UNITED STATES OF AMERICA
DEPARTMENT OF ENERGY

Securing the United States Bulk-Power System	)	Docket No. DOE-HQ-2020-0028

COMMENTS OF PROTECT OUR POWER IN RESPONSE TO DOE REQUEST FOR INFORMATION ON SECURING THE UNITED STATES BULK-POWER SYSTEM

Protect Our Power submits the following comments in response to the United States Department of Energy's ("DOE") Request for Information regarding Securing the United States Bulk-Power System, issued by the DOE on July 8. 2020.[1] Protect Our Power respectfully requests that the DOE take these late-filed comments into account in the above-referenced docket proceeding.[2]

I. BACKGROUND

Protect Our Power, an independent, not-for-profit, non-partisan advocacy group, was formed in 2016 with the single purpose of improving the U.S. electric grid's resilience to attacks. Our work includes efforts to "reach consensus on the ideal balance of 'incentives and mandates' needed to facilitate action."[3] Our 25-member Advisory Panel is comprised of experts from across a range of grid-related disciplines, including base load and alternative electric power generation,

[1] *Securing the United States Bulk Power System*, Request for Information, DOE-HQ-2020-0028-0001, 85 FR 41023 (2020) ("RFI").
[2] As described herein, Protect Our Power has been engaged in a collaborative effort over the last months to gather stakeholder input and formulate its comments with regard to this important topic.
[3] About Protect Our Power, https://protectourpower.org/about-us/.

electric transmission and grid design and operations, government agencies (the Federal Energy Regulatory Commission ("FERC"), the Federal Emergency Management Agency ("FEMA"), the U.S. Department of Homeland Security ("DHS"), the Central Intelligence Agency ("CIA"), the National Security Agency ("NSA"), the Office of Science and Technology Policy ("OSTP"), the U.S. Coast Guard), academia, finance, and insurance.

Over the past few months, Protect Our Power has actively engaged in interactions and conversations with representatives of the electric power industry and security thought leaders to develop a well-rounded overview of this issue and potential solutions. This collaborative project (or "Collaborative"), was a joint effort between Protect Our Power and Governor Tom Ridge, the first Secretary of the U.S. Department of Homeland Security and now Chairman of Ridge Global, an international security and risk management firm. Governor Ridge is a leader in this field with a wealth of experience, and has been a valuable partner to Protect Our Power in this effort.

In order to facilitate an open exchange of ideas, Protect Our Power and Ridge Global sought comment from participants on an anonymous basis. This allowed participants to speak freely, and better informed Protect Our Power and aided our ability to share with the DOE the insights gathered in the Collaborative. The participants in the Collaborative provided a unique and broad range of perspectives, and Protect Our Power and Governor Ridge were in a position to collect this feedback and transmit the results of the collaborative to the DOE.

II. COMMENT

Protect Our Power supports the DOE's important goal to "enable a phased process by which [it] can prioritize the review of BPS electric equipment by function and impact to the overall

BPS."[4] Through the Collaborative, Protect Our Power initiated a survey to gather information on the positions of the participants on a variety of questions and issues related to the potential DOE process. The result of this survey is a general consensus on a comprehensive cybersecurity supply chain framework for the electric industry, with certain additional recommendations and preferences that received substantial support.

Participants in the Collaborative support a comprehensive cybersecurity supply chain framework, and provided valuable feedback on features that framework should address. Most importantly, the framework resulting from the DOE's process in this docket must be established in a collaborative manner. As DOE is aware, there is significant variation across the industry, and for any framework to be workable it must be designed with implementation across these varied systems in mind. The framework must also recognize the individual asset owner's ability to assess individual system risks and assume the responsibility for that assessment. A framework that is designed with input from those that will work within the resulting framework increases the likelihood that the framework will be effective.

If the DOE creates further approved or prohibited designations regarding supply chain integrity, then the Collaborative urges the DOE to take certain steps to ensure that the resulting materials are workable. Regarding lists of designations, the Collaborative supports the creation of an "approved list" of evaluated components/vendors, and/or in the alternative a prohibited component / vendor list "prohibited list" denoting components and suppliers which are evaluated, based on threat intelligence, to pose undue risk to the Bulk Power System. The DOE should also establish collaborative information sharing efforts, including federal intelligence organizations

[4] RFI at 41024.

sharing information with the DOE, and the DOE and other intelligence agencies actively receiving information from the industry to inform its creation/maintenance of these lists.[5]

For 2021, Protect Our Power recommends that the DOE establish a system for testing and evaluating the integrity of components, and establish priorities for testing and evaluating the most critical equipment. The preference of the Collaborative is that the industry establish or utilize existing entities, including non-governmental organizations, to undertake the role to establish and oversee the review and/or certification process, including recommending priorities for testing. A number of organizations have the ability to test equipment to ensure installation will not be a threat to the electric grid. For example, the National Laboratories, have capabilities to undertake such protocols and programs.[6]

However, as there are numerous components that will need to be evaluated, other qualified organizations also have the capability to test equipment. The decision on which organization should do the testing and evaluation is complex and the industry (asset owners and vendors), working together with DOE and the intelligence community, should recommend the types of equipment that should be tested by these different organizations to match the capabilities of the testing organizations with the criticality of the equipment. A determination of qualified testing

---

[5] This recommendation is consistent with Cyberspace Solarium Commission supply chain recommendations: "As a first step toward securing supply chains and enabling U.S. competitiveness, the U.S. government must work with industry, partner countries, and state and local governments to identify key equipment and the components and materials that make its assembly possible." Cyberspace Solarium Commission, "Building a Trusted ICT Supply Chain," CSC White Paper No. 4, at 20 (Oct. 2020). *Accord* Paul N. Stockton, "Securing the Grid From Supply-Chain Based Attacks," at 4-5 (Sept. 2, 2020), located at https://inl.gov/wp-content/uploads/2020/09/Stockton EOReport.pdf.

[6] We are aware of the recent partnership entered into by DOE's Office of Cybersecurity, Energy Security and Emergency Response (CESER) and by Schneider Electric. *See* Press Release – DOE CESER Partners with Schneider Electric to Strengthen Energy Sector Cybersecurity and Supply Chain Resilience (Sept. 23, 2020, at https://www.energy.gov/ceser/articles/doe-ceser-partners-schneider-electric-strengthen-energy-sector-cybersecurity-and. By submitting these filings, POP expresses its support for continued development of DOE's Cyber Testing for Resilient Industrial Control System (CyTRICS), which made such partnership possible.

organizations could build on the concept set forth in the NERC Physical Security Reliability Standard CIP-014-2, which sets forth qualifications for unaffiliated third party reviewers of security plans.[7] This system allows for flexibility because it does not limit certification to only one entity, but also provides sufficient requirements to ensure the certification process is sufficient and consistent.[8] The creation, and coordination, of this certification process would need to be closely coordinated with DOE and the industry. Regardless of whether the DOE pursues an approved list, prohibited list, certification process, or any combination thereof, the industry must be involved to create a list of priority components for testing that are essential for reliable system operations.

The DOE should consider creating tiers of equipment and/or testing.[9] Creation of tiers would encourage the evaluation of the most critical components first; focus industry and vendors on the most critical risks; and facilitate prioritization on the most critical components if testing capabilities are limited. This is an area where vendors could be involved in the process of providing input to the guidelines to ensure a more secure supply chain. This tier system could also address issues related to selecting "approved" or previously certified components, or whether the decision to select pre-certified or approved components in certain tiers, even at an increased cost,

---

[7] Requirement R6.1 of NERC Reliability Standard CIP-014-2 requires unaffiliated third party reviewers that is either "[a]n entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification[,] [a]n entity or organization approved by the ERO[,] [a] governmental agency with physical security expertise[,] or [a]n entity or organization with demonstrated law enforcement, government, or military physical security expertise." Similarly, industry in collaboration with DOE, could develop a list of appropriate qualifications for organizations to test equipment for integrity.

[8] The concept in the NERC Standard is an example that provides flexibility for use of third-party experts. We do not endorse promulgating a NERC Standard implementing a testing/certification process.

[9] The Department of Defense Office of the Under Secretary of Defense for Acquisition and Sustainment recently introduced a framework that includes five tiers, or maturity levels, with differing supporting practices and processes. This framework, the Cybersecurity Maturity Model Certification ("CMMC"), was introduced in January 2020, and more information is available here: https://www.acq.osd.mil/cmmc/index.html.

would be assumed to be prudent. At each stage — from testing, to certification, to compliance — a system of tiers would help focus the conversation and ensure that resources are being directed at the most essential components and protecting against the most significant risks.

For components that are designated as prohibited, the DOE must consider the practical implications of this designation. These considerations include whether, and to what date, these designations are retroactive, and what actions entities that already have these components installed on their systems, purchased, or contracted must take. As DOE demonstrated with its Prohibition Order Securing Critical Defense Facilities,[10] committing to implement this order only for future transactions — and not retroactively — will help support security objectives without creating undue strain on current operations.

Additional areas which DOE needs to address to comprehensively mitigate supply chain risks are legal and regulatory issues relating to 1) cost recovery and 2) liability protections to implement a testing program. The procurement process for these critical components often involves years designing, sourcing, manufacturing, and testing equipment to validate the equipment's security and operational performance. Introducing further security testing measures — such as those with the National Laboratories — into this process would provide additional confidence in the equipment's security and valuable insight into supply chain vulnerabilities. This added value, which is to the ultimate benefit of national security and electric customers, however, comes at a significant financial cost.[11] As a result, DOE must work with its

[10] U.S. Dep't of Energy, Prohibition Order Securing Critical Defense Facilities (Dec. 17, 2020), 6450-01-P, available at: https://www.energy.gov/sites/prod/files/2020/12/f81/BPS%20EO%20Prohibition%20Order%20Securing%20Critical%20Defense%20Facilities%2012.17.20%20-%20SIGNED.pdf.

[11] Cost recovery issues likely will also be faced by entities purchasing higher cost components from non-adversarial nations, rather than banned lower cost equipment, as well as those entities that may be required to "rip and replace" banned equipment.

government and regulatory partners to improve cost recovery and reduce barriers to these security investments which are a joint industry and government priority and a national imperative.

Further, in the National Defense Authorization Act for Fiscal Year 2020, Congress granted liability protection to utilities that support the government's efforts to analyze grid equipment for cyber vulnerabilities.[12] We appreciate Congress's recognition of the importance of such measures and encourage DOE to work with its partners to expand these liability protections to include related activities, such as responding to Grid Security Emergencies,[13] as doing so will further enable the type of public-private collaboration necessary to combat the significant supply chain threats we face today.

Protect Our Power's Supply Chain Collaborative expects to continue its exploration of all dimensions of the challenges of making the power industry's supply chain more secure. The result of these collaborative discussions can assist the DOE in creating a workable framework for designation and enforcement on this essential issue. Addressing issues of implementation and workability at this stage of the process reduces the risk that the framework the DOE sets forth will encounter implementation issues, and a more collaborative process serves the DOE's interest and benefits all stakeholders and the security of the grid as a whole.

III. CONCLUSION

For the foregoing reasons, Protect Our Power encourages the DOE to consider the recommendations herein.

---

[12] *See* Section 5726 of the National Defense Authorization Act for Fiscal Year 2020, Public Law 116-92 (Dec. 20, 2019), 133 Stat. 1197, 2179.**]**

[13] Grid Security Emergency authorities here references those authorities granted to the Secretary of Energy under the Fixing America's Surface Transportation Act, Public Law 114-94 (Dec. 4, 2015), 129 Stat. 1773 (Section 215A of the Federal Power Act).

Respectfully submitted,

/s/ James Cunningham

James Cunningham
Executive Director
Protect Our Power
37 North Orange Ave., Suite 500
Orlando FL 32801
Telephone: 516-316-9758
jcunningham@protectourpower.org

Dated: December 21, 2020