures to patch devices when new vulnerabilities are discovered or the security requirements and needs of the operating environment change.

7. Providing a recovery plan and escalation process: A principle that focuses on providing a recovery plan/escalation process if a vulnerability is found on a device, unintended operational disruption, or if a security incident occurs in the network.

DOE Should Consider NEMA Responses to the RFI Questions

Please see NEMA Member responses to the DOE Request for Information[7] here:

<u>Question A-1</u>: What technical assistance would States, Indian Tribes, or units of local government need to enhance their security efforts relative to the electric system?

<u>Question A-2</u>: What specific additional actions could be taken by regulators to address the security of critical electric infrastructure and the incorporation of criteria for evaluating foreign ownership, control, and influence into supply chain risk management, and how can the Department of Energy best inform those actions?

<u>Question A-3</u>: What actions can the Department take to facilitate responsible and effective procurement practices by the private sector? What are the potential costs and benefits of those actions?

<u>Question A-4</u>: Are there particular criteria the Department could issue to inform utility procurement policies, state requirements, or FERC mandatory reliability standards to mitigate foreign ownership, control, and influence risks?

<u>NEMA Member Response to Questions A-1 Through A-4:</u>

Any actions the Department takes, or any assistance the Department provides, should be consistent with national standards described at length in these comments, including NEMA CPSP 1-2021 "Supply Chain Best Practices."[8]

NEMA Members support actions that mitigate foreign ownership, control, and influence (FOCI) in the supply chain. However, the guidelines for determining who is under FOCI are obtuse, subjective, and require intelligence assessments that are beyond the ability of manufacturers. We request the Department provide clarification and increased transparency in this area. DOE should inform stakeholders as to which sub-suppliers are under FOCI so that industry can take appropriate mitigation actions.

[7] "Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure," 86 Fed. Reg. 21309 (April 22, 2021), https://www.federalregister.gov/documents/2021/04/22/2021-08482/notice-of-request-for-information-rfi-on-ensuring-the-continued-security-of-the-united-states.

[8] Please see the "NEMA Cybersecurity Supply Chain Practices" section of these comments for more information.

Given that BPS vendors and manufacturers do not have access to intelligence agency information it is not clear they could assess FOCI mitigation for external third-party suppliers. DOE should model their program after export trade compliance lists that provide industry with very clear and implementable actions to take; like ensuring listed entities are not in their supply chain. Additionally, many BPS vendors and manufacturers are operating under existing trade agreements that are expected to be upheld.

On the incorporation of criteria for evaluating FOCI into supply chain risk management, the DOE should use caution when exploring such criteria. As utilities and manufacturers rely on a complex, global supply chain, we need to establish rules that mitigate foreign influence from specific actors and avoid rules that could harm allies upon which we rely. Where possible, such rules should avoid duplication with existing authorities and processes such as the Department of Commerce's efforts to mitigate threats to the information, communications, technology (ICT) supply chain and the Committee on Foreign Investment in the United States (CFIUS).

Question B-1:

To ensure the national security, should the Secretary seek to issue a Prohibition Order or other action that applies to equipment installed on parts of the electric distribution system, i.e., distribution equipment and facilities?

NEMA Member Response to Question B-1

NEMA Members do not support a full prohibition and instead urge DOE to make sure any actions taken are targeted and strategic. DOE avoid overreaching by extending the scope of any proposed executive order to include the full BPS. The DOE should work with industry to make sure it understands the scale and cost considerations associated with any proposed actions. NEMA urges DOE to limit scope of its actions to regulated equipment identified in the Prohibition Order:[9]

> Prohibition Order – Attachment 1, Regulated Equipment
>
> 1. Power transformers with low-side voltage rating of 69 kV or higher and associated control and protection systems such as load tap changers, cooling systems, and sudden pressure relays
> 2. GSU transformers with high-side voltage rating of 69 kV or higher and associated control and protection systems such as load tap changers, cooling system, and sudden pressure relays
> 3. Circuit breakers operating at 69 kV or higher
> 4. Reactive power equipment (Reactors and Capacitors) 69 kV or higher
> 5. Associated software and firmware installed in any equipment or used in the operation of items listed in 1 through 4.

[9] Please see "Attachment 1, Regulated Equipment" of Department of Energy Prohibition Order "Prohibition Order Securing Critical Defense Facilities," January 6, 2021, https://www.energy.gov/sites/prod/files/2020/12/f81/BPS%20EO%20Prohibition%20Order%20Securing%20Critical%20Defense%20Facilities%2012.17.20%20-%20SIGNED.pdf.

Even this list may be too broad for application beyond defense critical electric infrastructure (DCEI) as the previous Prohibition Order already produced a "chilling effect" on the industry, well beyond DCEI. Further expanding the scope will continue to imperil much needed grid investment at a time when manufacturers and the electric equipment supply chain are already facing disruptions due to the global pandemic and other factors.

It would be more impactful for DOE to provide an objective and transparent process for DOE to continuously assess threats to the bulk-power system and establish a process for issuing relevant mitigations actions or a listing of FOCI suppliers and entities to avoid. This process could include prohibition orders or binding operational directives (similar to those issued by the Cybersecurity and Infrastructure Security Agency (CISA) under their "Federal Information Security Modernization Act"[10] authorities).

NEMA recommends that the Department pursue a similar process to the one outlined in the "Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act"[11] that led to the creation of the "Federal Acquisition Security Council" (FASC),[12] which coordinates government-wide exclusion and removal orders to mitigate risks to the Federal government posed by certain products or vendors. The DOE should propose actions that are specific, implementable, and clear, using industry terms for clarity. Furthermore, costs should be mitigated by proposing forward-looking actions—no "rip-and-replace." Finally, adequate transition time must be provided to give stakeholders the time necessary to develop and implement new procedures.

To ensure the Department's next steps are effective and balanced, we urge DOE to consider our comments in the "Request for a Power Grid Equipment Manufacturer Subsector Coordinating Council (or Similar Platform)" section of these comments.

<u>Question B-2:</u>

In addition to DCEI, should the Secretary seek to issue a Prohibition Order or other action that covers electric infrastructure serving other critical infrastructure sectors including communications, emergency services, healthcare and public health, information technology, and transportation systems?

<u>NEMA Member Response to Question B-2</u>

NEMA Members caution against DOE taking such action at this time. In any regulatory action comparable to the original Prohibition Order (including implementing the original Prohibition Order), the key to success is clarity and communication with the regulated community.[13] This will give DOE the needed input and experience with DCEI before expanding further. Because

[10] https://www.congress.gov/bill/113th-congress/senate-bill/2521.

[11] https://www.congress.gov/bill/115th-congress/house-bill/7327/text.

[12] https://www.federalregister.gov/documents/2020/09/01/2020-18939/federal-acquisition-supply-chain-security-act.

[13] Please also see the "DOE Must Establish a New Council" section of these comments.

critical infrastructure is highly distributed and embedded in the electrical system, extending prohibitions to these sectors is essentially expanding the prohibitions to the entire electric grid. NEMA also believes that any actions taken should be targeted, strategic, and focused on high value mitigation actions. Expanding to all critical infrastructure essentially sweeps into scope innumerable pieces of electric grid equipment, many of which may not present vulnerabilities.

Question B-3:

In addition to critical infrastructure, should the Secretary seek to issue a Prohibition Order or other action that covers electric infrastructure enabling the national critical functions?

NEMA Member Response to Question B-3

NEMA Members caution DOE to make sure any actions taken are targeted and strategic and not try to overreach by extending the scope of any proposed executive order to include electric infrastructure enabling the national critical functions that are already governed by other federal agencies. The DOE should propose actions that are specific, implementable, and clear, using industry terms for clarity.

Also, NEMA Members request that DOE refer to our response to Question B-1.

Question B-4:

Are utilities sufficiently able to identify critical infrastructure within their service territory that would enable compliance with such requirements?

NEMA Member Response to Question B-4

NEMA Members believe this question should be left to the utilities. However, we welcome the opportunity to be a resource in this area.

Conclusion

We would like to request a meeting with you to discuss this matter further at your earliest possible convenience. Please contact Stacy Tatman (Stacy.Tatman@nema.org) to make arrangements.

Sincerely,

Philip Q. Squair

Philip Squair
Vice President, Government Relations