June 7, 2021

Submitted via *ElectricSystemEO@hq.doe.gov*

ATTN: Mr. Michael Coe
Office of Electricity
U.S. Department of Energy
1000 Independence Avenue SW
Washington, DC 20585

RE: **Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure (April 22, 2021); 86 Fed. Reg. 21309**

Mr. Coe:

The American Public Power Association (APPA), the Large Public Power Council (LPPC), the National Rural Electric Cooperative Association (NRECA), and the Transmission Access Policy Study Group (TAPS) (hereafter, the Associations) appreciate the opportunity to offer comments on the U.S. Department of Energy's (DOE) Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure and the implications for our members.

The American Public Power Association is the voice of not-for-profit, community-owned utilities. More than 2,000 public power systems provide over 15 percent of all kilowatt-hours sales to ultimate customers and serve over 49 million people, doing business in every state except Hawaii.

LPPC represents 27 of the largest state and municipally-owned utilities in the nation. LPPC's members are located throughout the nation, both within and outside the boundaries of regional transmission organizations and independent system operators. The members comprise the larger, asset-owning utilities in the public power community, owning approximately 90 percent of the transmission assets owned by non-federal public power entities.

NRECA is the national trade association representing nearly 900 local electric cooperatives and other rural electric utilities. America's electric cooperatives are owned by the people that they serve and comprise a unique sector of the electric industry. From growing regions to remote farming communities, electric cooperatives power one in eight Americans and serve as engines of economic development for 42 million Americans across 56 percent of the nation's landscape.

TAPS is an association of transmission-dependent utilities in located in 35 states. It is an effective voice in the fight for open and equal transmission access and for strong protections against the exercise of market power in electric markets. TAPS Supports vigorously competitive wholesale electric markets and a robust grid. It participates in policy proceedings at the Federal Energy Regulatory Commission, the Department of Energy and other federal agencies that deal with electric transmission and market power in

the electric utility industry. TAPS also testifies before Congress and educates members of Congress and their staffs on federal legislation issues related to competitive, reliable wholesale electric markets, open transmission access, and the need for a robust transmission grid."

We appreciate the opportunity to provide our perspectives on DOE's RFI below. The Associations strongly support DOE's efforts to provide assistance and information to the electric sector in managing the security of the electric grid. DOE has in important role to play in helping to support grid security. The Associations look forward to working together toward that end, and to benefiting from DOE's expertise and access to critical information.

As a replacement for Executive Order 13920 is considered, the Associations urge DOE to incorporate into its thinking these four foundational principles:

(1) New Measures Must Be Risk-Based: The consideration of any new standards, measures, or prohibitions must be calibrated to reflect the risk of the related infrastructure or activity to the nation's security or public health. The definition of Critical Electric Infrastructure in Section 215A of the Federal Power Act ("Critical Electric Infrastructure Security") provides an important touchstone for prioritization of these efforts, specifying that "Critical Electric Infrastructure" means "a system or asset of the bulk-power system, whether 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." Key elements of this definition focus attention on the bulk power system (as opposed to distribution systems), and on the impact that the incapacity of such system may have on national (not local) security, economics and public health or safety.

(2) Directives Should Be Clear, Prospective, and Scalable: Clarity in connection with any directives, with respect specifically to the facilities that are addressed, and the nature of any activity prescribed or prohibited, is critical. Ambiguity can be costly and time consuming and ultimately undermine the effectiveness of the directive. Further, directives should be prospective only, and effective only once all definitions and required regulations are in place. Again, ambiguity as to whether the directive applies to infrastructure already in place, or to activities and contracting already underway, will be both costly and may adversely affect grid reliability. Finally, where possible, directives should be scalable, in recognition of widely varying size and capabilities of affected electric utilities.

(3) Directives Must Be Cost-Conscious: Closely related to the precept that any new measures must be calibrated to reflect varied risks, DOE must be mindful of the cost of any directives. The cost of electric service is a key factor in the nation's economic health, and the reality of varying, but finite resources and budgets suggests that over-spending on security measures may compromise grid reliability in other respects. This is especially important to consumer-owned, not-for-profit public power utilities and rural electric cooperatives, who are owned by the consumers they serve and must bear any new costs imposed by new requirements.

(4) DOE Should Focus on Vendor Risks: The electric utility industry's ability to influence the security measures undertaken by industry suppliers is limited, and particularly so for smaller utilities. Though vendors are outside the direct authority of the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC), DOE may use its influence to affect supplier practices by encouraging suppliers to adopt shared security practices, and to foster security certification upon which the industry can rely.

Responses to Specific Questions

Development of a Long-Term Strategy

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

DOE could serve a vital role as a liaison between vendors and utilities as well as states, Indian tribes, and units of local government as they strive to better understand risk in the supply chain. Technical assistance that provides collaboration and coordination on best practices for procurement and/or testing and liaising with vendors would be most useful in our view. DOE serving as a liaison with vendors is especially important for smaller entities, such as public power utilities and electric cooperatives, who typically have less bargaining leverage in their procurements throughout the supply chain. Other examples of where federal support would be helpful include:

- Facilitating more sharing of threat intelligence with utilities, providing risk identification and mitigation support, and facilitating information sharing between states, Indian tribes, or units of local government.

- Expanding programs such as the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency's Requests for Technical Assistance without charge to smaller utilities such as public power utilities and electric cooperatives who may have less staff and resources available to improve their security posture.

- Providing support or assistance to help utilities meet (or exceed if additional national security risks are identified) the NERC supply chain standards (CIP-013) already in place.

The Associations encourage DOE to focus on scalable solutions calibrated to the level of risk and the size and resources of the relevant utility. DOE could do more outreach in regions determined to pose greater risk based on information, such as the amount of critical infrastructure located there, or areas identified by the federal government as particularly important to national economic stability. In any industry outreach, DOE should leverage the existing communication infrastructure that exists between NERC and the Electricity Information Sharing and Analysis Center (E-ISAC) and the industry through NERC alerts. DOE should make every effort to utilize NERC's industry expertise in evaluating the impact of threats and evaluating solutions.

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?

The concept of "foreign ownership, control, and influence" is very broad and the Associations encourage DOE to provide more detail on what it means to the department. Implementation under such a concept will be very difficult without further clarification from the information currently available. To the extent DOE moves in this direction, the industry would benefit from efforts by DOE and other government agencies to identify actionable information regarding threats from adversaries abroad. The Associations are concerned that utilizing this concept, even with more clarification from DOE, would create a substantial cost burden both directly on utilities for having to track country of origin for products and components, and indirectly through increased vendor costs due to the same requirements. Instead, DOE should develop its long-term strategy around protection of critical electric infrastructure based on risk. This risk assessment should be accomplished with the input of industry, vendors, other stakeholders, and other regulators with jurisdiction over the bulk power system. NERC issued multiple alerts in 2020 related to Executive Order 13920, *Securing the United States Bulk Power System,* requiring utilities to respond about equipment or vendors associated with foreign adversaries. DOE should consult with

NERC's E-ISAC on whether the responses to those alerts shed any new light on risks associated with equipment and systems serving the bulk power system posed by the supply chain.

The primary responsibility for demonstrating the security of their supply chain for all equipment, components, and sub-components used for critical electric infrastructure should rest with the vendors and manufacturers. Electric utilities do not regularly have access to information from the manufacturer of a finished product about who may have sub-contracted the design and/or manufacturing of the components they might purchase. The vendors and manufacturers hold this information, including the extent to which a foreign entity may play a role in their supply chain. It is critical that DOE work directly with equipment manufacturers and vendors to identify areas of concern before taking any action. Utilities should be an important and valued partner to DOE in these efforts. For example, DOE could work with manufacturers to identify a method of certification that can identify finished goods that comply with standards, including all sub-components. DOE could develop a standard for vendors of equipment that connects to the bulk power system that involves a defined process for review of code in software and chip sets for this equipment. Such approaches will be more effective than trying to replace equipment later found to pose a risk after it has already been installed.

The Associations urge DOE to focus on the extent to which existing standards have been successfully implemented in the electric utility sector to help frame the scope for any new regulations. If DOE sees risks that are not being addressed in the existing required NERC supply chain standards, DOE should consult with the FERC and/or NERC and provide actionable information that can inform appropriate standard revision. It would be burdensome on utilities, in particular smaller entities like public power utilities and electric cooperatives, to require them to report on supply chain requirements to more than one federal regulator.

If new regulations are developed, DOE should adhere to the following principles to best provide security improvements with the least amount of overhead:

- Prioritize compliance with any new requirements based on risk assessed to the bulk power system.

- Ensure that any new compliance requirements are not duplicative of existing FERC/ NERC standards, or other similar requirements imposed on bulk power system entities. NERC-CIP-013, Cyber Security – Supply Chain Risk Management, standards became effective on October 1, 2020. Sufficient time should be afforded for utilities to implement these standards and for NERC to assess their effectiveness before DOE considers imposing new requirements aimed at the same objectives.

- Phase in any new requirements to allow adequate time for compliance and avoid undue burden on utilities, taking into account multiple factors, including but not limited to, appropriate timing for outages, sourcing of long-lead time equipment, and other complexities that arise when maintaining bulk power system level equipment.

- Account for how any new such regulations could impact contracts that utilities have in place prior to a new regulation for ongoing procurement of equipment and allow for appropriate timelines to adjust these contracts if needed to avoid service interruptions.

- Clearly identify, down to the sub-component level if necessary, any assets that will need to be evaluated for foreign ownership and/or control to avoid confusion in implementation. Component and sub-component information should be identified by the vendors and manufacturers.

- Ensure any new regulations aimed at supply chain requirements on utilities are consistent with other existing regulations, including NERC CIP-013 and the U.S. Department of Agriculture's Rural Utilities Service (RUS) "Buy American" requirements (7 CFR Part 1787) that RUS borrowers, including more than 500 electric cooperatives, follow.

- Provide public power utilities and electric cooperatives the same funding and incentives for enhanced cybersecurity practices as FERC-jurisdictional entities.

If any new regulations are developed, DOE could work with the Small Business Administration to develop a process for identifying and mitigating small business impacts of new regulations. Most of the Associations' members are small businesses and any new regulation imposed can create unique burdens that may be more challenging for them to adapt to than large organizations with more resources.

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?

The vendors and manufacturers should bear the primary responsibility to ensure security in their supply chain for equipment serving the bulk power system; they are uniquely positioned to have the most knowledge on their equipment, components, sub-components, and supply chains. DOE should directly engage with the vendors serving the bulk power system to understand cost-effective ways to source equipment from domestic sources, or foreign countries not deemed a risk by the federal government. DOE should ask vendors for input on how timelines for procurement would be impacted if certain products in the supply chain were no longer available. Direct engagement with the vendors will be the most efficient way to learn about any additional actions needed to improve security in the supply chain. DOE could become the liaison with vendors to help the electric utility sector leverage its collective interest in the supply chain available for bulk power system equipment. For example, DOE could assist vendors with the necessary disclosures for utilities purchasing their equipment, such as software bills of materials.

Adding hurdles or required steps in the procurement process for bulk power system requirement could result in an overall negative impact on electric reliability. Prohibited transactions could lead to longer lead times for procurement, equipment that contain components from a variety of sources, limited availability of supplies, delayed delivery, and increased costs related to available supplies and resources devoted to review. Any increased costs that the manufacturers face will likely to be passed on to the utilities purchasing the equipment. As consumer-owned utilities, these increased costs will ultimately be borne by the consumers of public power utilities and electric cooperatives.

To facilitate more awareness and information sharing of supply chain risks, DOE could consider several actions and measures:

- DOE could assign "risk scores" for equipment and components serving the bulk power system to provide utilities with consistent information when procuring equipment. Any such scores should be consistent and inform compliance with NERC CIP-013 supply chain standards. For more granularity and effective cyber security supply chain risk management, DOE-provided "risk scores" could be manufacturer- and vendor-specific.

- DOE could consider a supply chain security "assist" program that would allow utilities to voluntarily request a review or assistance from DOE where they believe such a review would be beneficial to their programs.

- DOE could share new contract language and guidance with utilities that is now under development for information technology and operational technology service providers in response to Executive Order 14028, *Improving the Nation's Cybersecurity* (issued May 12, 2021).

- The Associations encourage DOE to work closely with the E-ISAC in processing and sharing known threats. E-ISAC serves a valuable role in sharing actionable information on emerging threats. DOE could more specifically identify the E-ISAC as a partner in the information sharing processes that would be needed to communicate the implementation of any of DOE's actions.

If DOE seeks to develop a "black list" of vendors that utilities cannot or should not use, the Associations urge the department to do sufficient vetting ahead of time to ensure that there are alternative suppliers that can meet demand for this critical electric infrastructure in a timely and cost effective manner. Some equipment and components have limited suppliers today. Eliminating these suppliers could cause serious supply chain issues and delay projects, impacting cost and reliability. The Associations urge DOE to closely consult with the utility sector about potential impacts of a "black list" if this is a path the department pursues. A "white list" that does not preclude use of other vendors would provide more flexibility to utility sector and could help mitigate concerns about insufficient supply of bulk power supply equipment.

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?

The vendors and manufacturers should bear the primary responsibility to ensure security in their supply chain for equipment serving the bulk power system; they are uniquely positioned to have the most knowledge on their equipment, components, sub-components, and supply chains. Utilities are not in a position to enforce supply chain requirements on the vendors.

Any new requirements or guidance that DOE issues should provide clarity on the definition of assets, including at the sub-component level as needed, that would be considered to pose a foreign ownership, control, and influence risk depending on the country of origin. DOE should also provide information regarding threats, mitigations, and remediations through the E-ISAC. Further, DOE should also provide use cases/examples regarding the long-term implementation of such requirements, e.g., how utilities are expected to respond/comply where a current domestic supplier is purchased by a foreign entity or vice versa. DOE should recognize that assets cannot be inherently "secure" or "not secure." Power systems are made secure by proper implementation of assets, such as through network segmentation, network monitoring, intrusion detection and prevention, multi-factor authentication, least-privilege authorization, and other measures.

Finally, DOE should work with FERC and NERC to determine whether the existing supply chain standards are sufficient for addressing DOE's supply chain concerns with respect to national security. NERC-CIP-013 standards became effective on October 1, 2020. Sufficient time should be afforded for utilities to implement these standards and for NERC to assess their effectiveness. If DOE determines additional requirements are needed, DOE should work with NERC to update the existing standards before DOE considers imposing new requirements aimed at the same objectives.

Prohibition Authority

DOE should not consider expanding prohibition authority without a risk-informed basis and well-developed record to support such action. Where risks are identified, the risk mitigation and management activities proposed need to be evaluated on a risk-benefit-cost basis to ensure that the proposed actions will produce the right level of risk mitigation without diverting resources from more valuable security-related activities. Given the costs associated with facility upgrades and overall supply chain restrictions, due consideration should be given to the benefits to be obtained from any expansion. We urge DOE to weigh whether a required investment will deliver commensurate benefits or if resources could be better expended to enhance security through other means.

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 Associations strongly urge DOE to focus its efforts on addressing any significant risks in the bulk power system before considering a Prohibition Order or other action focused on the distribution system. DOE should prioritize efforts according to the greatest potential risk to impact the grid and national security. For example, the potential for impact to the interconnected bulk power system from transmission facilities is substantially greater and different than the potential for impact from distribution facilities. It is unclear at this time what risk DOE is seeking to address in the distribution system or how an expansion of prohibition authority would achieve benefits to national security. DOE should use a risk-informed approach when considering any additional prohibition authority and incorporate multiple types of risk in the assessment – not only potential foreign ownership, control, and influence but also insider and other risks.

Further, DOE should not issue a new Prohibition Order covering supply chain management until utilities and NERC have had time to review implementation of the NERC CIP-013 supply chain standard. DOE should allow adequate time for determining NERC CIP-013 standard's impact to security and reliability and for measuring the standard's effectiveness. We urge DOE to concentrate its efforts on providing support and assistance to utilities to make NERC CIP-013 implementation as effective as possible. As mentioned earlier, DOE serving as a bridge with suppliers would be a significant help going forward. Any consideration of new prohibition authority should account for whether an adequate supply chain would be available to utilities to avoid negatively impacting reliability.

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?

Before considering another Prohibition Order on DCEI, the Associations urge DOE to focus its efforts on addressing any significant risks in the bulk power system. NERC Critical Infrastructure Protection (CIP) standards already cover necessary critical infrastructure. DOE should avoid implementing duplicative requirements for industry that do not improve security but rather add to the burden on utilities for implementation. The department could provide guidance on the equipment or components that it believes utilities should focus on when honing their cyber and supply chain programs. In addition, DOE should encourage Department of Defense facilities classified as critical defense facilities to have regular discussions with their utilities on specific concerns.

Utilities already have prioritization processes in place for serving critical infrastructure in their service territories under state and local regulations and their own internal processes and policies. There is no need for DOE to add another layer of regulation given that utilities are already prioritizing serving critical

infrastructure. Any such activities would have to be coordinated with state and/or local jurisdictions that typically are responsible for load service and prioritization of shedding loads for providers.

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?

Again, the Associations urge DOE to focus its efforts on addressing any significant risks in the bulk power system rather than considering any new Prohibition Orders or other actions covering critical infrastructure enabling the national critical functions. NERC CIP standards cover necessary critical infrastructure. DOE should avoid implementing duplicative requirements for industry that do not improve security but rather add to the burden on utilities for implementation. If there are lessons learned from implementing NERC CIP-013 that could be applied beyond the bulk power system, DOE should consult with the utility sector to understand how best to incorporate this knowledge.

A Prohibition Order affecting national critical functions would effectively cover the entire electric grid. DOE should not consider such an expanded approach unless a risk-informed basis exists to support such an expansion. The national critical functions are broadly defined, often interdependent, and cover a substantial portion of the U.S. economy. DOE should focus on the critical interdependencies in these functions, the risks they face, and whether these risks need to be mitigated. The department could facilitate discussions with state and local authorities.

If DOE pursues such prohibition authority, any equipment that needs to be replaced to serve national critical functions should be funded by the federal government and should be prioritized according to risk.

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

The answer to this question depends in part on DOE's definition of critical infrastructure. If DOE's definition is consistent with that used by NERC, utilities subject to NERC standards keep track of this information. If DOE utilizes a different definition of critical infrastructure in any Prohibition Order or other actions, then further guidance from DOE may be needed. DOE could provide support for utilities that request assistance in identifying or confirming facilities in their service territories.

There are already processes to identify critical or priority loads within utility service territories, as well as to request specific protections and mechanisms to meet utility customers' needs. Moreover, critical load plans are often developed and approved at the state level and are based on what each utility's customer has disclosed. Any activities would have to be coordinated with state jurisdictions that typically have authority over load service and prioritization of the shedding of loads for providers within their state.

In general, utilities only know what their customers disclose to them and may not be aware of the criticality of every business, building, or customer within their service territory. For this reason, there is typically a process through which customers can discuss priority load status, power quality, reliability, and other needs directly with their utility. This approach allows customers with critical power needs to work directly with their utility to determine the most appropriate action to be taken to address their needs. It also allows such needs to be addressed in the most cost-effective way for each service territory to ensure that rates for customers remain just and reasonable.

The Associations would like to understand more from DOE about whether it would require utilities to report such information to DOE and if so, how the Department will maintain data confidentiality. If new information needs to be shared with DOE, it could create a new security risk.

Conclusion

In summary, the Associations urge DOE to directly engage with vendors that provide equipment to electric utilities to address any concerns the department may have about risks in the supply chain. The vendors are best suited to address such questions. Any new measures, directives, requirements, or prohibition authority that DOE chooses to pursue regarding electric infrastructure must be risk-informed, clear, prospective, and scalable, and take cost into account to avoid unintended consequences to grid security and reliability.

Thank you for your consideration. We would welcome the opportunity to discuss our recommendations further with your team. Please contact us at if you have any questions.

Sincerely,

American Public Power Association
Large Public Power Council
National Rural Electric Cooperative Association
Transmission Access Policy Study Group