UNITED STATES OF AMERICA
BEFORE THE
DEPARTMENT OF ENERGY

	)
Ensuring the Continued Security of the	)
Unites States Critical Electric Infrastructure	)

COMMENTS OF THE PSEG COMPANIES

PSEG[1] appreciates the opportunity to submit these comments to the Department of Energy ("DOE" or "the Department") in response to its request for information ("RFI") on *Ensuring the Continued Security of the United States Critical Electric Infrastructure* published on April 22, 2021.[2] The RFI is focused on preventing exploitation and attacks by foreign threats to the U.S. supply chain by developing recommendations to strengthen requirements and capabilities for supply chain risk management practices by the nation's electric utilities.

PSEG participated in developing the comments filed by the Edison Electric Institute ("EEI") in this matter and incorporate those comments herein by reference. PSEG is filing these limited individual comments to further supplement the concerns and recommendations EEI expresses in response to the RFI.

I. COMMENTS

PSEG provides the following comments to inform the DOE as it considers potential recommendations for requirements that will strengthen supply chain risk management for the electric industry. PSEG appreciates the DOE engaging the electric power industry to address our mutual interest in ensuring the security of the U.S. supply chain. We firmly believe that open

[1] The PSEG Companies are: Public Service Electric and Gas Company, PSEG Power LLC and PSEG Energy Resources & Trade LLC (collectively referred to as "PSEG").
[2] 86 FR 21,309.

communication and information sharing between the federal government and the electric power industry is essential to mitigate evolving and increasingly sophisticated threats to critical U.S. energy infrastructure.

The RFI seeks comment on four specific questions related to developing a long-term strategy to address pervasive and ongoing grid security risks and four questions on the advisability and feasibility of an expanded approach that would cover distribution facilities that serve critical defense facilities.

A. Long Term Strategy

1. What technical assistance would States, Indian Tribes, or units of local government need to enhance their security efforts relative to the electric system?

The DOE should consider policies that promote enhanced cyber security tools around equipment that operates the electric system. For example, the DOE could partner with state and local governments to develop playbooks that provide guidance to utilities for implementing security tools around the National Institute of Standards and Technology Cybersecurity Framework, which include asset visibility, protective and detection controls, and responding to and recovery from cyber incidents. The Cybersecurity and Infrastructure Security Agency could make the Validated Architecture Design Review service widely available and also offer consulting services for implementing recommendations from the design review.

2. What specific additional actions could be taken by regulators to address the security of critical electric infrastructure and the incorporation of criteria for evaluating foreign ownership, control, and influence into supply chain risk management, and how can the Department of Energy best inform those actions?

Regulators should eliminate ambiguity and engage electric utilities directly and through, for example, EEI and the North American Electric Reliability Corporation ("NERC"), to drive a

focused and defined risk-based approach to supply chain risk management. It is also imperative for regulators to share information between the government and utilities, including timely classified information sharing on emerging risks. Additionally, hard-to-replace equipment such as SCADA and relay protection devices that in some instances have no alternative suppliers should receive particular scrutiny, and where warranted, targeted risk-based action. Finally, the DOE should support a database that allows utilities to obtain information about equipment it has or seeks to add to their electric systems.

3. What actions can the Department take to facilitate responsible and effective procurement practices by the private sector? What are the potential costs and benefits of those actions?

Before the Department chooses which procurement and risk management practices to implement, the Department should identify, clearly describe, and prioritize the highest impact equipment. The Department should integrate this strategic, risk-based approach as it contemplates any future action, and work with the electric industry to have a mutual understanding of the scope of supply chain risks.

PSEG suggests that the DOE promote a "USA Secure Electric System" that applies audit criteria across domestic and foreign providers of critical electric infrastructure equipment. Such a certification system could issue certification to those providers that meet supply chain objectives as defined by a risk-based approach. This certification would ensure that applicable standards are enforced reliably and consistently across different bulk-power system equipment subject to regulations.

Finally, many electric utilities are already subject to NERC Critical Infrastructure Protection ("CIP") standards, including a robust Supply Chain CIP standard, and are subject to intrusive, comprehensive audits of their CIP programs. Any new regulations contemplated

should take into account existing standards, and include coordination with Federal Energy Regulatory Commission ("FERC") and NERC to avoid costly and counterproductive duplication of effort.

4. Are there particular criteria the Department could issue to inform utility procurement policies, state requirements, or FERC mandatory reliability standards to mitigate foreign ownership, control, and influence risks?

The DOE should first conduct a rigorous analysis of risks posed by various pieces of equipment already in use or in development before implementing any new approach, and share the results with the industry for collaborative action. The DOE should eliminate ambiguity by being specific about which products and services are subject to future actions, e.g., entire components, sub components, operating systems, etc.

B. Prohibition Authority

1. To ensure the national security, should the Secretary seek to issue a Prohibition Order or other action that applies to equipment installed on parts of the electric distribution system, i.e., distribution equipment and facilities?

Before the Department chooses which procurement and risk management practices to recommend, the DOE should identify, clearly describe, and prioritize the highest impact equipment. The Department should integrate this strategic, risk-based approach as it contemplates any future action. The Department should work with the industry to have a mutual understanding of the scope of supply chain risk, and work collaboratively with industry on targeted action.

The distribution system is comprised of many types of equipment and therefore a wide variety of vendors are involved in procuring the equipment. The impact on components that would be most susceptible to a security event are primarily on supervisory and control elements,

and likely not the hardware that comprises most of the electric system, such as poles, underground cable, wire, and distribution transformers. The items of greater significance are the control systems such as supervisory control and data acquisitions systems, reclosers, and advanced distribution management system, along with the communication and relays to remote devices that these system utilize to monitor and control the system.

2. In addition to [Defense Critical Electrical Infrastructure], should the Secretary seek to issue a Prohibition Order or other action that covers electric infrastructure serving other critical infrastructure sectors including communications, emergency services, healthcare and public health, information technology, and transportation systems?

The DOE should identify, clearly describe, and prioritize the highest impact equipment before taking any action that covers electric infrastructure serving other critical infrastructure sectors.

3. In addition to critical infrastructure, should the Secretary seek to issue Prohibition Order or other action that covers electric infrastructure enabling the national critical functions?

Again, the DOE should identify, clearly describe, and prioritize the highest impact equipment before taking any other action that covers electric infrastructure serving national critical functions.

4. Are utilities sufficiently able to identify critical infrastructure within their service territory that would enable compliance with such requirements?

Electric utilities have the ability to sufficiently self-identify critical infrastructure. This is due to electric utilities such as PSEG having a unique and deep understanding of their own electric service territories, and by being members of multiple industry organizations including EEI, required compliance with NERC and FERC standards, and the current risk management plans and practices electric utilities have in place. Electric utilities also coordinate with the

Department of Homeland Security, the FBI, NERC, and state and local governments to identify and mitigate risks.

II. CONCLUSION

WHEREFORE, PSEG respectfully requests that the DOE incorporate EEI's comments in this matter by reference and consider these limited supplemental comments submitted in further support of strengthening the security of the U.S. supply chain. PSEG remains committed to working with DOE and other stakeholders to strengthen requirements and capabilities for supply chain risk management practices by the U.S. electric industry.

Respectfully submitted,

The PSEG Companies

/s/ Cara J. Lewis

Cara J. Lewis
Managing Counsel – Federal Regulatory
PSEG Services Corporation
601 New Jersey Ave NW STE 310
Washington, DC 20001
(202) 408-7581
Cara.Lewis@PSEG.com

Sean Cavote
Director NERC Compliance
PSEG Services Corporation
80 Park Plaza, P3
Newark, NJ 07102-4194
(973) 430-5310
sean.cavote@pseg.com

June 7, 2021