UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cybersecurity Incentives	**)**	**Docket No. RM21-3-000**

COMMENTS OF THE ELECTRIC POWER SUPPLY ASSOCIATION

Pursuant to the Federal Energy Regulatory Commission's ("FERC" or "Commission") December 17, 2020 Notice of Proposed Rulemaking ("NOPR"), the Electric Power Supply Association ("EPSA")[1] submits the following comments. EPSA members take very seriously the cyber and physical security of their operations and the grid. Ensuring that all cyber and physical security considerations are fully addressed is central to the reliable operations of all participants in the delivery of electricity to consumers, including independent power producers (IPPs) and competitive power suppliers who rely on capacity, energy, and ancillary market revenues for service supplied to continue to operate.

In issuing the instant NOPR, the Commission has expressed interest in incenting entities to exceed existing cybersecurity requirements established by the North American Electric Reliability Corporation ("NERC") through Critical Infrastructure Protection Reliability ("CIP") standards and the NIST Framework. Given the fluid and dynamic nature of the cybersecurity space—and the resultant complexity of developing regulations that match current on-the-ground realities—EPSA believes that an

[1] 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.

incentive-based approach would allow entities to make investments above and beyond existing standards to keep the Bulk-power system ("BPS") protected against emerging threats not yet reflected in standards or regulations. Accordingly, EPSA supports the incentive approaches outlined in the NOPR to encourage cybersecurity investments on a voluntary basis to better secure individual facilities as well as the Bulk-Power System. In order to achieve the goal of the NOPR, any incentives should be extended to all BPS facilities that may make improvements as outlined – including competitive power generators that recover their costs through competitive markets. Incenting only transmission providers misses an opportunity to fortify the Bulk-Power System in its entirety. Therefore, EPSA believes that a methodology or approach to offer incentives to merchant facilities that do not receive a guaranteed rate of return is needed.

I. COMMENTS

A. To Achieve the Desired Investment in Cybersecurity Improvements, the Commission Should Extend Incentives to All BPS Entities

As the NOPR highlights, Commission staff outlined in its *Cybersecurity Incentives Policy White Paper* that a new incentive framework could allow the electric industry to be more agile in monitoring and responding to new and evolving cybersecurity threats, to identify and respond to a wider range of threats, and to address threats with comprehensive and more effective solutions.[2] In the White Paper, Commission staff reasoned that an incentive-based framework would allow a public utility to tailor its request for incentives to the potential challenges it faces and take responsive action. Commission staff explains that, in the future, these voluntary actions

[2] NOPR, P. 14 citing *Cybersecurity Incentives Policy White Paper*, Notice of White Paper, Docket No. AD20-19-000 (issued June 18, 2020) ("White Paper").

taken by public utilities, if proven beneficial, could be the basis of future CIP Reliability Standards that could become mandatory.[3] While the NOPR and Staff White Paper are focused on incentives for utilities that operate under cost-of-service regulation, it stands to reason that offering a similar incentive paradigm to entities that recover their costs through competitive markets would serve the same end, if not as a force multiplier for the goals of the NOPR and cybersecurity readiness of the Bulk-Power System.

As the NOPR recognizes, "it is important that public utilities make cybersecurity investments to quickly and effectively address these cybersecurity challenges as well as other emerging threats."[4] While transmission providers ("TPs") do face complex cybersecurity risks, so do the generation resources that are an essential part of the BPS. For this reason, competitive suppliers routinely exceed what is required by standards and regulations. This protects generation facilities and ensures the most reliable operations. 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, and is why competitive suppliers invest in extensive security systems for their own protection and that of the BPS.

Given the interconnected nature of the modern interstate electric system, it is only reasonable that all segments of the BPS should be incented to fortify their cybersecurity defenses in the same manner as the Commission proposes for TPs in the NOPR in order to further strengthen the system. The NOPR specifically identifies this dynamic:

---

3 *Id.*

4 NOPR, P. 17.

> Encouraging utilities to address cybersecurity of the Bulk-Power System is uniquely important given the degree to which components of the Bulk-Power System are digitally interconnected with one another and the ever-expanding risks posed by adversaries create challenges for those tasked with defending those interconnections from cyber exploitation.[5]

As cyber threats can often cut across interconnected systems, it holds that the BPS would be well-served to be as fortified as is reasonably possible. Incenting one segment while leaving out others may squander an opportunity for the system as a whole to remain ahead of the curve regarding cybersecurity threats.

A broader cybersecurity paradigm would greatly benefit ratepayers as it would further solidify system security and, ultimately, reliability. The NOPR recognizes these benefits and seeks to maximize them by creating an incentive-based approach under FPA sections 205 and 206, rather than FPA 219, which the NOPR posits may "unnecessarily limit" effective incentives.[6] The NOPR also explicitly seeks to "incent a public utility to adopt cybersecurity practices that would not only better protect its own systems but also improve the security of the Bulk-Power System."[7] Given that power generators work in concert with transmission providers to deliver wholesale power, the system as a whole would benefit from both halves of the Bulk-Power System being incented to take measures beyond what is required of their them under CIP standards or the NIST Framework. The NOPR identifies incentive areas that could also apply to power generation facilities, including the Med/High Incentive and the High/Low Incentive.[8] This incentive parity should also apply to certain investments made by generators under the NIST Framework Approach. For example, installing a dynamic

---

5 *Id.*
6 NOPR, P. 19
7 *Id.*
8 NOPR. P. 26-31.

asset management program to improve an entity's ability to quickly detect and address new or previously unknown equipment on its network applies to generators as it does to transmission providers. These investments would benefit the system as a whole as they improve the BPS's ability to detect and respond to new threats and therefore minimize service disruptions.

B. Single Issue Ratemaking May Provide a Pathway to Incentives in Competitive Markets

EPSA recognizes that incenting voluntary behavior is not as straightforward for those entities that recover their costs through competitive markets rather than a guaranteed rate of return. While the Commission can offer an ROE adder to transmission providers, it has no such vehicle for IPPs and competitive suppliers that operate in competitive markets. With that said, single issue ratemaking may offer a pathway for the Commission to pursue.

For example, to reasonably mirror the incentive dynamic that the NOPR outlines for transmission providers, the Commission might publish a series of areas that it identifies as emerging and future cybersecurity risks—perhaps on an annual basis. In order to optimize the utilization of these investments, the Commission might set a threshold at which an entity is eligible for cost recovery for these investments if a demonstration is made that the Bulk-Power System as a whole would benefit from their installation. Hence, if a competitive market participant petitions the Commission for authorization to make an upgrade with the required showing of benefits and the Commission approves the petition, that entity would then be able to make the cybersecurity update and file for cost recovery of the costs incurred to make the upgrade. The Commission operates under a similar paradigm for assessing costs

associated with providing reactive power service. While not a perfect match for the incentive structure outlined in the NOPR, this pathway would ultimately help achieve the stated cybersecurity goal and lead to similar outcomes as the incentives proposed for transmission providers, all while preserving Commission oversight and discretion over the associated costs.

C. The Commission Should Ensure that Cross-subsidization Does Not Occur in Vertically Integrated Entities

While addressing important issues around voluntary incentives, the NOPR also raises potential issues for entities that are vertically integrated. While these companies may have separate legal entities for their transmission and generation operations, cybersecurity programs are often administered as a shared service. Accordingly, the Commission must ensure that any entities to which it extends incentives on the transmission side are not cross-subsidizing cybersecurity operations for their generation arms, particularly if those incentives are not available to generation competitors, like the Regulatory Asset Incentive.[9] In some RTOs—including MISO and SPP—IPPs and competitive suppliers compete against vertically integrated utilities to supply power to the system operator; allowing these entities to use transmission incentive monies to subsidize their generation operations would put IPPs and competitive suppliers at an even greater competitive disadvantage than they already face in these regions.

[9] NOPR, P. 40.

II. Conclusion

Due to the interconnected nature of the Bulk-Power System and the Commission's desire to incent entities to exceed existing cybersecurity requirements established by NERC through CIP standards and the NIST framework, the Commission should extend those cybersecurity incentives offered to TPs on an equal or symmetrical level to voluntary measures taken by power generators. Additionally, the Commission should take measures to ensure that vertically integrated utilities do not cross-subsidize their generation operations with incentives received for voluntary transmission cybersecurity measures.

Respectfully submitted,

ELECTRIC POWER SUPPLY ASSOCIATION

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

Dated: April 6, 2021