Mr. Michael Coe
Director
Energy Resilience Division
Office of Electricity
U.S. Department of Energy
Mailstop OE-20, Room 8H-033
1000 Independence Avenue, SW
Washington, DC 20585

June 7, 2021

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

Dear Director Coe:

Schneider Electric strongly supports the national security objectives behind the recent Request for Information (RFI) on Ensuring the Continued Security of the U.S. Critical Electric Infrastructure. As a critical manufacturer, we look forward to partnering with the Department on this important work.

At Schneider Electric, we drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

Our integrated solutions enable homes, commercial buildings, data centers, and critical infrastructure to operate more efficiently and securely. Our products and systems are used in over one million buildings and 40,000 water & wastewater treatment installations throughout the world. The cybersecurity of these products and systems is therefore of vital importance to us and our customers.

Our responses to the RFI questions are listed below.

Part A. 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?***

In our experience working with states, Indian Tribes, and local governments, there are three broad areas where the Department could offer additional assistance to these entities.

The first is enabling the **rapid sharing of quality cyber threat information with these entities**. This could be through expansion of the Department of Energy's Cybersecurity Risk Information Sharing Program (CRISP) or the Cybersecurity & Infrastructure Security Agency's (CISA) Automated Indicator Sharing (AIS) program. From our perspective, the government should focus more on delivering positive security outcomes to the relevant entities and less on which agency or program is the appropriate "sector-specific agency". The focus should be on delivering high quality, near real time indicators that these entities can use in their own network defense activities. Additionally, beyond just the relevant entities referenced in the question, a key goal of the government should be to **swiftly declassify threat information** on malicious actors' activities so that network defenders can act on such information as quickly as possible. Such rapid declassification would help states, Indian Tribes, local governments, utilities, and manufacturers respond to cyber threats more quickly.

Second, these entities would benefit from **no cost cyber and physical security assessments** that do not come with the burden of regulatory consequences. An example of the type of service that could be provided includes CISA's National Cybersecurity Assessments and Technical Services (NCATS) program or a similar program administered by either the Department of Energy or a relevant National Laboratory. Such assessments should include technical resources to assist relevant entities remediate findings from these assessments.

Finally, to supplement government conducted assessments, the Department could also provide these entities with a **pre-approved list of private cyber/physical security services/assessment providers** that can perform detailed assessments and assist with relevant remediation activities. For example, the Department could customize the General Services Administration (GSA) Highly Adaptive Cybersecurity Services (HACS) initiative for the relevant entities to ensure their ability to augment assessment services provided by the government.

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 Department could advise utilities to grant preferential treatment in bids to equipment manufacturers that can demonstrate conformance with relevant international cybersecurity standards (e.g. ISA/IEC 62443 and ISO 27000). For example, Schneider Electric has a robust product development and security program that adheres to the ISA/IEC 62443 suite of standards for industrial control systems cybersecurity. To reinforce trust with our customers, many of our processes, products, solutions, and sites are tested and certified by independent third parties for conformance to the ISA/IEC 62443 suite. Some of the foundational practices required to achieve such certifications include secure product development, vulnerability management, source code integrity and protection, supplier cybersecurity verification, and incident detection, management, and response practices. Examples of our independent certifications include:

- ISA/IEC 62443-4-1 certification for the site that produces Power Meters and some PME/PSO software.
- ISA/IEC 62443-4-1/-4-2 product certification for the Power Monitoring Expert product
- ISA/IEC 62443-4-1/-4-2 product certification for EcoStruxure Power SCADA Operation
- ISA/IEC 62443-4-1 process certification for secure development lifecycle process

Additionally, Schneider Electric would like to see the DOE Cyber Testing for Resilient Industrial Control Systems (CyTRICS) scaled to include more equipment used in our grid today. Schneider Electric was the first equipment manufacturer to participate in this program (https://www.energy.gov/ceser/articles/doe-ceser-partners-schneider-electric-strengthen-energy-sector-cybersecurity-and) and we believe that the program can play a critical role in protecting our electric grid from threats of compromise. Expanding this program could help the government, utilities, and manufacturers provide more transparency to hardware and software bills of material and help accomplish one of the main goals of the recent Executive Order on Improving the Nation's Cybersecurity. Such expansion could be accomplished through an independent third-party broker to collect and evaluate bills of material while protecting the underlying intellectual property of the relevant vendor.

Regarding the incorporation of criteria for evaluating foreign ownership, control, and influence into supply chain risk management, the Department should use caution when exploring such criteria. As utilities and manufacturers rely on a complex, global supply chain, we will look to the government to establish rules that mitigate foreign influence from specific actors and to avoid rules that could harm the allies upon which we rely. Where possible, such rules should avoid duplication with existing authorities and processes such as the Department of Commerce's efforts to mitigate threats to the information, communications, technology (ICT) supply chain and the Committee on Foreign Investment in the United States (CFIUS).

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?***

Where possible, the Department should encourage procurement practices that reward vendors with preferred status that have demonstrated conformance with existing international cybersecurity standards and/or subjected their products and systems to the independent validation and rigor required to participate in the DOE CyTRICS program. It is through this transparency and rigor that we will ensure the safety and security of our electric grid.

The growing trend of critical infrastructure owners and operators establishing their own "country of origin" bans for the manufacturing and sourcing of relevant products poses several challenges to critical manufacturers. Often times, these bans are not explained and are inconsistent with existing U.S. government guidance. These independent actions by owners and operators complicate global supply chain operations by increasing uncertainty and reducing predictability. We recommend that the Department regularly communicate with relevant sector coordinating councils so that owners and operators have a forum to discuss and align procurement practices. This dialogue could also provide the Department with an opportunity to provide specific guidance to owners and operators on how they should address cybersecurity issues within their respective procurement processes in a consistent manner that aligns to relevant U.S. government cyber threat information. This type of dialogue will ensure that country of origin bans, such as the previous Administration's Prohibition Order Securing Critical Defense Facilities, remain the domain of the U.S. government and are always based upon objective facts and demonstrated evidence of threats.

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?***

Please see our response Part A Question 2.

Part B. Prohibition Authority:

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?***

In our assessment, what is more important than issuing a new Prohibition Order is that the Department lay out an **objective and transparent process to continuously assess threats to the bulk-power system**, and establish a process for issuing relevant mitigations, which could include prohibition orders or binding operational directives (similar to those issued by the Cybersecurity and Infrastructure Security Agency (CISA) under their *Federal Information Security Modernization Act of 2014* authorities). We recommend that the Department pursue a similar process to the one outlined in the *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act* that led to the creation of the Federal Acquisition Security Council (FASC), which coordinates government-wide exclusion and removal orders to mitigate risks to the Federal government posed by certain products or vendors. It is through this robust and objective process that both U.S. national security and economic interests will be met as it relates to the electric grid.

Furthermore, it is our view that the distribution grid could benefit from more oversight to incentivize the deployment of cybersecurity best practices. The problem at hand is of a strategic nature and not one that will be solved through the issuance of prohibition orders alone. The cybersecurity of the generation and transmission portions of the electric grid are overseen today by FERC and NERC, but we assess that there is a gap in the oversight of the distribution portions of the electric grid.

The Department could play a constructive role in incentivizing the deployment of cybersecurity best practices within the distribution grid. Currently, there is a lack of incentive for distribution utilities to modernize much of their aging infrastructure technology. This older technology, which has a typical lifespan of 20+ years, was originally designed and manufactured prior to the existence of robust cybersecurity controls.

A more cybersecure approach would be to drive and enable collaboration between the customer, supplier, and relevant integrator to continuously improve cybersecurity protections. In this scenario the utility customer would be incentivized to modernize and maintain their technology, to include following relevant supplier product release cycles and to regularly update associated software and firmware. However, given the uncertain process around potential rate increases, it is difficult for distribution utilities to prioritize necessary technology modernization and upgrades, even if those upgrades would come with stronger cybersecurity protections.

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?***

In addition to our response to the previous question, we would encourage prospective action to be taken in coordination with the FASC, Department of Homeland Security, and Department of Commerce to avoid duplication**.**

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?***

In addition to our response to Part B Question 1, we would encourage prospective action to be taken in coordination with the FASC, Department of Homeland Security, and Department of Commerce to avoid duplication.

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

No response as this question should be answered by utilities.

Schneider Electric sincerely appreciates the opportunity to comment on the RFI. If you have any questions or need additional information, please contact me at Patrick.Ford@se.com.

Sincerely,

Patrick M Ford

Patrick M. Ford
Regional Chief Information Security Officer, Americas Region
Schneider Electric