NYU TANDON SCHOOL OF ENGINEERING

Tandon School of Engineering
6 Metrotech Center
Brooklyn, NY 11201

P: 646-997-3596
rkarri@nyu.edu

June 7, 2021

Dear Ms. Hoffman and Mr. Coe,

We appreciate the opportunity to comment on the DOE Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure (2021-08482) published on April 22, 2021.

As the United States Government considers whether to recommend a replacement to Executive Order 13920, *Securing the United States Bulk-Power System*, we refer you to an article on the subject that was published in IEEE Spectrum last year. The article, "Executive Order Shines a Light on Cyberattack Threat to the Power Grid: It aims to protect the U.S. bulk-power system, but local electricity networks are just as vulnerable" by Yury Dvorkin, Assistant Professor at New York University, identifies several vulnerabilities that warrant attention.

While EO-13920 limits attention to transmission network hardware equipment, we are gratified that the Department of Energy recognizes the importance of similarly protecting certain distribution networks. With this in mind, these comments specifically address the high vulnerability areas that could benefit from a revised Long-Term Strategy:

(i) **Secure distribution networks**
Regarding the expanded attention to distribution facilities that serve CDFs (Critical Defense Facilities), while prioritizing these facilities is sensible, other loads should not be neglected. Securing distribution networks is critical not only because the effects of attacks could propagate to the bulk-power system, but also because of the possibility that local failures, particularly in large urban areas, can have significant and cascading impacts on many electricity consumers and systems. These impacts are more than just an inconvenience affecting a good deal of critical transportation, communications and healthcare systems. With a growing frequency of high-impact disasters, these effects may also concern electricity vulnerable population groups (e.g., people with pre-existing conditions that require uninterrupted electricity supply or may experience severe health complications in case of longer shutdowns >4 hours). Networks with high impact electricity vulnerability will require similar reliability and backup resources as the CDFs.

(ii) **Unify cybersecurity protocols across the country**
A unified set of cybersecurity protocols to streamline cyber-physical interfaces between consumers, regulators, third-party companies and utilities is lacking. Consider, for example, a company operating a charging station for electric vehicles that serves as an intermediary between the car manufacturers, car owners/users and utilities, each of whom use different protocols, have different access to industry-grade cyber defense means and exhibit different cybersecurity hygiene practices because of their inherently

different cyber risk profiles and exposure. There are similar examples for in demand response aggregators, community photovoltaic and storage assets, and even heavy-industry processes. The Department of Energy can facilitate consensus between these stakeholders across the different states and territories in order to unify cybersecurity protocols across the country and ensure consistency in practices. The Department could also assist stakeholders by sharing best practices for companies participating in the supply chain. For example, software developers (a prime target for cyberattacks) need to assure the integrity of software systems throughout development and deployment. Also, the Department can inform best practices when dealing with particular threats such as ransomware attacks.

(iii) **Focus on firmware and software**
Fortifying the US supply chain and domestic production will be an effective mitigation to manage energy infrastructure risks. However, because the electrical supply chain is fractured with multinational companies supplying a diversity of components and systems to the international power community, it will be challenging to eliminate all hardware vulnerabilities while maintaining reliability and economies of scale. A significant limitation of the EO-13920 is its attention to hardware without a corresponding focus on firmware and software. Software solutions such as advanced, real-time monitoring of the grid to detect cybersecurity breaches can help mitigate some of these vulnerabilities. However, one can compromise bulk- and local- power systems software. There are ways not only to do real-time monitoring to secure the grid but also to detect cybersecurity breaches. While companies test software against known vulnerabilities, a valuable modification to EO-13920 is to develop protocols for cradle-to-grave software analysis and improvements in order to discover new vulnerabilities, patch them and for the Department to provide recommendations about how to mitigate cybersecurity vulnerabilities (which are a well-known point-of-entry for attackers). Such an undertaking led by the Department of Energy will be important for stakeholders that may otherwise have limited capabilities to evaluate and mitigate potential risks.

(iv) **Cyber Education**
Regarding other actions that the Department can take to facilitate responsible procurement practices by the private sector, as an academic institution, it should be no surprise that we raise the topic of broad cyber education. We often see that best practices of risk-averse corporations emphasize workforce development and education in cybersecurity as a critical component to protect their business and infrastructure. A lack of understanding of how businesses can be compromised (for example, because of poor cyber hygiene) can have a significant effect on U.S. infrastructure.

Thank you for the opportunity to comment on this important topic. Please let us know if you have any questions or if we can be of any help moving forward.

Sincerely,

Yury Dvorkin, *Assistant Professor, Electrical and Computer Engineering, NYU Tandon School of Engineering*
Ramesh Karri, *Co-Chair NYU Center for Cybersecurity, Professor of Electrical and Computer Engineering, NYU Tandon School of Engineering*
Farshad Khorrami, *Professor of Electrical and Computer Engineering, NYU Tandon School of Engineering*