

October 3, 2019

Susan J. Riley
Interim President and CEO
PJM Interconnection, LLC
2750 Monroe Boulevard
Audubon, PA 19403

PJM Board of Managers
c/o Ake Almgren, Ph.D., Board Chairman
2750 Monroe Boulevard
Audubon, PA 19403

RE: Comments of Securing America's Future Energy (SAFE) on the Notice of Transmission Owners' Intent to File a New Attachment M-4 to the PJM Tariff Solely Applicable to the Planning of CIP-014 Mitigation Projects

Dear Ms. Riley, Dr. Almgren, and PJM Board Managers:

Securing America's Future Energy and its Energy Security Leadership Council (referred to herein as "SAFE") appreciate this opportunity to submit comments in response to the PJM Transmission Owners' (TOs) plan to file a new Attachment M-4 to the PJM Tariff that is solely applicable to the planning of the CIP-014 Mitigation Projects (CMPs). North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Standard, CIP-014-2, is a physical security standard that requires TOs to undertake a risk assessment, which must be verified by an unaffiliated third party, "to identify and protect [critical t]ransmission stations and [t]ransmission substations . . . that if rendered inoperable or damaged as a result of a physical attack, could result in instability, uncontrolled separation, or [c]ascading within an [i]nterconnection."¹

I. Background on SAFE

SAFE is a nonpartisan, nonprofit organization committed to strengthening U.S. energy and national security, by uniting prominent military and business leaders to develop and advocate for

¹ North American Electric Reliability Corporation (NERC), NERC Critical Infrastructure Protection (CIP) Standard, CIP-014-2, available at: <https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf>.

policies in this realm. It was founded in 2004 to reduce oil dependence for economic and national security reasons. SAFE's Energy Security Leadership Council is co-chaired by General James T. Conway, 34th Commandant of the U.S. Marine Corps, and Frederick W. Smith, FedEx Founder, Chairman, and CEO. The Energy Security Leadership Council is comprised of over 20 four-star Admirals and Generals who are among the most respected voices on U.S. national security. SAFE recently has launched a Grid Security Project (GSP), which is being led by 33rd Commandant of the U.S. Marine Corps, General Michael W. Hagee, in conjunction with General John W. Handy, former Commander of Transportation Command and Air Mobility Command, and General Carlton Everhart II, former Commander of Air Mobility Command.

SAFE views the reliability and resilience of the electric grid as critical to both the economic and national security of the United States. Physical security and cybersecurity pose significant, and growing, threats to the electric system, as do extreme weather events. Thus, it is critical to increase the security of the grid, as well as its reliability and resilience, beyond where measures heretofore have worked.

SAFE believes that utilizing competitive market constructs can enable and encourage investments and innovation that truly enhance grid reliability, resilience, and security.

II. Background and Context for This Issue

As the PJM Transmission Owners (TOs) note in their August 12 Notice of Intent (NOI):

Reliability Standard CIP-014-2 deals with [the] physical security of certain critical transmission substations; under the standard, the location of these substations and the consequences of their loss should damage occur are highly confidential. The purpose of CIP-014-2 is to identify and protect transmission stations and substations that, if rendered inoperable or damaged due to physical attack, could result in significant grid concerns – widespread instability, uncontrolled separation, or cascading. The [S]tandard requires Transmission Owners to physically protect these transmission stations and substations, which are identified through a screening process set forth in the [S]tandard. However, the physical security enhancements that CIP-014-2 requires do not fully mitigate the risks associated with the loss of these critical substations. Thus, without additional mitigation measures, the electric system is still vulnerable to long-term loss of load and loss of service to critical infrastructure should these substations be damaged.²

² PJM Transmission Owners, "Notice of Transmission Owners Intent to File a New Attachment M-4 to the PJM Tariff Solely Applicable to the Planning of CIP-014 Mitigation Projects (CMPs)," August 12, 2019, p. 1.

As members and representatives of the security and defense communities, we share the TOs' concerns and underscore that the physical security of certain critical transmission stations and substations is paramount to our local, regional, and national security. Every aspect of our economy and daily lives depends on a functioning electric system.

While CIP-014-2 is premised on the need to identify and protect transmission stations and substations from instability, uncontrolled separation, or cascading outages in an interconnection, the TOs' proposal is premised on the Standard allowing only the TOs to mitigate the identified risks, while the Standard is in fact silent on the processes to mitigate such risks.

We nevertheless concur with the TOs' premise that additional mitigation measures could be required to protect the electric system from loss of load. Moreover, we agree that the "construction of new transmission facilities may more effectively mitigate the risks associated with the loss of these critical substations than physical security enhancements alone."³

Above all, we wish to emphasize that we *can* protect our critical energy infrastructure and maintain our national security, while *also* opening up the processes to build or upgrade such regional infrastructure to competition. Contrary to the claim by the TOs, national security and market competitiveness are *not* mutually exclusive. We will elaborate in the following section.

III. SAFE's Concerns with the TOs' Rationale for an Alternative Vetting Approach to Solving These Challenges

We respectfully *disagree* with the TOs' proposed alternative approach and solution to "vetting certain transmission projects that will mitigate critical vulnerabilities associated with a subset of substations identified through TO compliance with NERC Standard CIP-014-2,"⁴ and their suggested rationale for the need for doing so.

More specifically, the TOs claim that: "they cannot implement [such a] solution without divulging highly sensitive information regarding the need for and location of the proposed project through applicable public processes. While the PJM Tariff and/or state processes offer some degree of protection of sensitive information through CEII requirements, the severity of potential system impact of divulging information about these critical substations warrants information protection beyond CEII."⁵

Again, SAFE respectfully disagrees for the following reasons.

³ Ibid.

⁴ Ibid.

⁵ Ibid.

- FERC defines CEII and, in compliance, PJM has procedures in place to which entities participating in stakeholder processes must adhere.⁶
- Indeed, highly-sensitive information referring to the *methodology and analyses* pertaining to how a critical facility is identified and verified rests solely with a utility or TO. However, the issue at hand here pertains to the outcome, i.e., the construction of a new transmission line, for which CEII procedures should be sufficient.
- We do not believe there is reason to require an alternative vetting process for doing so, and do not support the approach or argument that such transmission lines cannot or should not be allowed to be bid through a competitive process.
- Moreover, because these substations are critical, PJM (not the TOs) should drive the process to determine the appropriateness of any necessary additional transmission facilities. PJM is already tasked with the development of a Regional Transmission Expansion Plan (RTEP), as reflected in PJM's *Operating Agreement*, and as the entirety of the PJM States have stated,⁷ PJM is the appropriate entity to plan for these regional needs in its regional transmission planning process.⁸
- The TOs assert in the NOI that “the location[s] of these substations ... are highly confidential” – implying a higher standard, as a result of which stakeholders should be denied access. However, the Standard contains a process pursuant to which third parties can review such information, provided that confidential information is not publicly disclosed.⁹

⁶ “CEII is specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that: Relates details about the production, generation, transmission, or distribution of energy; Could be useful to a person planning an attack on critical infrastructure; Is exempt from mandatory disclosure under the Freedom of Information Act; and Gives strategic information beyond the location of the critical infrastructure. *Critical energy/electric infrastructure* means a system or asset of the bulk-power system, (physical or virtual) the incapacity or destruction of which would negatively affect: national security, economic security, public health or safety, or any combination of such matters.” Federal Energy Regulatory Commission (FERC), CEII definition, available at: <https://www.ferc.gov/legal/ceii-foia/ceii.asp>.

⁷ Organization of PJM States, Inc. (OPSI), Comments on “Attachment M-4, *Special Procedures Solely Applicable to Planning of CIP-014 Mitigation Supplemental Projects*,” August 12, 2019, available at: <https://www.pjm.com/-/media/about-pjm/who-we-are/public-disclosures/20190925-opsi-letter-regarding-transmission-owners-proposed-attachment-m-4.ashx?la=en>.

⁸ PJM, *PJM Operating Agreement*, Schedule 6, Section 1.1, available at: www.pjm.com/directory/merged-tariffs/oa.pdf.

⁹ Requirement B., 2.4, in CIP-014-2 provides that: “Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.” *See also* CIP-014-2 Requirement B, 6.4 (providing same).

- Parties bidding for such lines would be required to (and almost certainly already do) meet Critical Energy/Electric Infrastructure Information (CEII) procedures and would be required to keep requisite information confidential as such. FERC Order No. 1000 requires PJM to establish financial and technical qualifications for regionally-planned projects; if PJM chooses, it could implement additional qualification processes for developers bidding on these sensitive regionally-planned projects.
- The U.S. Department of Defense (DoD) has procedures for seeking competitive bids on projects, portions of projects, and for selecting competitively-bid development and production solutions, without divulging similarly confidential or sensitive types of information.
 - For instance, one Report cites some of the advantages of using a competitive process during the development phase of an acquisition with respect to the Joint Direct Attack Munition (JDAM): competition among two prime contractors “reduced development time by 33 percent, development cost[s] by 42 percent, and an average per-unit cost reduction of more than 50 percent.”¹⁰ This example also emphasizes that its competition “was held to more commercial-like standards . . . focused on performance characteristics and price, and, in this case, it was the competitive pressure . . . [that led to] an outstanding product.”¹¹
 - In addition, “[n]umerous historical studies have demonstrated the benefits of including competition during production in terms of cost savings—ranging from 12 percent to 52 percent.”¹²
 - For classified programs, DoD has contractors with the appropriate clearances to bid. This is true whether the project involves a new bid, such as a B-21 Bomber, or a project or equipment upgrade.¹³ With respect to business confidential

¹⁰ Gansler, Jacques, William Lucyshyn, and Michael Arendt, *Competition in Defense Acquisitions*, University of Maryland’s Center for Public Policy and Private Enterprise, School of Public Policy, partially sponsored by a grant from the Naval Postgraduate School, Revised February 2009, pp. 16-17, available at: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a529406.pdf>.

¹¹ Gansler, Jacques, William Lucyshyn, and Michael Arendt, *Competition in Defense Acquisitions*, University of Maryland’s Center for Public Policy and Private Enterprise, School of Public Policy, partially sponsored by a grant from the Naval Postgraduate School, Revised February 2009, p. 17, available at: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a529406.pdf>.

¹² Gansler, Jacques, William Lucyshyn, and Michael Arendt, *Competition in Defense Acquisitions*, University of Maryland’s Center for Public Policy and Private Enterprise, School of Public Policy, partially sponsored by a grant from the Naval Postgraduate School, Revised February 2009, p. 19, available at: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a529406.pdf>.

¹³ For instance, DD Form 254 is a resource for providing security requirements and classification guidance to a contractor. The DD Form 254 is a U.S. publication referenced in the Defense Federal Acquisition Regulations (DFAR) and applied to contracts involving access to classified information by U.S. contractors. And, this is for classified information, not just CEII information.

information, DoD would sign a binding Non-Disclosure Agreement (NDA) with the relevant company(ies), just like companies do with one another.

- In addition, the private defense industry has procedures by which they respond to such bids – and implement solutions – without divulging sensitive, business confidential, or proprietary information or intellectual property.

There is no reason that PJM could not replicate such competitive processes, perhaps similar to these types of processes within DoD. At PJM, however, the process should be simpler than is the case in the defense sector, given the complexity of various weapons systems, the length of time for their development, nature of classification, and more, where competition exists but the sensitive information, and sometimes even public knowledge of the bidding process, is still protected.

The pursuit of protecting national security interests and competition are not mutually exclusive.

IV. Conclusion

This PJM critical energy infrastructure issue has a clear regional and national security scope. However, it does not prevent a competitive transmission process from occurring, as the CIP-014-2 Standard clearly allows third parties to have access to relevant confidential information. There is no reason that PJM cannot implement competitive processes, while still protecting confidential, sensitive information.

If the existing practices are found to be insufficient, PJM should address changes to those practices that should occur to allow broad stakeholder participation in addressing solutions needed to provide for competitive, highest-value transmission outcomes.

Should you have any questions regarding this submission, please contact Ladeene Freimuth, SAFE's GSP Senior Advisor, at: lfreimuth@secureenergy.org. Thank you for this opportunity to comment on the matter at hand.

Sincerely,

/s/ General Michael W. Hagee
General John Handy
General Carlton Everhart II
SAFE's Grid Security Project

Cc: Transmission Owners, PJM; The Honorable Neil Chatterjee, Chairman, FERC