June 7, 2021

Via Electronic Submission

Michael Coe
Director, Energy Resiliency Division of the Office of Electricity
U.S. Department of Energy
1000 Independence Ave, SW
Washington, D.C. 20585

Re: Notice of Request for Information on Ensuring the Continued Security of the United States Critical Electric Infrastructure

The American Council on Renewable Energy ("ACORE") respectfully submits these comments concerning the April 22, 2021 Notice of Request for Information ("RFI") from the U.S. Department of Energy ("DOE" or "Department") on Ensuring the Continued Security of the United States Critical Electric Infrastructure. ACORE is a national nonprofit organization dedicated to advancing the renewable energy sector through market development, policy changes and financial innovation.

Critical infrastructure security is a priority for the renewable energy developers, component manufacturers, utility operators and corporate energy buyers at ACORE. A secure grid is a more reliable grid and one that can sustainably transition toward a clean energy future. ACORE is particularly grateful for DOE's substantive attention to this issue through the RFI. Dialogue between government and industry is the best way to ensure the effective security results sought by the Department.

In response to question A3, *"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?"*

We encourage the Department to build upon successful regulatory regimes to date and apply its cybersecurity best practices to procurement security as well. Recent events around ransomware and the nation's natural gas pipeline infrastructure lay bare the importance of strong cybersecurity standards in particular. Fortunately, our nation's bulk electric system, unlike our natural gas system, is subject to mandatory cybersecurity standards authored by the North American Electric Reliability Corporation ("NERC") and approved by the Federal Energy Regulatory Commission ("FERC"). This NERC-FERC regulatory regime has worked well and avoided the kinds of security events that have afflicted the natural gas system.

Supply chain risks may have cybersecurity implications. While these concerns are not identical, their ties suggest that further building upon the effective NERC-FERC model, whereby expert regulators have already proven success, is a commonsense way to ensure the continued security of our nation's critical electric infrastructure while avoiding the duplication of efforts.

Cybersecurity control measures, such as the deployment of sophisticated equipment or third-party services, are expensive and novel. Accordingly, we encourage the Department to make sure the benefits to the system of actions recommended or required by DOE or others should justify the costs to the system. Additionally, we encourage steps to ensure that recommended actions are commensurate with the risk posed by specific threats to the electric system.

In response to question A4, *"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?"*

To avoid the market-dampening uncertainty generated by previous prohibition orders of unclear scope, we encourage the Department or other regulators to be specific in identifying — and proactive in sharing — the exact products and services at risk of prohibition. Impacted countries, manufacturers and components should all be enumerated both to ensure maximum compliance and to limit the costs of that compliance.

Thank you for the opportunity to submit these comments. Please do not hesitate to contact ACORE's Director of Regulatory Affairs, Tyler Stoff, at stoff@acore.org or (202) 507-4634 with any additional questions you may have.

Sincerely,

/s/ *Tyler Stoff*
Tyler Stoff
Director of Regulatory Affairs
American Council on Renewable Energy