June 7, 2021

VIA ELECTRONIC SUBMISSION AT: ElectricSystemEO@hq.doe.gov

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

RE: Ensuring the Continued Security of the United States Critical Electric Infrastructure

Dear Director Coe:

ABB Inc., on behalf of ABB, Ltd. ("ABB") submits this response to the Request for Information on Ensuring the Continued Security of the United States Critical Electric Infrastructure issued by the U.S. Department of Energy and published in the Federal Register on April 20, 2020.

ABB, a New York Stock Exchange listed corporation headquartered in Zurich, Switzerland, is one of the United States' and world's largest providers of distribution grid equipment and electrical and control system technologies used across the energy, utility, industrial, transportation, and critical infrastructure sectors. We produce many of these products at our 50 U.S. manufacturing or major facilities across 30 states. Central to our product development, manufacturing, and service offerings are safety, reliability, and security, including the reduction and mitigation of cybersecurity risks and vulnerabilities.

We have developed and adopted a number of practices and procedures to mitigate security threats to our products and our customers, including owners and operators of energy, utility, and critical infrastructure assets. That said, the industry still faces a number of challenges in staying ahead of security threats and the Department of Energy could play an important role in helping to secure critical electrical infrastructure.

We appreciate the opportunity to respond to this Request for Information and share some of ABB's and the industry's best practices and make some suggestions as to how the Department of Energy could help industry improve security of critical electrical infrastructure.

Background

Cyber and supply chain security are key requirements in everything we do and is embedded throughout ABB's product lifecycle, including design, testing, procurement and risk management protocols, and robust and responsible manufacturing.

ABB's "Defence in Depth" strategy covers a broad spectrum of threats which include personnel training, change management procedures, system configuration guidelines, and physical security. ABB employs threat modeling, security design reviews, and security training of software developers. We conduct in-house and external security testing to provide reliable and secure solutions for our customers. And ABB has a well-developed and transparent vulnerability handling process for addressing reported vulnerabilities and disseminating patches and fixes.

The key reference architecture for a number of our products is based on IEC 62443 which provides a layered infrastructure that allows for segmentation of critical zones and controlled access

between zones of differing levels of trust. Our own cybersecurity product requirements, which we also pass on to our sub-suppliers, include the following best practices, among others: disallowing backdoors, use of proper cryptography, system hardening, protection against malware propagation, vulnerability handling, and security patch testing.

ABB believes that there is much that regulators can do to encourage the adoption of responsible risk mitigation techniques and related industry standards.

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

States, Indian Tribes, and units of local government could benefit from technical assistance in evaluating and conducing cyber risk assessments and then designing appropriate risk mitigation plans. Cybersecurity does not inherently provide a clear financial or operational return on investment, often making it challenging to convince governing bodies of the value of such capital investments and ongoing operational expenses. Rather, cybersecurity delivers intangibles such as avoiding the potential for a safety or environmental incident, prevention of unplanned outages, the theft of intellectual property, the avoidance of regulatory violations, and the economic damage that each of these may cause. As such, private, public, and government entities often prioritize other capital or service investments at the expense of cybersecurity.

Providing state, Indian tribes, and local governments with the tools to value cybersecurity investments could help them justify the investments and expenditures needed. There are a number of cybersecurity return on investment models that the Department could draw on in providing assistance and criteria for baseline analyses to state and local governments. For example, providing a standardized risk calculation and catalog of criteria to measure in risk assessment models could help governments assess their risk in a consistent way. As an example, a typical risk model provided by the SANS Institute for Annualized Loss Expectancy (ALE) would be as follows:

Annualized Loss Expectancy (ALE) = SLE x ARO
Single Loss Expectancy (SLE) = Asset Value x Percentage of Loss (EF)
Annualized Rate Occurrence (ARO) = Likelihood x Frequency.

While SLE is based upon qualitative metrics, ARO is the product of subjective variables, likelihood and frequency, in which different asset owners may attribute different values. Therefore, one State may attribute higher risk to a system than another State for a similar system, thus creating an uneven analysis of risk which could result in an uneven distribution of funding. If the asset owners were provided with standard criteria to evaluate subjective variables in their risk calculation, they could feel confident they are on an even playing field with one another.

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 December Prohibition Order introduced confusion into the marketplace because it lacked clear, actionable guidance and criteria as to what qualifies as foreign ownership, control, or influence ("FOCI"). Without well-defined, objective, and actionable criteria that could be consistently applied, industry took disjointed approaches to compliance with the December Prohibition Order which created confusion and challenges. One of the most impactful actions the

Department could take to mitigate risk of foreign ownership, control and influence in the critical infrastructure supply chain is to provide industry with (a) a list of entities that it has assessed are subject to FOCI and therefore prohibited; or, if that is not possible (b) a clear set of guidelines and criteria that industry can use to determine if an entity is subject to FOCI.

ABB[1] is committed to ensuring that our company and supply chain remains free from risks associated with foreign adversaries and takes significant steps to mitigate risks in our supply chain. ABB, and industry, could incorporate new criteria provided by regulators if that criteria are clear, objective, and actionable. ABB utilizes a comprehensive global trade compliance system to screen procurement and sales transactions against a constantly updated Sanctioned Party List. The Sanctioned Party List is based on official sanction lists produced by government institutions, law enforcement agencies, national banks, and other entities. Domestic examples of those lists include those published by the U.S Department of Treasury's Office of Foreign Assets Control[2] and the U.S Department of Commerce's Entity List[3]. Like these other Federal agencies, the Department could provide a list of known entities under FOCI that industry could incorporate into our supplier screening and qualification process.

If the Department is unable to provide a list of entities that are subject to FOCI and should be avoided, they should provide a well-defined list of criteria that industry can use to make its own determination or certification that they are free from FOCI in their supply chains. For example, as part of our supplier qualification process, we require suppliers to disclose their ownership structure, percentage ownership stake of each owner, and additional companies controlled by the shareholders. The Department could provide additional criteria that industry can add to its supplier qualification and screening process. However, those criteria should be for things that the private sector is equipped to investigate. The Defense Counterintelligence and Security Agency's definition of FOCI referenced by the RFI from April 2020, includes a number of criteria that private industry is not capable of answering, like "record of economic government espionage against U.S. targets." Industry does not have access to such information and therefore cannot use that criteria in making its own FOCI determination. Companies, like ABB, rely on government intelligence and threat assessment information as companies are not equipped to conduct geo-political intelligence gathering and identification.

If the Department cannot provide an actionable list of known entities under FOCI, then they should provide industry with objective and actionable criteria, that doesn't rely on geo-political intelligence gathering, for incorporation into existing supplier screening and qualifications processes.

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?

---

[1] As noted in ABB's previous comments filed on August 20, 2020, ABB is a multinational enterprise headquartered in Switzerland, but whose shares are listed on the New York Stock Exchange, the Swiss SIX Exchange in Zurich and the NASDAQ OMX in Stockholm. Our shares are widely held (only three shareholders hold more than 3% of our shares, and the largest shareholder, a Swedish fund, holds only 12.5% of our shares). As a result, our company is most affirmatively not under FOCI with respect to foreign adversaries.

[2] https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information#:~:text=OFAC%20Sanctions%20Lists,that%20are%20not%20country%2Dspecific

[3] https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list

ABB has a robust supplier qualification process, but we understand that some in the private sector may not. The Department can:

(1) Develop and share best practices. Use the Department's convening, technical, and educational expertise to bring industry together to share best practices for supply chain risk mitigation and then disseminate those best practices across industry; and

(2) Technical assistance. Provide technical assistance to critical electric infrastructure, manufacturers, owner, and operators, as they design and implement supply chain risk mitigation programs as well as installation, operational, and cyber hygiene maintenance programs for that equipment.

Are there particular criteria the Department could use to inform utility procurement policies, state requirements, or FERC mandatory reliability standards to mitigate foreign ownership, control, and influence risks?

As noted above, the most effective and efficient way for the Department to inform procurement policies to mitigate FOCI is to provide the private sector with a list of entities it believes are under FOCI and therefore should be avoided. Such guidance would provide a clear and unambiguous way to mitigate FOCI risk from foreign adversaries. A number of US Government agencies provide similar information to private industry (see above), and the Department could follow suit for the critical electric infrastructure sector.

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?

Without understanding the particular risks that a blanket prohibition order on the distribution system is meant to mitigate, it is hard to opine on whether the Department should pursue such actions. As a general matter, removing 100% of risk is an impossibility and prohibitively expensive. As such, risk mitigation protocols tend to be designed to be commensurate with the risk they are trying to neutralize or avoid. A blanket prohibition for the electric distribution system is particularly challenging considering the innumerable amount of electrical equipment of widely varying types that are installed on the electric distribution system. Further, much of the equipment used on the distribution system is also used by industrial and commercial entities in their "behind the meter" operations; thereby unintentionally extending any such prohibition order to vast sectors of the economy unrelated to the electrical grid system.

The December 2020 Prohibition Order restricted transactions for a discrete list of specific electrical equipment that are susceptible to known risks, on an identifiable portion of the electric grid (over 69kV that supports DCEI). It is not clear what risk the Department would be trying to mitigate by extending such a prohibition to the entire electric distribution system nor is it clear that it would ensure the national security.

If the Department wants to seek to issue a Prohibition Order or other action that applies to equipment installed on parts of the electric distribution system, we encourage the Department to be more specific about (a) what type of equipment it wants to restrict, (b) where on the distribution grid it wants to restrict it, and (c) what particular risks such restrictions are meant to mitigate. In most cases, specific tactical actions can more effectively mitigate a risk than a blanket or general action.

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?

Given their numerous and distributed nature, extending a Prohibition Order to electrical infrastructure that serves non-DCEI sectors like communications, healthcare, IT and transportation is practically equivalent to extending a Prohibition Order to the entire bulk and distribution electrical systems. We caution against such an action at this time for reasons stated above.

We recommend the Department first implement a successful regime around the targeted equipment and portions of the grid detailed in the December 2020 Order.

That said, the biggest challenge still remains understanding the Department's definition of FOCI. Without clear guidance or a list of entities that it believes are FOCI, industry is filling the void with inconsistent and scattershot definitions and approaches.

In addition to critical infrastructure, should the Secretary seek to issue a Prohibition Order or other action that covered electric infrastructure enabling the national critical functions?

We caution against extending the Prohibition Order to electrical infrastructure enabling the national critical functions at this time. For reasons stated, that would bring the entire electrical system within scope which we think is inadvisable at the moment. Additionally, given the breadth and volume of electrical equipment in use on the electric grid, implementing such an action in an "overnight" fashion could halt grid investments across the country as utilities, technology providers, suppliers, and more would have to understand what equipment is covered by the Order and potentially re-make their supply chains. Before pursuing such an Order, we recommend the Department first implement a successful regime around the targeted equipment and portions of the grid detailed in the December 2020 Order.

As that is underway, we suggest that the Department engage in a substantive stakeholder process where it investigates distribution grid vulnerabilities in order to understand the greatest risks and design an Order aimed at mitigating them in a targeted way.

Thank you for the opportunity to submit comments to the Request for Information; we would be glad to discuss these questions further.

Regards,

Asaf Nagler Digitally signed by Asaf Nagler Date: 2021.06.07 16:09:44 -04'00'

Asaf Nagler, Esq.
Senior Director, Government Relations
ABB Inc.