UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Security Investments for Energy Infrastructure Technical Conference	))))	AD19-12-000

COMMENTS OF THE ELECTRIC POWER SUPPLY ASSOCIATION

Pursuant to Rule 211 of the Rules of Practice and Procedure of the Federal Energy Regulatory Commission ("FERC" or "the Commission"),[1] the Electric Power Supply Association ("EPSA")[2] hereby submits these comments in response to the Commission's Notice Inviting Post-Technical Conference Comments[3] in the above captioned proceeding. EPSA members take very seriously the cyber and physical security of their operations and the grid and are therefore pleased to submit comments and recommendations on this issue pursuant to the discussion at the March 28th technical conference on security investments for energy infrastructure.

I. OVERVIEW AND SUMMARY

Cyber and physical security are essential to electricity generation operations and represent a clear and extensive commitment by EPSA members and competitive suppliers (or, independent power producers) in the delivery of safe and reliable power to

[1] 18 C.F.R. §§ 385.211.

[2] Launched over 20 years ago, EPSA is the national trade association representing leading independent power producers and marketers. EPSA members provide reliable and competitively priced electricity from environmentally responsible facilities using a diverse mix of fuels and technologies. Power supplied on a competitive basis collectively accounts for 40 percent of the U.S. installed generating capacity. 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] See Notice Inviting Post-Technical Conference Comments, Issued April 25, 2019.

customers across the United States. The electric sector is taking broad-based action to confront and prevent known and emerging threats, and competitive suppliers are a crucial and active part of that effort. Ensuring that all cyber and physical security considerations are fully addressed is central to the operations of all participants in the delivery of electricity to consumers, particularly independent power producers and competitive power suppliers who rely on capacity, energy, and ancillary 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.

Competitive suppliers recognize the challenge of balancing traditional societal electricity goals of reliability and reasonable costs with the critical goal of ensuring security. Given the diversity of power providers, business models, and asset portfolios, it is necessary to allow a level of flexibility to companies across the country to prioritize and address critical security matters. Factors including company size, extent of asset ownership, transmission configuration, physical location and design of facilities, presence in organized wholesale markets, regional resource and system constraints, and prior patterns of theft, vandalism, and other security-related activities all influence analyses and decisions regarding critical asset identification and risk threat

assessments by individual companies. While this concern is standard operating procedure for all generators based on their current market model, should the government opt to vastly ramp up or change cyber and physical security requirements, additional cost recovery avenues or mechanisms may merit consideration for companies which operate in market-based rate regimes.

II. COMMENTS

A. Cyber and Physical Security Are Critical Components in Competitive Electricity Supplier Operations and Business Practices

Competitive suppliers operate under a myriad of cyber and physical security regulatory regimes. They each participate in the development of, and comply with, North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") standards. NERC Reliability Standards define the reliability requirements for planning and operating the North American bulk power system and 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. FERC has oversight and approval authority over this regime and is therefore well informed of the extensive work taking place at NERC in the development of new standards and constant improvement of existing standards.[4] For instance, FERC Order 848 requires NERC to update the CIP standard for cybersecurity incident reporting (CIP-008), which will require Independent System Operators/Regional

[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). The first panel on the agenda features leadership from NERC and its Regional Entities reporting to the Commission on current trends and risks to reliability, whether additional resources or steps are needed for certain types of risks, and how evolving threats are or should be addressed.

Transmission Organizations ("ISOs/RTOs") to update practices and procedures associated with cybersecurity event investigations and incident investigation and reporting. Additionally, generators can participate in the Electricity Information Sharing and Analysis Center ("E-ISAC")[5] in order to share and get information on security data gathering and analysis, incident management coordination, and communication mitigation strategies among stakeholders. The E-ISAC, which is run by NERC, provides a monthly briefing and regularly scheduled security conferences, as well as organizing the NERC GridEx exercises on cybersecurity and physical security, in which competitive suppliers participate.

Competitive suppliers are also represented on the Electricity Subsector Coordinating Council ("ESCC"), through the participation of EPSA's CEO, who serves on the Council's nine-member Steering Committee.[6] The ESCC functions as the principle liaison between leadership across multiple agencies in the federal government and in the electric power sector by convening CEO level decision-makers from all parts of the industry and government around the table to coordinate efforts to prepare for national-level incidents or threats to critical infrastructure. At this forum, competitive suppliers and other electricity sector representatives are able to share clearance-level information and exchange best practices in order to better prepare for and protect against emerging threats.

---

[5] Participation in the E-ISAC helps industry learn about emerging trends, share information and provides access to monthly reports and bulletins, advanced analytical capabilities.

[6] The ESCC is a voluntary organization which has been convened to support the Nation's energy security and resilience mission in accordance with the Presidential Policy Directive 21: Critical Infrastructure Security and Resilience; Executive Order 13636, Improving Critical Infrastructure Cybersecurity; and the National Infrastructure Protection Plan (NIPP). See the ESCC charter on the Department of Homeland Security website: https://www.dhs.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf

Under the auspices of NERC, there are also seven Regional Entities each of which hosts conferences and monthly/quarterly meetings to address and educate market participants on region-specific issues, risks, and threats.

In addition to NERC requirements, competitive suppliers are actively involved in the FBI InfraGard program. InfraGard is a partnership between the FBI and members of the private sector that provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of critical infrastructure. This forum serves as a platform for Chief Information Security Officers ("CISOs"), Chief Security Officers ("CSOs"), and their staffs to train and share intelligence and best practices to help protect their organizations and the grid by contributing industry specific insight and advancing national security. Each meeting has an assigned FBI special agent in attendance and typically also features an agent from the Department of Homeland Security.

Outside of these formal processes, competitive suppliers contract third party vendors to conduct regular, proactive cyber compromise assessments to continually evaluate and improve their risk posture. Additionally, security subject matter personnel and officers attend an array of security conferences and seminars for education and to share information among similarly situated energy companies and across the electricity industry broadly.

B. Competitive Suppliers Recover Some Security Costs Through Competitive Markets

Competitive suppliers are currently able to recover costs associated with cyber and physical security through a number of sources, whether through market-based

rates collected in the organized electricity markets, retail revenues, provisions within power purchase agreements or other sources of revenue. Looking forward, however, issues around cyber security and physical security continue to rapidly evolve and therefore deserve continued observation and analysis as a strategic matter. For this reason, EPSA appreciates the Commission and the Department of Energy ("DOE") continuing the dialogue around these issues. While DOE indicated that changes to the regulatory regime are necessary,[7] FERC Chairman Neil Chatterjee rightly pointed out that "it is not possible or cost effective to design our energy infrastructures to withstand every type of attack that could possibly occur. Striking the right balance for consumers is a complex, but important undertaking."[8]

Competitive suppliers recognize the challenge of balancing the goals of electric reliability and reasonable costs while ensuring security. EPSA would emphasize that its members are continually working at improving their security solutions to enhance and refine their practices to protect cyber and physical systems. Should the Commission—or any other state or federal authority—deem it necessary to implement new standards or requirements or change current standards or requirements, EPSA believes that first there should be an assessment of the flexibility that can be afforded to market participants and resource owners in addressing critical security matters. Organizations must consider a number of business risks (e.g., compliance, financial, operational, and reputational) for continuity and security. Companies' risk management programs are focused on reducing all broader business risks that an organization might face, including cyber and physical threats, by taking measures to ensure that available (but

---

7 Transcript at p. 165, DOE Assistant Secretary Bruce Walker, "[T]he status quo does not work."

8 Transcript at p. 9.

limited) resources are targeted at reducing critical risks. However, should changes to existing standards or requirements include more prescriptive practices to address cyber and physical security, or should threat levels continue to rise and diversify, additional opportunities for cost recovery may be necessary.

C. Additional Avenues for Cost Recovery if Needed

While cyber and physical security issues can arise from individual decisions or errors, these issues can affect the entire electric system. For this reason, all participants in the supply chain are and must be focused on threats to the system as a whole as well as to the individual parts under their control as integral parts of that system. Accordingly, should additional unforeseen costs be imposed upon competitive suppliers in order to protect the system broadly or to address new risks, it may be reasonable that these costs be recovered on a regional or system-wide basis. As such, an area that may merit consideration is to reflect those costs in ISO/RTO capacity constructs which are designed to address a resource's fixed costs, including Operations and Maintenance ("O&M").

While competitive suppliers recover costs through multiple organized wholesale markets, the markets come with parameters for which costs can and cannot be included in supplier bids. In the capacity markets, which are designed to address fixed costs for generation or supply resources, Net Cost of New Entry ("Net CONE") is an estimate of the total project capital cost and annual fixed O&M expenses, over and above what it can earn in the energy and ancillary services markets, of a new generating plant of a type likely to provide incremental capacity in the forward delivery year or years addressed by the capacity auctions. As some of the cyber and physical security costs

clearly fall into the O&M bucket, EPSA believes that the capacity markets are where these costs should be appropriately priced and ultimately recovered. By reflecting these costs into Net CONE calculations, ISOs/RTOs will ensure that resources have the opportunity to be compensated through the capacity markets for their costs of doing business, including necessary cyber and physical security investments, when determining their expected revenues.

D. Additional Suggestions to Improve the Security of the Electric System and Individual Resources

Aside from cost recovery changes, there are additional aspects of the cyber and physical security regime that EPSA and its members believe could be improved. One of the most effective tools in the security toolkit is the sharing of information, as the E-ISAC and ESCC demonstrate. However, even with robust programs like those in place, competitive suppliers have experienced a lag in receiving information about security incidents or specific threats which have taken place and may affect their own risk assessment. For instance, EPSA member companies have reported notification delays of 18-24 months from the date of an event, which makes preparing for and girding against these threats more difficult or not timely as the incident/threat may have already run its course or caused significant damage by the time they are briefed.

As discussed at the March 28 conference, it is important that companies have access to the critical information needed to ensure that their systems and awareness are up to date. An important improvement would be to ensure that such information is not overly restricted as classified unless warranted, and that there are numerous persons at a company with the necessary security clearance to receive it. The security of the system is far too important to hinge on the availability of one or two people at a

company with the necessary clearance to receive timely information. An efficient, timely process for granting security clearances is critical. This may require revisions or improvements to the clearance process, some of which could be particular to the energy industry. Such improvements would likely ensure that all affected entities receive the information needed, speed up the process of disseminating that information, and allow for faster response and mitigation.

III. CONCLUSION

Competitive suppliers prioritize cyber and physical security and currently recover some of those costs necessary to meet and exceed regulatory requirements. Additional costs imposed on these entities may require additional avenues for cost recovery. Should such costs be imposed, EPSA respectfully requests that the Commission consider alternatives while allowing for flexibility in complying with requirements in order to maximize an entity's resources, program, and approach to its own physical and cyber security.

Respectfully submitted,

Nancy Bagot

Nancy Bagot
Senior Vice President
Bill Zuretti
Director, Regulatory Affairs and Counsel
Electric Power Supply Association
1401 New York Ave, NW, Suite 950
Washington, DC 20005

Dated: May 28, 2019

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the comments via email upon each person designated on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C., May 28, 2019.

Bill Zuretti

_____

Bill Zuretti, Director, Regulatory Affairs, and Counsel