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

In the matter of	**)**	
Securing the United	**)**	**Docket DOE-HQ-2020-0028**
States Bulk-Power System	**)**	

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

Pursuant to its July 8, 2020, publication in the Federal Register,[1] the Electric Power Supply Association (EPSA)[2] submits the following comments on the U.S. Department of Energy's (DOE) Request for Information (RFI) on Securing the United States Bulk-Power System (BPS). EPSA appreciates the opportunity to provide feedback to the Department on issues of such importance. In order to develop the most complete and helpful record, the original equipment manufacturers (OEMs) of bulk power equipment are the best source of information to answer the questions posed by the RFI as the entities able to identify the supply chain for BPS components in order to highlight concerns, vulnerabilities, or current practices that require attention from DOE. Also, it should be noted that many of the questions posed in the RFI raise issues or processes that currently are addressed pursuant to existing regulatory requirements, such as NERC's Critical Infrastructure Protection (CIP) Standards.

EPSA suggests that in undertaking this process, DOE should focus its inquiry on bulk power equipment consisting of transformers as these are the devices routinely

---

[1] 85 FR 41023, pp 41023-41026, Document number 2020-14668, published July 8, 2020.

[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.

deemed critical to the grid and through which all grid power flows. Given that there are many components of transformers, the requests posed to equipment suppliers should be limited to first tier subsuppliers. Further, in order to garner the most useful responses to the inquiry while limiting unnecessary administrative burden on providers of electricity and the DOE, EPSA suggests that the RFI should be limited to transformers that fall within Defense Critical Electric Infrastructure (DCEI) Pathways. To collect data on all BPS equipment casts a very wide a net and catches an array of information that is not helpful in assessing the security of the system.

I. Concerns Outlined in Section A are Being Addressed by Industry and Overseen by Governmental Entities Pursuant to Existing Practices and Regulations

As the trade association representing competitive electricity suppliers, including generators, EPSA highlights that several of the issues outlined in Section A are currently being 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] 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.

[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/.

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.

As to Questions A4(a) and A6 which inquire about information sharing, a partnership already exists between competitive suppliers and government agencies responsible for cybersecurity. IPPs are represented on the Electricity Subsector Coordinating Council (ESCC). 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 & 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. With respect to Question A5, 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.

II. Original Equipment Managers are Best Positioned to Respond to the RFI

Many of the remaining questions posed in the RFI are best addressed to OEMs. IPPs rely on OEMs to conduct vulnerability testing of the parts that they manufacture and issue vulnerability notifications. Additionally, DHS/CISA issues notifications and vulnerability scoring systems. Even where IPPs have inquired about OEM subcontractor and subsupplier relationships, OEMs are often reluctant to grant complete visibility into their proprietary supply chains. Supply chain sourcing is viewed as a significant competitive commercial advantage, thus severely limiting the scope of information that OEMs are willing to share with customers like the IPPs. This makes it particularly challenging if not impossible for IPPs to comprehensively respond to the RFI questions in a meaningful way.

Both DOE and electricity providers would be better served by posing questions in this RFI directly to OEMs. This would save the unnecessary step of having all IPPs, along with several other industry sectors, inundate the OEMs with requests to assist in the response to the RFI inquiries. As crafted, responding to the RFI would require an entity to initiate expansive information requests to equipment manufacturers; information requests that may receive responses. Even assuming IPPs have the contractual and commercial relationships sufficient to obtain this information from the OEMs, there may be concerns related to the comment schedule of the RFI process as, at that point of the supply chain, equipment suppliers may be overwhelmed by information requests from their customers, both direct and indirect. Thus, fulfilling the

request will likely create a sizeable administrative burden at duplicative points along the supply chain.

It is important to note that IPPs often are not in contact with the OEM through their vendors and therefore may not be able to identify numerous equipment suppliers. Further, it is unclear how far back IPPs and other utilities will be able to trace the source of certain equipment, or sub-components of various equipment, if their vendors are purchasing and re-purchasing from other sources. This could raise significant cost and resource burdens, most of which could be mitigated or avoided altogether by directing these inquires to the originating OEMs.

III. The Inquiry into Security Concerns on Bulk Power Equipment Should be Limited to Transformers That Fall within DCEI Pathways

In order to further reduce the potential burden on industry and still collect the information required to protect the integrity of the grid, DOE should limit the scope of its inquiry to transformers that fall within DCEI pathways. Transformers face challenges that make them vulnerable components on the grid in relation to other equipment. As DOE's Office of Electricity points out, transformers are "expensive, difficult to transport, and typically custom-made with procurement lead times of one year or longer."[4] While all segments of the bulk power system—including generation equipment—face some level of cyber and physical security risk, the loss of critical transformers in DCEI pathways could disrupt electricity services in areas that cannot afford to lose them for any length of time. While generators aim to run as frequently as possible, the loss of any one power plant would not compromise grid reliability, whereas the loss of a critical

[4] DOE Office of Electricity, *Addressing Security and Reliability Concerns of Large Power Transformers,* (retrieved on August 6, 2020), https://www.energy.gov/oe/addressing-security-and-reliability-concerns-large-power-transformers.

transformer could have cascading effects on the grid's ability keep power flowing. In directing its inquiries to OEMs that manufactured transformers that fall within these zones, DOE can reduce administrative burden and still ensure the security of the nation's most critical transformers.

IV. Conclusion

IPPs prioritize the cybersecurity of their facilities and systems and have therefore implemented extensive, comprehensive processes to ensure the safety of their equipment. In order to best assist DOE in its assessment of one aspect of this critical security issue, the recommendations and responses herein will assist in the efficient and timely collection of all necessary information regarding the electricity industry's current practices to identify and mitigate vulnerabilities in the supply chain for components of the bulk-power system. In particular, DOE should direct inquiries to OEMs and limit its scope to transformers that fall within DCEI pathways.

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: August 24, 2020