UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security	**)** **)** **)**	**Docket No. RM20-19-000**

COMMENTS OF THE ELECTRIC POWER SUPPLY ASSOCIATION

Pursuant to the Commission's September 17, 2020 Notice of Inquiry,[1] the Electric Power Supply Association (EPSA)[2] submits the following comments. EPSA members take very seriously the cyber and physical security of their operations and the grid. Ensuring that all security considerations are fully addressed is central to the operations of all participants in the delivery of electricity to consumers, particularly independent power producers (IPPs) and competitive power suppliers who rely on capacity, energy, and ancillary services market revenues for service supplied to continue to operate, rather than guaranteed cost recovery from ratepayers.

Any day with a service disruption is a day that a competitive power supplier is not able to conduct its business or sell its product. Further, any day with a service disruption is a day that customers will not be able to conduct their business or make or sell their products. Neither is acceptable. Hence, competitive suppliers are deeply committed to producing safe and reliable energy for delivery to customers across the country in a manner as secure as possible on both the cyber and physical fronts.

---

[1] Notice of Inquiry, *Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security*, Docket No. RM20-19-000, (issued September 17, 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.

As further detailed below, a pivotal plank in EPSA members' security efforts is the establishment of robust procurement protocols and procedures. EPSA members have myriad measures in place to limit the procurement of equipment from both the Covered Companies list as well other potentially problematic sources. Additionally, EPSA members believe that the suite of Critical Infrastructure Protections (CIP) standards continues to prove effective at mitigating risks aimed at disrupting the bulk electric system (BES). These standards allow for the identification, prevention, detection, response, and recovery of impacts associated with the risks that may result from the use of a Covered Company's equipment.

I. COMMENTS

A. EPSA Members Have Extensive Procurement Protocols in Place

In order to reduce the risk of the acquisition of problematic equipment EPSA members regularly conduct enterprise-wide risk assessments as part of their NERC CIP programs.[3] IPPs also conduct risk assessments on all new technologies that are brought into their systems. Further, both as part of the CIP regime and through their broader information security protocols, IPPs have already implemented robust processes to protect cyber and company data related to limited product development or source code in compliance with NERC reliability standards in the least. In addition to these measures, IPPs utilize protocols—which can include Sanctions Act validations—in order to ensure that they are protecting sensitive or critical data.

In the event that equipment from the list of Covered Companies were to be installed within an entity's infrastructure, controls mandated by the CIP standards and

[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/.

operational controls would remain in place. Specifically, High and Medium Impact sites would maintain controls, such as intrusion detection, security monitoring, cyber incident detection and response, and malicious software prevention. Low Impact sites would continue to maintain cyber incident response controls. Additionally, 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.

To a limited extent, IPPs do rely on original equipment manufacturers (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 advantage, thus severely limiting the scope of information that OEMs are willing to share with customers like the IPPs. To strengthen security on this front, the Commission could evaluate the development of security certification standards for OEMs. These standards would allow the OEM to pursue a security certification, in accordance with criteria determined by the Commission, and would ensure that a specific security baseline was met through issuance of this certification.

B. EPSA Members Find NERC's CIP Regime to be Effective

As the previous section outlines, NERC CIP standards play a critical role protecting the grid and preventing the acquisition of components from the Covered Companies list. EPSA and its members find the CIP regime to be highly effective in mitigating risks and protecting the BES. A number of these standards, including CIP-

005, CIP-007, CIP-008, CIP-009, CIP-010 and CIP-013, all complement each other to some degree and require the entity to take actions that detect and/or mitigate risks associated with the use of Covered Company equipment.

As the Commission knows through its oversight and approval authority over this regime, extensive work takes place at NERC in the development of new standards and constant improvement of existing standards.[4] Standards are developed using a results-based approach that focuses on performance, risk management, and entity capabilities, and are constantly being updated to address emerging threats. The program, and compliance by electric sector companies, ensures the appropriate security measures are in place to protect the BES.

In addition to the requirements outlined above, the CIP program requires entities to use firewalls to block vulnerable ports and to implement cyberattack monitoring tools. Entities are also required to enforce IT controls protecting access to critical cyber assets. Systems for monitoring security events must be deployed, and organizations must have comprehensive contingency plans for cyberattacks, natural disasters and other unplanned events. NERC utilizes compliance monitoring and an enforcement program to monitor, assess, and enforce uniform compliance. At any time, electric providers—each a Registered Entity—may be subject to an audit or spot check for compliance with all applicable CIP Standards. These standards are critical to the protection of the BES and EPSA and its members continue to support this paradigm.

[4] NERC and its Regional Entities regularly report to the Commission on current and evolving activities to address system reliability, including threats or risks to the security of the system. As an example, on May 10, 2019, the Commission issued a Supplemental Notice of Technical Conference for its annual Reliability Technical Conference (Docket No. AD19-13-000).

C. EPSA Members Support Additional Information Sharing Efforts

As the Commission is aware, EPSA and its members are represented on the Electricity Subsector Coordinating Council (ESCC). Many IPPs participate actively in existing bi-directional information sharing forums 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.

Despite this extensive list of information sharing efforts, EPSA believes that the Commission could play a pivotal role in coordinating or encouraging additional avenues to exchange critical security information. For example. FERC could encourage the E-ISAC to track vulnerabilities and develop a holistic repository for entities to reference. Those same entities could be encouraged to anonymously post any additional helpful information at their discretion. EPSA and its members have greatly benefitted from the expanded information sharing and additional avenues to do so would surely yield additional security benefits to the security efforts of IPPs and the grid as a whole.

II. Conclusion

IPPs prioritize the cyber and physical security of their facilities and systems and have therefore implemented extensive, comprehensive processes to ensure the safety

of their equipment. EPSA members continue to support NERC's CIP standards as well as the avenues through which information is currently shared throughout the electric sector. EPSA encourages FERC to consider developing a list of security certification standards for OEMs and believes that that the Commission should work with the E-ISAC to develop a holistic repository for entities to reference and explore additional opportunities to share information in order to increase the security efforts of BES participants.

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: November 20, 2020

CERTIFICATE OF SERVICE

I hereby certify that I have this day served the foregoing document on each person designated on the official service list compiled by the Secretary of the Federal Energy Regulatory Commission in this proceeding.

Dated at Washington DC, this 20th day of November, 2020.

/s/ Bill Zuretti
Bill Zuretti