UNITED STATES OF AMERICA
BEFORE THE
DEPARTMENT OF HOMELAND SECURITY
TRANSPORTATION SECURITY ADMINISTRATION

Enhancing Surface Cyber Risk Management	)	TSA-2022-0001

COMMENTS OF PJM INTERCONNECTION, L.L.C.

PJM Interconnection, L.L.C. ("PJM") submits these comments in response to the Transportation Security Administration ("TSA") of the Department of Homeland Security's ("DHS") Advanced Notice of Proposed Rulemaking in the above-referenced docket.[1] PJM is the federally regulated regional transmission organization ("RTO") charged with planning and reliably operating the bulk electric system that serves 65 million customers in all or portions of Illinois, Indiana, Michigan, Kentucky, Tennessee, Ohio, West Virginia, North Carolina, Virginia, Maryland, Delaware, Pennsylvania and New Jersey and the District of Columbia.[2] PJM appreciates the opportunity to comment on the critical efforts by the TSA to consider implementing a comprehensive and forward-looking approach to cybersecurity requirements for interstate pipelines and rail, which are critical means for fuel delivery and the transport of other key materials needed in the electricity industry.

The issues in this docket are critically important to the reliability of the bulk electric system and the protection of the United States economy and national security. Natural gas generating capacity is approaching nearly 50% of total installed capacity in the PJM region.[3]

---

[1] *Enhancing Surface Cyber Risk Management*, 87 FR 73527-01 (Nov. 30, 2022), *as modified by*, 87 FR 78911-02 (Dec. 23, 2022).
[2] *Regional Transmission Organizations*, Order No. 2000, FERC Stats. & Regs. ¶ 31,089 (1999), *order on reh'g*, Order No. 2000-A, FERC Stats. & Regs. ¶ 31,092 (2000), *aff'd sub nom. Pub. Util. Dist. No. 1 of Snohomish County, Washington v. FERC*, 272 F.3d 607 (D.C. Cir. 2001) ("FERC Order No. 2000").
[3] *See* PJM's Capacity by Fuel Type (as of June 1, 2021), available at: https://www.pjm.com/-/media/markets-ops/ops-analysis/capacity-by-fuel-type-2021.ashx; *see also* RPM Commitment by Fuel Type in PJM, available at: https://www.pjm.com/-/media/markets-ops/ops-analysis/capacity-by-fuel-type-2021.ashx.

Coal and oil generating capacity is approximately 30% of the fleet.[4] These generators, and in turn, PJM's 65 million electricity customers, depend upon the physical and cyber security of the interstate pipeline system and rail system to keep the lights on. Although to date TSA has provided some direction to the industry through a more voluntary program, given ever-increasing cybersecurity threats[5] and gas/electric and supply chain interdependencies, the need for a more robust program of cybersecurity for the pipeline system and rail system has dramatically increased. Regulators (including TSA), in collaboration with pipeline operators at all levels of the supply chain and rail operators, must take swift action to close this gap and provide a more comprehensive set of cybersecurity standards.[6]

The good news is that TSA need not paint on a blank canvass. TSA can and should leverage the considerable work that FERC and the North American Electric Reliability Corporation ("NERC") have already done over the years to enhance the cybersecurity of the bulk electric system. Those efforts are embodied principally in the NERC Critical Infrastructure Protection ("CIP") standards.[7] PJM strongly urges the TSA to swiftly consider:

1) adopting the NERC CIP standards, making any revisions necessary in light of potential differences between pipelines/rail and the bulk electric system (particularly in terms of the scope of assets covered by the standards); and

---

[4] *Id.*
[5] The Colonial Pipeline ransomware incident is one such example. *See, e.g.*, David E. Sanger & Nicole Perlroth, *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity*, N.Y. Times (May 14, 2021; updated June 8, 2021).
[6] Undoubtedly, some in this docket will argue that they have already taken steps to secure their facilities from cyber attacks. PJM does not doubt these efforts and has worked well with many stakeholders on these very issues. However, individual efforts, even if well-planned, should not substitute for a more comprehensive set of enforceable standards to promote a baseline of cybersecurity across the nation for this vital infrastructure.
[7] *See* Reliability Standards for the Bulk Electric Systems of North America, Critical Infrastructure Protection (CIP) standards (updated Dec. 6, 2022), available at: https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf.

2) offering pipelines/rail a reasonable safe harbor period (not to exceed two years, and preferably even shorter) to avoid the risk of compliance fines while they make any additional investments necessary to satisfy the NERC CIP-like standards.

PJM's proposal yields multiple efficiencies for regulators and the industry alike. First, regulators would not need to develop a wholesale new set of standards for pipelines/rail because such a robust framework has long existed for other, interrelated critical energy infrastructure. Second, the adoption of the NERC CIP-like standards is not inconsistent with the history of inter-agency collaboration on cybersecurity matters.[8] Third, utilities that have both electric and pipeline operations would be able to import into their pipeline operations their electric operation's existing knowledge of and compliance with the NERC CIP standards, to the extent this has not already happened. Fourth, NERC CIP standards determine the criticality and protection level of assets based upon their role in the operation of the bulk electric system. A similar construct for pipelines/rail will help to identify and protect the most critical assets that serve downstream dependencies, such as electricity.

In the case of natural gas specifically, recent challenges in the production and provision of the natural gas commodity from wellheads both in Texas during Winter Storm Uri and in the PJM region during Winter Storm Elliott have highlighted the need for a comprehensive approach to cyber and physical security from the wellhead to the end user. A weak link in the chain for any fuel can bring challenges to all entities that depend on that chain. As a result, any effort should not be focused solely on pipeline facilities but also involve state and federal regulators

[8] *See, e.g.*, Ratification of Security Directive, TSA Security Directive Pipeline-2021-02, 86 FR 52953-01 (Sept. 24, 2021) ("Security Directive Pipeline-2021-02 requires Owner/Operators to take the following additional actions: Implement specified mitigation measures to reduce the risk of compromise from a cyberattack, drawing on guidelines published by the National Institute of Standards and Technology (NIST) and recommendations from CISA [Cybersecurity and Infrastructure Security Agency] as reflected in a series of recent alerts[.]").

that have authority over natural gas gathering, production, and processing facilities to ensure that there are consistent and robust cybersecurity standards throughout this critical supply chain.

PJM has worked with TSA as well as other key stakeholders to analyze the impact of cybersecurity or physical attacks on critical infrastructure that, in turn, could impact the provision of fuel to critical generation. PJM wishes to build on that positive working experience with TSA and serve as a resource to TSA as it continues this inquiry. PJM thanks the TSA for this opportunity to participate in this docket on a matter of critical significance to the reliability of the bulk electric system, the economy, and national security.

Respectfully submitted,

By: /s/ Mark J. Stanisz

Craig Glazer
Vice President–Federal Government Policy
PJM Interconnection, L.L.C.
1200 G Street, N.W, Suite 600
Washington, D.C. 20005
(202) 423-4743
Craig.Glazer@pjm.com

Mark J. Stanisz
Assistant General Counsel
PJM Interconnection, L.L.C.
2750 Monroe Blvd
Audubon, PA 19403-2497
(610) 666-4707
Mark.Stanisz@pjm.com

Dated: February 1, 2023