UNITED STATES OF AMERICA
BEFORE THE
DEPARTMENT OF ENERGY

Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure

COMMENTS OF THE AMERICAN CLEAN POWER ASSOCIATION

The American Clean Power Association ("ACP")[1] appreciates the opportunity to submit comments on the Department of Energy's ("DOE") Request for Information ("RFI")[2] seeking input from stakeholders to inform DOE's development of recommendations to prevent foreign exploitation and attacks on U.S. critical infrastructure including the electric grid and relevant supply chains. ACP and its members support consideration of ways to mitigate such risks and the broader goal of enhancing critical infrastructure security. As the largest national trade organization that represents utility-scale wind and solar energy, energy storage, and electric transmission developers, among others, ACP has a material interest in any actions DOE implements based on the information collected through the RFI.

For the reasons discussed below, we encourage DOE to leverage the existing activities, guidance, and tools already being used by clean energy companies, as well as others in the electric sector, and partner closely with industry stakeholders to address the

[1] ACP is the national trade association representing the renewable energy industry in the United States, bringing together over 1,000 member companies and a national workforce located across all 50 states with a common interest in encouraging the deployment and expansion of renewable energy resources in the United States. By uniting the power of wind (both land-based and offshore), solar, storage, and transmission companies and their allied industries, we are enabling the transformation of the U.S. power grid to a low-cost, reliable, and renewable power system. Additional information is available at http://www.cleanpower.org.

[2] 86 Fed. Reg. 21,309 (Apr. 22, 2021), *available at* https://www.govinfo.gov/content/pkg/FR-2021-04-22/pdf/2021-08482.pdf.

grid security issues raised in the RFI, rather than creating and/or imposing an entirely new and untested set of requirements. We look forward to working collaboratively with DOE and other industry stakeholders to address these important issues in the long term.

I. Background and General Comments

Our member companies currently engage in many activities that underscore the seriousness with which they take the role of ensuring the continuous, reliable, and resilient operation of the electric grid. Understanding that sophisticated adversaries could potentially target supply chain vulnerabilities with the intent to attack the electric grid, ACP members have already developed measures that supplement the electric power sector's efforts to address grid-related threats. Our member companies employ a variety of existing tools, methods, and programs to strengthen the Bulk-Power System ("BPS") and seek to enhance, adapt, and add to these tools as threats evolve. In fact, ACP members are continually maturing capabilities in this area to effectively monitor and protect important grid facilities, systems, and resources, including identifying and implementing a variety of enhanced controls to address supply chain risks.

Our members follow a multi-layered approach to security that encompasses integration of leading industry standards, guidance, and, in some cases, compliance with rigorous, mandatory, and enforceable reliability standards and regulations. These key tools, tactics, strategies, programs, and partnerships protect and support grid reliability and supply chain risk management programs. These measures are numerous, and they can be grouped into four general categories:

1) Deploying technologies that improve situational awareness and ensure actionable intelligence;
2) Ensuring threat indicators are communicated at the right time to the right people in industry and government while also being assessed for impact and needed action internally;

3) Preparing for and exercising coordinated responses to both natural and malicious threats to energy grid operations; and
4) Working closely with other interdependent infrastructure sectors to enhance preparation and responses to threats.

Of note, under Federal Energy Regulatory Commission ("FERC") oversight, the BPS and much of the clean energy industry is subject to mandatory and enforceable North American Electric Reliability Corporation ("NERC") reliability standards that include a robust framework for operations, planning and security. FERC and NERC, in collaboration with the industry, have invested more than a decade of significant work and substantial resources to enhance BPS reliability and security through the development and implementation of Critical Infrastructure Protection Reliability Standards ("CIP Standards"). These standards focus on the high-risk assets within critical infrastructure and include cyber and physical security mandates. They are developed through complex industry participation processes and aligned with the National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("CSF"). [3] This approach results in requirements that inform and guide supply chain and cybersecurity programs for all organizations, even where CIP is not applicable.

The CIP Standards take a broad and "defense-in-depth" approach to cybersecurity for cyber systems and their associated cyber assets, addressing vendor remote access and software authentication and integrity risks and extending cybersecurity requirements from the internal operational environment to the external procurement of cyber systems. To keep up with the ever-evolving threats to the reliability of the BPS, the CIP Standards are routinely updated. Certain standards also require operators to conduct periodic assessments of their assets to determine which assets fall within the updated CIP

[3] National Institute of Standards and Technology. The NIST CSF is a leading practice, nationally recognized cybersecurity framework guiding the design and implementation of robust cybersecurity programs and includes supply chain security within the defined domains.

Standards, based on risk to the system. Many of the CIP Standards also require certain protections so that the BPS can resist, absorb, and rapidly recover from coordinated cyber attacks.

Importantly, the CIP Standards allow regulated entities to choose compliance approaches best tailored to their systems. Clean energy companies dedicate resources and personnel to implement customized and proprietary in-house processes, procedures, and technology to comply with the CIP Standards. This built-in flexibility allows these standards to be effective, while providing a solid foundation for strengthening the industry's supply chain and security posture.

Given the dynamic threat environment, clean energy companies have developed layers of protection beyond CIP Standards. Companies tailor security programs to their unique operating and business environments to mitigate supply chain and security risks as threats and vulnerabilities change. Specifically, recognizing this critical priority over the last few years, our members have established programs that support risk-based flexible approaches to deal with the ever-changing threat landscape. This risk-based, defense-in-depth approach to designing and implementing programs, controls, and supporting security tools ensures critical assets are prioritized. In addition, there have been focused efforts by industry forums and collaboratives, such as the North American Transmission Forum ("NATF"), North American Generator Forum ("NAGF") to help guide such efforts. Examples of these voluntary actions include:

- Conducting proprietary in-house risk assessments and supply chain protocols, which can include methodology recommended by DOE's Cybersecurity Capability Maturity Model ("C2M2") and NIST Tier 1, 2, and 3 risk level assessments.
- Performing routine audits that conform to ISO 27001/27002 or other industry-recognized information security policies.

- Routine data sharing through Electric Sector's Information Sharing and Analysis Center ("EISAC"), including using supply chain risk sharing community tools such as the Asset to Vendor Network for Power Utilities ("A2V"), a data repository that collects and monitors data by participating utilities.
- Participating in Department of Energy security programs at the Idaho National Laboratory and the National Renewable Energy Laboratory.
- Engaging with federal agencies responsible for protecting the grid, including using and routinely contributing to resources provided by the Cybersecurity & Infrastructure Security Agency (CISA), such as the Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT").

Given this existing focus and prioritization by the clean energy industry—indeed, the entire electric sector—the best path forward would be to leverage existing standards and guidance through enhanced directives on how to implement recommended processes, rather than creating and/or imposing an entirely new and untested set of requirements (e.g., a "Prohibition Order") that could inadvertently disrupt existing grid security measures. This approach would maximize efficiencies and help achieve national security objectives faster and with fewer roadblocks, for example by not impeding the Biden administration's goal of reaching a 100 percent clean energy economy by 2035. It would also avoid conflicts with the ongoing cyber and physical security work occurring daily at clean energy companies across the nation through existing, time-tested programs.

In considering future measures, DOE should consider how any proposed measures would affect the market for critical equipment and impact day-to-day grid reliability. For example, if certain suppliers are prohibited by DOE, but there are few commercially viable alternatives for clean energy components, market or production capacity may be stretched, thus restricting access to key equipment classes that are

necessary for electricity generation. As such, DOE should avoid implementing any measures that would necessitate immediate and widescale equipment replacement unless the measure is determined to be truly critical to prevent a major security risk that cannot otherwise be mitigated.

DOE should also consider how a proposed action could stress limited market capacity by creating a surge in demand and could introduce reliability challenges if supply cannot meet this new demand immediately. Companies would also face significant material lead time increases if demand is consolidated in fewer suppliers. In other words, DOE should appropriately consider the time and rigor involved to qualify alternative suppliers and equipment and balance those costs against the risk being addressed and availability of other options to sufficiently mitigate the risk before taking any actions.

DOE should also consider whether prospective measures would likely increase costs to electric customers. Renewable power generation and storage equipment are typically manufactured to customer specifications and have long lead times that are sensitive to raw material availability and complex logistics chains and represent significant investments for electric companies. Further, removing certain suppliers from established markets may reduce already limited competition and drive up costs for critical equipment. Given the complexity and length of the procurement and manufacturing process, DOE should take into account that the sources of supplier equipment and the parts that make up the equipment come from diverse locations, and maintaining this supply chain is an important tool for mitigating risks that can impact grid security. Thus, DOE should ensure that any future approach avoids disrupting these established supply chains and markets and incorporates cost considerations to minimize the financial impact to customers to ensure the continued reliability and affordability of the nation's energy supply.

Any measures that DOE imposes could have unintended consequences for clean energy companies and other electric companies, grid reliability, consumer costs, climate

goals, security, and supply chains. If DOE determines additional measures are needed, a strategic, risk-based approach should be taken to ensure clean energy companies can better focus valuable resources on the highest priority threats. Specifically, we encourage DOE to prioritize and limit any future actions to high-risk threats and/or assets. This includes clearly identifying any components and subcomponents that are and are not covered so clean energy companies can focus time, money, and efforts on the appropriate items that truly pose a risk to critical infrastructure.

Additionally, to the extent DOE undertakes any action for *existing* equipment, due to the potential scale of impact, DOE should develop a prioritized and phased approach where the most susceptible equipment and highest impact equipment are addressed first. Once the equipment is identified, addressing potential concerns could come in the form of a process for identifying the vulnerability, and testing to determine the likelihood of a security incident, misoperation, or damage to equipment, with replacements being used only when all other options are not viable.[4]

In sum, to the extent DOE pursues any future measures, they should be implemented in a manner that reflects the clean energy industry's existing measures and expertise in supporting clean, affordable, safe, and reliable energy, as well as taking into account the following:

- Recognizing the existing risk-based, defense-in-depth philosophy and corresponding programs, controls and tools that are integrated as part of clean energy companies' security culture.
- Allowing for flexibility in implementation by recognizing that clean energy companies face unique threats due to their location, size, system design, customer base and security controls.

[4] One example of a reliability request with similar scale and impact within industry is the NERC "Facility Ratings Alert" initiative, which required entities do a risk-based full assessment of all system ratings to ensure actual field conditions, and not just design, were properly integrated into current facility ratings.

- Avoiding contradictory or duplicative guidance, standards, or regulations, as well as program activities, tools, or processes that are already widely used and continue to be developed by industry and government.
- Understanding that the equipment identified in the RFI is complex and interconnected with long lead times for design, procurement, testing and deployment.
- Considering that many assets/components may not pose a risk (e.g., non-programmable components) or that the risk may be able to be substantially mitigated at the entity level as part of strong change management, testing and production, and threat monitoring processes.
- Avoiding actions that affect the market for critical equipment, including disruptions to the use of existing equipment and availability of replacement equipment, and considering potential impacts to day-to-day grid reliability upon which our communities and customers rely for essential services.
- Exercising prudence by recognizing that any regulations that affect electric equipment markets may increase the equipment cost and the ultimate costs to electric customers.
- Considering that clean energy companies have ongoing projects already in development and any proposed mitigation actions may take months or years to implement effectively and could slow down the deployment of clean energy.
- Ensuring strong coordination is occurring at federal, state, and local levels to prevent a complex myriad of recommendations or regulations that will add to the already substantial volume of material and requirements entities designing and implementing programs must consider.

II. Answers to Request for Information Questions

A. Development of a Long-Term Strategy

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***?

As securing the bulk power system is an issue of national security, we support the centralized approach that DOE is taking to address these issues on the federal level. We recognize there may be a need for financial and possibly even technical assistance for states, tribes, or units of local government, as well as participants in the electric sector, that may not have the financial or human resources to develop or acquire the appropriate technologies or data in order to identify and mitigate risks in assets already deployed. These items often come at significant cost in today's market and some may not have the ability to obtain the information or resources needed to comply with any order or requirement established by the DOE. We support DOE's inclusion of these entities in developing collaborative resources, as appropriate, as explained in more detail in our answer to Question A.2 below.

A.2 What specific **additional actions** could be taken **by regulators** to ***address the security of critical infrastructure*** **and** the i**ncorporation of criteria** for **evaluating foreign** ownership, control, and influence into **supply chain risk** management, and **how can [DOE]** best **inform** those actions?

Additional standards or criteria are not needed; however, we would welcome better guidance, clearer directives and information about recommended priorities, broader access to real-time or enhanced information about threats and risks. Such information would enhance existing resources available to entities in applying risk assessment programs and controls to mitigate supply chain risk.

Focused, formal processes and controls to ensure critical infrastructure security has been a top priority for ACP, its members, and the industry for more than a decade. As discussed above, many entities are already applying rigorous controls pursuant to applicable NERC CIP obligations. And, others, who are not regulated, have leveraged guidance to develop and implement supply chain risk mitigation programs tailored to the specific organizational needs, size, scope, and scale of the potential impact for applicable potential risks.

All leading practice supply chain risk management programs include a Risk Assessment Methodology, which provides a detailed scoring mechanism with specific criteria to evaluate risks based on the entity's organizational profile (e.g., how its systems and networks are configured, what types of assets it has, its tools and access to systems, size, resources, and the nature of operational and other risks). The risk criteria also typically include factors related to foreign vendors, manufacturers, and services suppliers. How these are scored is typically dependent on what information the organization has about these vendors, which is collected through a variety of means (*e.g.*, cyber risk questionnaires, public information, patch and tool vendor bulletins and alerts from the ISACs, and similar agencies). Additionally, programs that include strong Security and Incident Event Management ("SIEM") and other threat management and monitoring tools allow organizations to automate certain activities to better inform this scoring system, and enhance monitoring of existing equipment or vendor risks.

If a vendor or product is determined to present additional risks, there are many actions an entity can take to mitigate or eliminate that risk. Some companies may determine that simply avoiding that vendor or product is the proper action. However, that may not always be possible. Availability of supply, cost-prohibitive alternatives, and the potential that the risk posed is to existing equipment that cannot be removed, can all factor into the individual entity's decision about whether to use a particular vendor or product. Applying increased or expanded monitoring controls and requiring heightened testing and pre-deployment practices within configuration and change management

programs, and even implementing firmware scanning, are all measures that may be able to effectively mitigate supply chain security threats within a system.

These efforts can be time-consuming and resource-intensive depending on the size, scale, resource options, and risk profile of the particular entity. There are several actions regulators, with support from DOE, may be able to take to better support these efforts with regard to foreign supply chain influenced risks and threats:

- Support the expansion of access to collaborative resources and programs that provide guidance and real-time information about threats to critical infrastructure. This includes real-time information about risks, an alert or prioritization scale, better information sharing across industry, and practical guidance with recommended actions for mitigation of these risks. Current approaches often do not include adequate information about the threat level, clear guidance with recommended actions that may be taken to mitigate and exclude participants supporting smaller utilities and organizations operating within the critical infrastructure. Balancing security against the amount of information and access will remain a priority, but any efforts here should also consider existing small organizations, entities, and information sharing venues (*i.e.*, EISAC, Fortress A2V Network) that support industry to ensure the underlying objectives of maximizing strong security and efficient implementation of responses.

- Support the development of a national database that allows critical infrastructure entities a single location to obtain information about the cyber and supply chain security practices of vendors and products being purchased and deployed in the critical electric infrastructure. This would eliminate the need for each individual entity and vendor to design, implement and respond to security criteria questionnaires, creating

significant efficiencies in the application of this element of supply chain risk management programs. A single national repository may also motivate vendors to provide more accurate information and ensure that regulated entities are implementing the processes and controls they identify.

- Support the development and implementation of a robust Software and Hardware Bill of Materials (SBOM/HBOM) program for manufacturers providing products used within any critical infrastructure.
- Support existing initiatives to continue to develop and improve publicly available supply chain risk management programs, controls and leading practice guidance (e.g., the NATF, the CISA ICS-CERT and NIST guidance materials).

As discussed above, additional requirements and industry obligations are likely unnecessary. However, to the extent DOE decides to take further action (e.g., expanding the applicability of existing FERC or NERC standards or developing additional requirements), it is imperative that DOE, FERC, NERC, and state regulators work together to coordinate and minimize the impact of additional requirements so that our member companies' administrative resources are used prudently on enhancing security, rather than managing complex and potentially conflicting regulation.

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

As stated previously, our members already employ company-specific responsible and effective procurement practices. In addition, some of our members are subject to the NERC CIP Supply Chain Security Standard (CIP-013), which requires regulated entities to take certain procurement actions and meet certain requirements. We urge DOE to first consider the existing actions that private entities take, such as the requirements of CIP-013, and then consider if additional regulation is needed.

Additionally, we urge DOE to ensure that critical electric infrastructure is formally defined, and that definition is understood by the entities that are subject to any new standards or regulations, so that there is no ambiguity in what is expected and what is not. Finally, any supplier information-sharing requirements should be flexible, so that entities can make their own risk-based procurement decisions.

As far as costs and benefits, the costs of DOE actions could be significant, depending on the depth of assessment required, the number of assets covered, and the specifics of the standards. However, without any details as to what a standard or regulation may look like, it is impossible for us estimate. Some impacts of a comprehensive testing and registration process, as outlined in this response, could result in higher costs for acquired products, reduced availability of products, increased time to procure products, and possibly even reductions in the reliability of the grid if replacement parts are not available due to restricted supply chains caused by losses of available components impacted by a Prohibition Order against certain manufacturers' source of components.

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

As discussed in our answers to A.2 and A.3, much of the industry takes steps to secure our supply chain, either through market-based voluntary measures or through compliance with FERC and NERC CIP standards. The previous administration did not achieve its goals in this area, in part because it issued overbroad, sweeping orders that failed to account for stakeholder guidance and existing measures. To the extent DOE does issue any guidance, regulation, or other information, DOE should keep the following principles in mind:

- Explicitly identify all products and services that it attempts to cover, including whether the guidance covers components or subcomponents of the product.
- Be specific regarding which countries, manufacturers, and/or systems are impacted by the controls established.
- Identify the specific parties to be regulated and at what level the parties are regulated (i.e., utility, OEM, Tier 1 supplier, O&M) and specify which actions each party is obligated to take.
- Specify requirements regarding when information is to be provided by manufacturers and developers to the regulating authority or any system or service for the collection of that information.

B. Prohibition Authority

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?

See answers to B.2 and B.3.

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?

As discussed in more detail below, a Prohibition Order similar to the December 2020 Prohibition Order would be overreaching, unnecessary, and problematic for both industry and for effective administrative implementation. However, if DOE does determine that a Prohibition Order is required, we agree that DOE should consider all critical assets and industries and not limit the order to the electric sector. Again, we would also encourage interagency partnerships and/or private-public partnerships to better explore these issues and ensure that all stakeholders have a chance to participate before any Prohibition Order is issued.

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***?

ACP believes that a specific Prohibition Order would be overreaching, unnecessary, and problematic for both industry and for effective administrative implementation. While it is difficult to comment on a Prohibition Order that has not yet been issued, we summarize below some challenges industry would face in attempting to comply with an overbroad Prohibition Order.

Our members often spend years and invest significant capital in determining what equipment is necessary and what suppliers have provided robust, secure, and reliable equipment. A sweeping Prohibition Order would easily undo years of budgeting,

engineering, and planning; and, in certain cases, it could result in entire clean energy projects being canceled due to lack of supplies or funds. Further, removing certain suppliers from established markets that do not presently have a U.S. manufacturing base may reduce already limited competition and drive-up costs for critical equipment.

Prohibition Orders may result in an outsized response and overly burdensome restrictions relative to the risk for specific organizations/entities. As noted above, a Prohibition Order may result in removal of a technology that may be necessary to operate but unavailable from any other source. Further, it may only address a known risk at a particular point in time, which would undermine overarching security objectives. The better approach is to continue to ensure organizations consider both immediate risks and long-term foreign threats as part of a comprehensive supply chain risk management strategy. Risk assessment methodologies should be developed with criteria that specifically integrates this strategy for selecting and implementing mitigation activities based on the universe of risks (up to and including selection of alternative products or suppliers). Under such an approach, entities would be responsible for employing appropriate mitigation where the component may introduce unacceptable risks to the supply of energy in critical facilities.

In addition, industry efforts may also be enhanced through public-private partnerships to accelerate private sector efforts around supply chain security, such as through federal government efforts to encourage transparency in supply chains so that critical infrastructure asset owners can assess cyber risk for themselves through existing solutions. This will help ensure that any future action avoids disrupting established supply chains and markets and incorporates cost-benefit considerations to minimize financial impacts.

In sum, we believe that a Prohibition Order is unnecessary for many reasons, and a "one-size-fits-all" order would not provide a workable solution for our members or for others in the energy industry. If, as DOE states, its goal is to create a "stable policy environment," DOE should not attempt to issue a blanket Prohibition Order without first

conducting further industry outreach, such as through a notice and comment rulemaking, and ensure that all interested stakeholders receive a seat at the table, including new market entrants as well as the legacy providers.

If DOE does issue a Prohibition Order, the order should be solution-oriented, targeting what DOE perceives to be risks that cannot wait to be addressed through a future rulemaking, guidance, or voluntary action. To eliminate uncertainty, any Prohibition Order should also be as specific as possible and limited in nature—clearly articulating the parties it intends to the regulate, the timelines DOE expects parties to comply within, and the actions DOE expects the parties to take.

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

Subject to the definition of "critical infrastructure," ACP believes that utilities should be able to identify critical infrastructure within their service territories, consistent with their existing responsibilities.

III. Conclusion

ACP appreciates the opportunity to provide feedback and information regarding this request and hopes to stay actively involved in this process as DOE moves forward and considers actions that may impact the clean energy industry.

Sincerely,

Gene Grace

General Counsel

Jo Jochum

Counsel

American Clean Power Association.
202-657-7434
ggrace@cleanpower.org