UNITED STATES OF AMERICA
DEPARTMENT OF ENERGY

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

COMMENTS OF PROTECT OUR POWER IN RESPONSE TO DOE REQUEST FOR INFORMATION ON CONTINUED SECURITY OF THE UNITED STATES CRITICAL ELECTRIC INFRASTRUCTURE

Protect Our Power submits the following comments in response to the United States Department of Energy's ("DOE") Request for Information on Ensuring the Continued Security of the United States Critical Electric Infrastructure, issued by the DOE on April 19, 2021.[1] Protect Our Power respectfully requests that the DOE take comments into account in the above-referenced docket proceeding.

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."[2] 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, electric transmission and grid design and operations, government agencies (the Federal Energy Regulatory Commission ("FERC"), the Federal Emergency Management

[1] *Ensuring the Continued Security of the United States Critical Electric Infrastructure*, Request for Information, DOE-HQ-2020-0028-0001, 86 FR 21309 (2021) ("RFI").
[2] About Protect Our Power, https://protectourpower.org/about-us/.

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.

Protect Our Power submitted comments related to these subjects in response to the DOE's prior Request for Information [3] on *Securing the United States Bulk Power System*, which are attached as Attachment 1 hereto for ease of reference. In the intervening time, Protect Our

[3] *Securing the United States Bulk Power System*, Request for Information, DOE-HQ-2020-0028-0001, 85 FR 41023 (2020) (the "BPS RFI").

Power has continued to engage with experts through the Collaborative, and the further learnings obtained through these sessions are incorporated into these comments.

II. COMMENTS

Protect Our Power supports the DOE's important goal to "[develop] recommendations to strengthen requirements and capabilities for supply chain risk management practices by the Nation's electric utilities."[4] The RFI clarifies that these recommendations will build on, and where appropriate modify, prior executive agency actions. 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 initiated in the BPS RFI. 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.

The DOE's questions on this front are encouraging, and show a focus on utilizing existing mechanisms and authority, as well as innovative tactics, to result in a comprehensive plan that will fully address this critical issue. As the DOE's RFI recognizes, addressing the complex and developing risks facing the electric grid will require an all-hands-on-deck response that includes full participation from all relevant entities. In particular, Protect Our Power is encouraged by the RFI's distinction that there are both immediate concerns that can be addressed using emergency powers and long-term concerns that will require a comprehensive long-term strategy.[5] This avoids the potential pitfalls of acting quickly and neglecting to establish continuing safeguards and of developing long-term strategies while neglecting to address

[4] RFI at 21310.
[5] *Id.*

immediate risks. Protect Our Power has engaged with various stakeholders on issues of grid security and both short-term and long-term solutions, and appreciates the opportunity to share these findings with DOE.

a. Development of a Long-Term Strategy

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

A national effort is required to enhance security of our most critical infrastructure, the electric grid. This requires federal, state and local governments to work together in reaching a consensus to implement a coordinated, comprehensive program that will dramatically improve the resilience of the existing electric grid now. Access to expertise, relevant information and money are the essential ingredients of all efforts to improve grid security, especially at the State and local level. Such an effort would require a national program that would provide needed expertise and ongoing, updated guidance to state commissions that regulate retail distribution utilities to ensure their oversight is advancing grid security within each state and the District of Columbia. Independent reports confirm most state regulatory commissions need funding and expertise to take the lead within their state.

DOE, DHS, and the National Association of Regulatory Utility Commissioners ("NARUC") should form audit teams to provide guidance to local and state government agencies as part of national effort to improve timeliness of information flow and coordination as well as sharing and promoting awareness of best practices to overcome the threat of cyber attacks. Also, the acceleration of efforts to build and expand broadband network for electricity-only operations will enhance overall security of the electric grid.

Finally, Indian Tribes are served by Investor Owned, Rural Co-ops and Municipal Utilities that have their own unique financial needs that must be met to facilitate and encourage the investment needed to dramatically improve grid security in their areas. Grants, loans and regulatory initiatives that assure recovery of investments in grid security must be established. These funds could be used to also identify and expedite important technology transfer throughout the power community as well as create testing centers to assure the integrity of power industries supply chain. In addition, funding the development of a skilled workforce with incentives to assure the availability of talent on state and local level will provide the sustainable technical protection needed.

ii. **Question A.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?*

Protect Our Power has formulated a series of positions from its own policy analysis and from the results of the Collaborative. These positions are informed by discussions with representatives of electric generation, transmission, and distribution systems, as well as recently with developers of distributed energy resources and vendors of IT and equipment. Protect Our Power feels that a broad range of opinions and expertise, including from non-utility entities like IT vendors, is essential to avoid crafting a set of recommendations that when implemented prove incomplete or impractical.

Protect Our Power addressed this issue in detail in its December 21, 2020 with the comments in response to the BPS RFI, which are incorporated here. Furthermore, Protect Our Power can respond specifically to this inquiry by reiterating that it is difficult for the industry to

establish or recommend specific criteria for the evaluating propriety of foreign interests in the supply chain but we can opine that:

- A list of approved vendors is generally preferred
- A list of prohibited vendors would be otherwise useful
- Regardless of the nature of such a listing, such lists should be established and maintained and updated

These list should be created, and updated, using information that is sourced from robust information sharing between the DOE, DHS, the Department of Defense ("DOD") or other security and national defense agencies, and also with information shared from and to the industry. The lists should be updated with sufficient frequency that they can be treated as having "evergreen status." If the lists are updated on a regular but infrequent basis, then the emergence of new products or vendors may cause an ongoing issue.

While not specifically responsive to this particular inquiry about criteria, Protect Our Power believes that regardless of the nature of the ownership and control there needs to be clearly established enterprise risk management, cybersecurity risk management, and equipment / procurement management protocols for any vendor of IT or equipment to the electric sector. The DOE can and should work with regulators to establish such guidance, as described in Protect Our Power's answers to questions A.3 and A.4, below.

Protect Our Power is of the opinion that testing and evaluation of IT and equipment is advisable and generally supported by the industry, and Protect Our Power previously commented and now reiterates these positions on potential testing regimes.[6] The testing regime should include two essential pillars: 1) there should be tiers for testing of equipment based on the critical nature of the components, and 2) such testing would result in a certification that that the industry

[6] See Protect Our Power December 12 Comments at 5.

could rely upon. A tiered system helps both to focus the urgency of testing certain equipment as well as to manage costs. One potential cost-saving measure associated with the tiers could be that if the DOE determines, for example, that testing should be under the purview of the National laboratories, it could allow that testing for low-tier components could be performed by other third-party vendors. A tiered system allows for flexibility in implementation as well as flexibility to adjust the testing structure based on experience once it is implemented. The value of a certification that the industry can rely on provides necessary stability for utilities in making component purchasing and installation decisions.

While a certification that can be relied on can address the issue going forward, when approved/prohibited lists and testing requirements are implemented there will be a number of programs or equipment that are currently in use or installed and otherwise subsequently deemed to be non-approved / prohibited. Protect Our Power is also of the opinion, particularly informed by the industry deliberations, that any guidelines for use of IT or equipment that is currently in use or installed and otherwise subsequently deemed to be non-approved / prohibited, should be then evaluated three main concerns in mind: 1) Consequence-Based Risk Assessments; 2) prioritization of testing of equipment; and 3) and/or evaluation of the risk of vulnerability balanced against the cost of replacement or need to undertake immediate testing. For security reasons, as well as practical and cost concerns, the requirements implemented by the DOE should recognize that all non-approved / prohibited components or programs are not created equally, and some components necessitate immediate removal while others may be able to be phased out or removed on a longer timeline.

Regardless of how the DOE determines to evaluate security of components and/or programs, Protect Our Power has very clearly commented in the public domain that these

protective measures will require additional costs that will be borne by either ratepayers or taxpayers. Protect Our Power believes that investments to secure the electric grid are necessary regardless. Protect Our Power also believes that the DOE should work actively with FERC, State regulators and industry to evaluate and provide research or education to ensure cost recovery of additional costs due to higher-cost of allowed equipment over banned equipment.

iii. **Question A.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?*

Protect Our Power supports the DOE's interest in addressing the questions of how the DOE can facilitate these practices, as well as the cost benefit relationship of such actions, near to the outset of this initiative. These questions must be addressed early, and on a continuing basis going forward, in order to achieve a result this is practicable, able to be implemented, and appropriately balances costs and benefits to maximize the effect of each dollar spent.

While the industry has a desire to implement responsible and effective procurement practices, there needs to be direction as to what practices are effective and how such practices should be implemented. Protect Our Power has established through its Collective sessions that the industry and vendors have a desire to determine and maintain certain standards at the enterprise level around cybersecurity and integrity of vendor procurement.

One issue that the DOE should consider is that the entities that must act to secure the electric grid consist of a wide variety of utility sizes and means, as well as operational structures. The DOE must consider in establishing its requirements that these must be capable of application to investor-owned utilities from very large to very small, to municipalities, and to co-operatives or other organizations. While Protect Our Power will not opine on jurisdictional issues, a set of requirements could be useful on a voluntary basis even to entities that are not bound by it, and

can prove useful in centering the conversation and providing a universal set of terms and priorities. Likewise, vendors may implement these practices that are not strictly subject to any DOE policies or requirements.

Addressing cost recovery concerns is essential to developing requirements that re actually able to be implemented and have an effect on grid security. While there are many security measures that can be implemented, at various levels of effectiveness, these technologies are costly. On a macro level, the increased cost of increased protections is justified due to the importance of ensuring national security and economic and physical well being of the nation. However, from a practical perspective, not every added security measure is worth its expense. The DOE is in a position to leverage the experience and expertise of utilities nationwide to analyze the cost versus impact of various measures in order to determine where funds are best spent. In addition, an absolute set of rules that would require a significant investment to comply with would not be feasible for many rural and/or public power utilities. Providing some flexibility for utilities with funding issues will ensure that the highest priority security developments can be implemented in a timely fashion.

iv. **Question A.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?*

As touched on above, DOE should set up formal testing and evaluation program of critical equipment, working with electric system owners and operators and vendors to prioritize equipment for testing. While it would be ideal to require testing of every potentially harmful component, the scale of the electric system, as well as scale of testing resources, require the DOE to prioritize and establish tiers with different requirements. A priority system can also mitigate

the risk of delays resulting from the implementation of the DOE's requirements causing an influx of components requiring testing.

The equipment and software to be tested should be prioritized based on Consequence-Based Risk Assessments. The DOE can leverage the existing frameworks to support its requirements, including expanding existing DOE programs such as CyTRICS. Because of the scale of the testing operation, the DOE should also leverage the private sector. Since there will be a large amount of equipment and software from multiple manufacturers (including equipment and software supplied by lower tiered vendors), a testing and evaluation process should allow for private testing and evaluation of equipment/software that need not be performed at National Labs. In order to facilitate this, the DOE should work with owners, operators and vendors on issues relating to confidentiality and intellectual property. To reduce the need for continuous testing in the future, the outcome of the testing can be used by DOE to develop lists of approved/banned vendors.

The DOE should work to increase technology transfer of DOE/US Government developed technologies such as CRISP, the Cybersecurity Risk Information Sharing Program. The DOE developed this platform to facilitate the timely bi-directional sharing of unclassified and classified threat information among energy sector stakeholders, and it will be a very useful tool for the information sharing that will be required to properly develop security requirements, as well as to implement them going forward. Because of the cost of some of the equipment to smaller owners and operators, there may need to be provisions to share costs.

It is important that the policies and requirements the DOE promulgates be flexible. Because types of equipment that may be banned will continue to change (including equipment that is found to include questionable parts from lower tiered vendors), mandatory reliability

standards are ill-suited. A flexible framework, with established protocols for modification of the framework where necessary, is an appropriate means to implement these standards.

The DOE should work with Federal and State regulators, as well as electric system owners and operators, to establish processes for supply chain procurement and risk management, as described in response to Question A.2, above. These processes should include the ability to audit the cyber supply chain processes or vendors and for DOE/owners and operators to share the results within the industry, and possibly with other critical infrastructure sectors that use the same equipment. DOE should work collaboratively with the industry and vendors on appropriate scope of such audits, which similar to CMMC, would have different attributes depending on the criticality of the equipment. Sharing the results, subject to appropriate confidentiality is necessary to avoid duplication.

b. Prohibition Authority

i. **Question B.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?*

The DOE should use a full set of tools to include Prohibition Orders, as well as lists of approved/banned vendors for equipment and software installed on the electric distribution system. There a numerous types of equipment and software installed on the distribution that if compromised could result in interruption to critical loads such as distribution automation equipment and software; distribution control centers; communications equipment; and smart

inverters connecting DERS.[7] Compromised equipment on the local distribution system can cause severe harm to national security and health and safety of the US.

While Protect Our Power will not opine on jurisdictional questions, the DOE should utilize all the powers available to it to prevent compromised equipment from being used on the electric system at any level, especially when it has determined that a certain component or components pose a risk to the system. The fact is that almost all load is served by distribution facilities rather than directly from the transmission system. DOE should consider how to provide research or educational resources and collaborate with both FERC and state utility commissions to establish how any such directives could be most effectively implemented in cooperation with state oversight of distribution systems

ii. Question B.2: *In addition to DCEI, 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?*

Yes. Losing electric supply to other critical infrastructure sectors can have a severe impact on the US economy and on the people's health and safety. For example, loss of service to water treatment facilities affects all residents. The critical infrastructure sectors identified are essential in day-to-day life but are even more important in the event of a large-scale disaster, which could include an attack on our national electricity infrastructure. The ability to communicate, obtain emergency services and/or medical care, and travel by roads or public

[7] *See A Review of Power Industry's Supply Chain Security Risks,* Ridge Global (prepared for Protect Our Power), February 20, 2020, available at https://protectourpower.org/2020-cyber-risk-report.pdf; *see also Potential Electric Grid Vulnerability from Cyber Enabled Foreign Actors,* Ridge Global (prepared for Protect Our Power), available at: https://protectourpower.org/wp-content/uploads/2018/11/Ridge-Global-and-Potential-Electric-Grid-Vulnerability.pdf.

transportation will increase in importance in a scenario where portions of the electric grid are impaired.

In addition to the criticality of these other sectors (including using the same or similar control and communication equipment), there are interdependencies between the electricity subsector with these other criterial infrastructure sectors, especially the natural gas/oil subsector and the communications sector. As an example of these interdependencies, during the February 2021 extreme cold in ERCOT, generators were unable to operate because their supply of natural gas was interrupted. In addition, when ERCOT initiated load shedding, some natural gas production and transmission facilities had their electric supply interrupted, further reducing the supply of natural gas.

In order to ensure that these critical services are not interrupted, it is appropriate for the DOE to specifically address electric infrastructure serving other critical infrastructure sectors including communications, emergency services, healthcare and public health, information technology, and transportation systems, and national and defense critical infrastructure.

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

As described above, we believe that DOE should use all its tools to protect the electric supply to critical functions. Just by its definition, National Critical Functions are those that "their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[8] The DOE's

[8] *See* Cybersecurity & Infrastructure Security Agency National Critical Functions webpage, available at https://www.cisa.gov/national-critical-functions.

prioritization of electric infrastructure serving other critical systems should include infrastructure that enables the national critical functions.

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

In order to enable utilities to identify critical infrastructure within their service territory that would enable compliance with such requirements, the definitions of critical infrastructure must be clear and unambiguous. If that is done, then subject to the limitations below, utilities should be able to identify critical infrastructure to which they provide electric service.

It is important to understand that in general, distribution facilities serve a variety of loads, i.e., facilities may not be dedicated to serve only critical infrastructure. As part of load shedding programs, utilities already identify (to the extent they know) critical loads, including customers such as hospital, police stations, natural gas compressors, customers needing life support, water treatment and processing plants. Moreover, the same equipment is used throughout the distribution system whether serving critical or non-critical loads.[9]

However, there may be cases where utilities are not aware of critical loads within their service territory. For example, there may be critical defense facilities of which the utilities have not been notified are critical due to the need for secrecy. Second, some customers, such as those using life support equipment, may not have informed the utility of their needs or may not know that they need to inform the utility of their special needs. Following the February 2021 extreme cold in Texas, there was confusion of some natural gas production facilities as to whether they

[9] While utilities use the same equipment throughout their system, for 'rip and replace' situations, priorities need to be set as to which critical loads have electrical equipment replaced first. In such a case, DCEI, other critical infrastructure loads, National Critical Function loads should have banned equipment replaced before other loads.

were critical facilities and/or the process to notify the utilities. This goes to the first point, that the definitions need to be clear and unambiguous.

DOE needs to work with state regulatory agencies to review program and processes to identify critical loads. DOE also needs to work with DOD and other national security organizations on how to ensure electric service to critical facilities of which the utility may be unaware are protected. Because there may be critical facilities of which the utility is not aware for the reasons stated above; because loads are constantly changing; because distribution equipment is used throughout an electric system; and because in general distribution facilities serve critical and non-critical loads, it may be best that any Prohibition Order or list of banned or acceptable equipment and software, apply to the entire distribution system.

III. CONCLUSION

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

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: June 7, 2021

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