May 28, 2020

VIA EMAIL: bulkpowersystemeo@hq.doe.gov

Dear Sir/Madam:

Re: Executive Order 13920: "Securing the United States Bulk-Power System"

The National Electrical Manufacturers Association (NEMA) represents nearly 325 electrical equipment and medical imaging manufacturers that make safe, reliable, and efficient products and systems. The GridWise Alliance (GWA) represents the broad and diverse stakeholders that design, build, and operate the electric grid, including utilities, utilities, equipment manufacturers, vendors, and others, and since 2003, our members have been at the forefront of educating key industry stakeholders on the critical need to modernize our nation's electricity system.

NEMA Member companies, representing over 370,000 American manufacturing jobs, include 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 make many of the products comprising "bulk-power system electric equipment" as defined in EO 13920, including: capacitors, transformers and voltage regulators, metering equipment, reclosers and switchgear, protective relays, and substation safety and control systems.

Executive Order (EO) 13920 declares that potential vulnerabilities of the United States bulk-power system (BPS) are a "national emergency."[1] The EO has raised questions within the electroindustry that we hope to resolve with relevant government Departments and Agencies. As the companies that domestically manufacture many of the items addressed in this document, we have significant real-world experience that we believe would be integral to the U.S. Government effort to fashion solutions to the issues raised in the EO.

Attached are comments and questions related to the EO. NEMA Member companies count on your careful consideration and look forward to serving as a key resource as we work towards the common goal of securing the U.S. power grid. If you have any questions on these comments, please contact me or Stacy Tatman (703-841-3221 or stacy.tatman@nema.org).

Sincerely,

Philip Squair
Vice President, Government Relations

[1] https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system

Our Shared Commitment to National Security

NEMA Members are committed to the security and the integrity of the power grid and view us as an integral partner of U.S. Department of Energy (DOE) to help minimize any potential vulnerability to the U.S. bulk-power systems. The ambiguous nature of the EO text, however, causes confusion within the covered product manufacturing community. The purpose of this document is to express clearly the questions that have arisen and to offer the expertise of the electroindustry to the government in addressing this challenge.

Promulgation of Rules

As DOE works to implement the EO, we intend to be a partner with the Department to add industry depth of knowledge to technical matters. We strongly believe that any new regulation(s) will achieve intended outcome(s) only with strong up-front participation of the U.S. bulk-power system manufacturing base. As such, **we urge DOE to publish in the Federal Register a Request for Information (RFI)** and establish a process in advance of the issuance of any rule(s) in order to accomplish the following:

- Actively elicit and consider best practices used by industry (or have in development) to reduce overall cybersecurity risk and that may mitigate those risks associated with undue influence from national governments
- Actively solicit and discuss challenges, limitations, and gaps faced by power grid equipment manufacturers where DOE action may benefit from our collective ability to mitigate relevant risks (i.e., strategic transformer reserves and/or interconnection of Regional Transmission Organizations (RTO)/Independent System Operators (ISO) markets)
- Analyze collaboratively proposed actions and rules to reveal possible follow-on effects and unintended consequences

NEMA Members have developed the following preliminary list of specific questions:

- <u>Collaboration with the Manufacturing Community</u>

    - Will there be a formal RFI process and/or defined process to ensure that the voice of the U.S. bulk-power system manufacturing base is heard before proposed rule(s) is issued? If so, what is the planned timing and ground rules? (e.g. When will it start? Who will be allowed to participate? How many opportunities for input will participants have? What confidential business information (CBI) protections will be assured?)
    - Will DOE broaden the scope of the input beyond the Electricity Subsector Coordinating Council (ESCC) and Oil and Natural Gas Subsector Coordinating Council (ONG SCC) participants to ensure comprehensive input from additional affected entities across the entire supply chain?
    - When will DOE provide a timeline of planned implementation actions?

- Prequalification List

    - Will DOE confirm that the scope of this EO is limited only to electrical equipment rated at 69kV and above as has been asserted by the Department on various public briefings?
    - Is DOE considering a risk assessment process as pertains to products subject to the pre-qualification list? For instance, a process that is less resource intensive for low-risk applications and more resource intensive for high-risk applications would seem logical.
    - How will DOE confirm that the prequalification list will be based upon objective, measurable criteria as widely understood and used in the industry?
    - Will DOE define what conformance regime it will use (e.g., IEC 62443 suite of Standards for industrial automation cybersecurity) as a basis for pre-qualification decisions?
    - To what extent will manufacturers be able to demonstrate either self-certification or existing third-party certification regarding the cybersecurity of a given product as a factor in the pre-qualification process?
    - The Department of Defense has stated that its Cybersecurity Maturity Model Certification (CMMC) will evolve from a data-focused certification to a product-focused certification in 2021. Although details are still unclear, industry has recommended that this product-focused version of the CMMC rely on existing Federal guidance in this space (e.g., NISTIR: 8259 - Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline) and/or existing international Standards (e.g., IEC 62443 suite of Standards).[2] To what extent does DOE plan to provide reciprocity between the pre-qualification list and the soon to be released product focused CMMC certification?

- Prohibited Transactions/Vendors

    - A key component to assessing scope and applicability of the EO is in understanding what entities will be viewed as "foreign adversaries" and how the government (and what entity(ies) in the government) will assess whether a given company is operating under the control or "jurisdiction" of a foreign adversary to the extent relevant to the EO. Noting that the government may not want to elaborate on either point, how will DOE provide advisory opinions (either proactively or in response to vendor inquiries) that would identify specific vendor actions that have come into question and corresponding recommendations on how a vendor could mitigate these concerns?
    - Title II of the Secure Technology Act created the Federal Acquisition Security Council (FASC) to, in part, coordinate the assessment and mitigation of supply

[2] https://csrc.nist.gov/publications/detail/nistir/8259/draft

chain risks to the U.S. supply chain. To what extent will DOE and the Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security coordinate with the FASC on supply chain security matters to ensure consistency, to reduce duplication, and to increase public input opportunities?

- Vendor Mitigation of Risk

    - In the context of mitigating risk, the DOE FAQ document referenced that additional funding may be needed for "supply chain testing and evaluation."[3] Can DOE elaborate on what this might look like? Who would do the testing and what safeguards would be put in place to protect vendors from liability concerns for matters found during an inspection that are not germane to the EO? Would the government potentially investigate a vendor's entire supply chain or simply that of a specific product? How would the government handle a supply chain that contains products sold to commercial and government customers alike?

The electroindustry welcomes an early comprehensive response to these and other questions that may arise from further analysis of EO 13920.

If you have any questions on these comments, please contact Phil Squair (703-841-3274 or philip.squair@nema.org) or Stacy Tatman (703-841-3221 or stacy.tatman@nema.org).

[3] https://www.energy.gov/sites/prod/files/2020/05/f74/DOE%20BPS%20EO%20FAQ.pdf