Before the Department of Energy
Washington, D.C. 20585

In the matter of
Ensuring the Continued Security
of the United States
Critical Electric Infrastructure

COMMENTS OF THE ELECTRIC POWER SUPPLY ASSOCIATION ON THE REQUEST FOR INFORMATION

Pursuant to the April 22, 2021, publication in the Federal Register[1] of the U.S. Department of Energy's (DOE) Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure, the Electric Power Supply Association (EPSA)[2] submits the following comments in response to the request. EPSA appreciates the opportunity to provide feedback to the Department on issues of such importance and commends DOE's efforts in exploring a long-term strategy for securing the nation's critical infrastructure.

I. COMMENTS

As the trade association representing competitive electricity suppliers, including generators, EPSA highlights that a large swath of supply chain issues are currently addressed, monitored, and reported pursuant to existing standards and business practices. For example, independent power producers (IPPs) regularly conduct enterprise-wide risk assessments as part of their NERC CIP Compliance programs.[3]

---

1 86 FR 21309, pp 21309-21312, Document number 2021-08482, published April 22, 2021.

2 EPSA is the national trade association representing competitive power suppliers in the U.S. EPSA members provide reliable and competitively priced electricity from environmentally responsible facilities using a diverse mix of fuels and technologies. EPSA seeks to bring the benefits of competition to all power customers. This pleading represents the position of EPSA as an organization, but not necessarily the views of any particular member with respect to any issue.

3 *Cybersecurity in the Electric Power Supply Sector*, EPSA Report issued September 2019, available at https://epsa.org/epsa-report-on-cybersecurity-in-the-electric-power-supply-sector/.

IPPs also conduct risk assessments on all new technologies that are brought into their systems. Further, as part of the CIP regime, IPPs have processes in place to protect cyber and company data related to limited product development or source code in compliance with NERC reliability standards.

Importantly, the Federal Energy Regulatory Commission (FERC) has oversight and approval authority over NERC's CIP regime, adding another layer of federal oversight and authority regarding the cyber and physical security of the BPS. FERC has visibility into industry efforts as well as the development of new standards and ongoing improvement of existing standards at NERC. In addition to these measures, IPPs have processes in place—which can include Sanctions Act validations—in order to ensure that they are protecting sensitive or critical data.

IPPs also participate in bi-directional information sharing with the U.S. intelligence community via the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and its National Cybersecurity and Communications Integration Center and are actively involved in the FBI's InfraGard program. IPPs further support their efforts by participating in the Electricity Information Sharing and Analysis Center (E-ISAC), NERC's GridEx, and events and training exercises offered by third-party independent experts, some of which are offered free of charge to encourage participation from electric suppliers of all sizes and resource levels.

While IPPs already include provisions and protections in contractual arrangements to help ensure the cybersecurity of components and sub-components that they and their vendors acquire on their behalf, the Department could craft standard

contract terms and procurement practices that are non-negotiable. Such action would alleviate a large legal and negotiating burden on the electricity sector while also ensuring by proxy that all supplier components and sub-components are up to a certain standard.

For an example of how such action might influence procurement behavior, one could look to how entities behave with relation to a sanctioned countries list. When a country is put on a sanctioned list, IPPs all know not to procure equipment from that country and how to adjust their business practices. Were DOE to create a standardized section of cybersecurity contract language, IPPs—as well as the rest of the electricity sector—would have a higher standard to hold firms with which they contract accountable. Should any firm be unwilling to operate under this standard contract language, the procuring entity would then look to find another firm amenable to the contract.

DOE could also strengthen security and relieve a burden on the electric sector by creating a “whitelist” of approved suppliers. In creating a list of approved suppliers, DOE could give the electric sector an even greater degree of confidence that they are buying secure products. In order to limit market power and increase competition among manufacturers, DOE should take measures to ensure multiple suppliers are open for selection.

I. CONCLUSION

IPPs prioritize the cybersecurity of their facilities and systems and have therefore implemented extensive, comprehensive processes to ensure the safety of their equipment. DOE could strengthen industry procurement efforts by crafting standardized

cybersecurity contract language and creating a whitelist of suppliers who manufacture component and subcomponent parts.

Respectfully submitted,

ELECTRIC POWER SUPPLY ASSOCIATION

By: *Bill Zuretti*
Bill Zuretti
Director, Regulatory Affairs & Counsel
Electric Power Supply Association
1401 New York Ave, NW, Suite 950
Washington, DC 20005

Dated: June 7, 2021