Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

June 7, 2021

U.S. Department of Energy
Attn: Ensuring the Continued Security of the U.S. Critical Electric Infrastructure EO RFI

Re: Exelon Corporation's Response to Electricity Subsector Industrial Control Systems Cybersecurity Initiative

Exelon Corporation ("Exelon" or "the Company") submits these comments in response to the Request for Information ("RFI"), *Ensuring the Continued Security of the U.S. Critical Electric Infrastructure*, issued by the Department of Energy ("the Department" or "DOE") on April 20, 2021.[1] Exelon appreciates the opportunity to respond to this RFI. Our submission includes answers to the questions in sections 2(A) and 2(B) of the RFI to provide DOE with the perspective of a utility owner and operator to assist the Department as it considers whether to recommend a replacement Executive Order that appropriately balances national security, economic, and administrability considerations.

I. Background

To further secure the Nation's electric grid, the Department is developing recommendations to strengthen requirements and capabilities for supply chain risk management practices by the Nation's electric utilities. These recommendations are intended to enable an approach that builds on, clarifies, and, where appropriate, modifies prior executive and agency actions.

Executive Order ("E.O.") 13920, *Securing the United States Bulk-Power System*, issued on May 1, 2020,[2] authorized the Secretary of Energy (the "Secretary") to work with Federal partners and the energy industry to take actions to further secure the Nation's bulk-power system ("BPS") from threats to the electric industry's supply chain for a sub-set of BPS equipment. Informed by industry responses to a July 8, 2020, request for information on implementation of E.O. 13920,[3] the Secretary issued a Prohibition Order on December 17, 2020, invoking the authority of E.O. 13920 (the "December 2020 Prohibition Order").[4] Pursuant to the December 2020 Prohibition Order, a

[1] Notice of Request for Information (RFI) on Ensuring the Continued Security of the U.S. Critical Electric Infrastructure, 86 FR 21309, 2021-08482
[2] Executive Order 13920, Securing the United States Bulk-Power System, 85 FR 26595 (May 4, 2020).
[3] Securing the United States Bulk-Power System: Request for Information, 85 FR 41023 (July 8, 2020).
[4] Prohibition Order Securing Critical Defense Facilities, 86 FR 533 (Jan. 6, 2021).

Exelon

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

subset of utilities[5] were prohibited from acquiring, importing, transferring, or installing certain BPS electric equipment on facilities serving Defense Critical Electric Infrastructure ("DCEI").[6] That order targeted select equipment manufactured or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the People's Republic of China ("PRC").[7]

On January 20, 2021, Executive Order 13990, *Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis*, was issued, which suspended E.O. 13920 for 90 days.[8] As the December 2020 Prohibition Order was predicated on the authorities delegated to DOE by E.O. 13920, the Prohibition Order was also suspended during this same time period. The E.O. 13920 suspension has expired and effective April 20, 2021, the Secretary revoked the December 2020 Prohibition Order. On April 20, 2021, a new Request for Information (RFI) was issued to solicit responses on the development of a strengthened approach to address the supply chain security of the U.S. electricity subsector.

To ensure that the Department's considerations for a replacement Executive Order appropriately balance national security, economic, and administrability considerations, the Department is seeking information from electric utilities and other stakeholders to develop "recommendations to strengthen requirements and capabilities for supply chain risk management practices by the Nation's electric utilities."[9]

II. Introduction

Exelon Corporation has the largest number of electricity and natural gas customers in the U.S. Exelon does business in 48 states, the District of Columbia and Canada and had 2020 revenue exceeding $33 billion. Exelon serves approximately 10 million customers in Delaware, the District of Columbia, Illinois, Maryland, New Jersey and Pennsylvania through its Atlantic City Electric, Baltimore Gas and Electric Company, Commonwealth Edison Company, Delmarva Power & Light Company, PECO Energy Company and Potomac Electric Power Company. Exelon operates 11,150 transmission line miles for its utilities. Exelon is one of the largest competitive U.S. power generators, with more than 31,000 megawatts of nuclear, gas, wind, solar and hydroelectric

[5] The December 2020 Prohibition Order defined "Responsible Utility" as "an electric utility that owns or operates Defense Critical Electric Infrastructure (DCEI), as defined by section 215A(a)(4) of the Federal Power Act (FPA), that actively serves a CDF, as designated by the Secretary under section 215A(c) of the FPA." Id. at 534.
[6] *Id.*
[7] *Id.*
[8] Executive Order 13990, Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis, 86 FR 7037, 7042 (Jan. 25, 2021).
[9] Notice of Request for Information (RFI) on Ensuring the Continued Security of the U.S. Critical Electric Infrastructure

Exelon

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

generating capacity comprising one of the nation's cleanest and lowest-cost power generation fleets. The Company's Constellation business unit provides energy products and services to approximately 2 million residential, public sector and business customers, including three fourths of Fortune 100 corporations.

Exelon is a member of both the Edison Electric Institute ("EEI") and the Nuclear Energy Institute ("NEI") and supports the general comments of both associations. Exelon encourages DOE to consider their comments as it solicits feedback through the RFI issued on April 20, 2021. In addition, Exelon offers these comments in response to the RFI to provide details on Exelon's security posture and make specific recommendations for DOE's consideration as it develops a framework for supply chain security for the electric industry.

III. Comments

Exelon fully supports the national security objectives in the RFI on Ensuring the Continued Security of the United States Critical Electric Infrastructure and appreciates the urgency of these efforts. Exelon looks forward to working with DOE, other government entities, and our industry colleagues and equipment vendors in efficiently and effectively implementing any forthcoming requirements to enhance BPS supply chain security and grid resilience. Our submission provides Exelon's input to assist DOE in developing recommendations for further executive action as well as necessary guidance for implementing any changes.

We believe that a critical element of an executive order to replace E.O. 13920 is the development of a centralized, risk-based framework for enhancing supply chain security, informed by feedback from both the electric industry and its vendors. This approach should include a phased implementation plan that applies supply chain security controls to a prioritized set of high-risk devices in critical facilities based on risk intelligence from existing DOE programs like the Cyber Testing and Resilient Industrial Control Systems ("CyTRICS"), and the Cybersecurity Risk Information Sharing Program ("CRISP"). Successful implementation on the most sensitive or critical BPS facilities is the most effective and efficient approach to making meaningful progress in strengthening supply chain cybersecurity for the electrical system and will facilitate subsequent expansions of security controls to less critical components.

Any executive or regulatory action should allow for the lead time necessary to plan and implement security controls and be aligned with the timeline to complete the efforts utilities and

Exelon

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

vendors must undertake. The Department should also provide sufficient guidance on how to achieve the objectives of any new requirements. A key strategy for achieving the objectives of any new requirements in a subsequent executive order would be to provide a list of prohibited vendors and equipment, as this would reduce the need for utilities to establish their own processes – requiring additional time and cost and introducing inconsistencies – to identify whether particular vendors meet a more qualitative set of foreign control concerns.

Any new requirement should also avoid broad "rip and replace" orders targeting equipment with components from suspect countries and suppliers unless there is an intelligence-driven security risk that cannot be mitigated. A broad order requiring prompt replacement of components could lead to service outages and may not be possible to implement because of the limited availability of certain devices, components, or subcomponent parts from U.S.-based suppliers. If the use of certain devices becomes prohibited due to foreign ownership, control or influence framework, utilities may be challenged to promptly discover existing market alternatives – creating a risk to the reliable delivery of power if operational equipment is removed from service. Depending on what component or subcomponent is identified, there may also be significant impacts to other industries as well, similar to what has been reported in current events where microprocessor supply chain disruptions have caused significant backlog for the U.S. automobile industry. A more efficient and effective approach would be for the Department to communicate the specific risks to specific devices, with a narrowly tailored rule that enables utilities to mitigate accordingly.

Public-private information sharing can be used to identify potentially hazardous devices on existing networks. Once identified, electric utilities can then work with DOE and other government agencies to remediate those concerns. Starting with a "prohibited list" of vendors or devices that is informed by specific intelligence DOE has received would be an effective way to begin prohibiting certain equipment. As originally raised in the Company's response to the August 24, 2020, RFI[10], Exelon believes a "prohibited list" rather than a "prequalified list" is a more effective and efficient way to implement supply chain controls.

[10] Exelon Response to Request for Information on Executive Order 13920, Securing the United States Bulk-Power System, 85 FR 26595 (May 4, 2020). Submitted August 24, 2020.

Exelon

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

QUESTION RESPONSES

Section I: 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?**

As the topic of supply chain security has increasingly moved to the forefront of security conversations, more State, Local, Tribal, and Territorial ("SLTT") governments are becoming involved and expressing a desire to help. In general, state departments of energy and state utility commissions could benefit from being informed of the resources currently available to industry including, but not limited to: (a) the development of materials that provide education and training on how to interact with utilities on supply chain topics; (b) DOE can develop, compile and share common information sharing templates and agreements to disclose sensitive information between government and industry; and (c) guidance on how to implement localized supply chain security controls that are not inherently contradictory. However, the interest and concerns from multiple levels of government creates a risk of overlapping requirements that could be unnecessarily duplicative, or conflicting. While many of these costs will be incurred at the Bulk Electric System ("BES") level, DOE could play a useful long-lead role in educating PUCs on the prudence of distribution-level investments in purchasing more secure system hardware. Exelon believes the Department is in a unique position to coordinate these activities.

The Department should identify resources currently available and share them with SLTT governments to ensure that all interested agencies are current on best practices in this area. The template Security Risk Assessment[11] developed through the North American Transmission Forum ("NATF") is one of several excellent resources that the industry has developed to collectively address some of the issues this RFI seeks to understand. It would be beneficial not only to local governments, but industry and vendors as well if this and other helpful templates and information were stored in a central location on the DOE website.

It would also be helpful for local governments to have some primer materials for how to interact with utilities on the topic of supply chain security. With respect to cybersecurity, the National Association for Regulated Utility Commissions ("NARUC") has developed a Cybersecurity Primer for State Utility Commissioners[12] that is designed to equip utility

[11] "Energy Sector Supply Chain Risk Questionnaire", https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

[12] Keough, Miles; Thomas, Sharon. "NARUC Cybersecurity: A Primer for State Utility Regulators", Version 3, January 2017. https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F

Exelon.

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

commissioners with background information and questions designed to elicit information on whether regulated utilities have a mature cybersecurity posture. A similar document with a focus on supply chain security that defines important key terms and identifies risks and impacts could be very beneficial. The Department certainly has the expertise necessary to develop appropriate guidance documents in conjunction with industry experts involved in cybersecurity and procurements.

Proactive information sharing agreements and arrangements with other governmental agencies could expedite the response to any potential issue or vulnerability that may arise. Information sharing has been a long-standing effort across the electric industry, and with Federal agencies. For example, Exelon has a Security Intelligence and Threat Analysis ("Intel") team that centralizes the Company's threat and vulnerability identification and assessment. The team sits within Exelon's Corporate & Information Security Services ("CISS") group and provides regular updates to company leadership and the Board of Directors. Exelon's Intel team coordinates regularly with several federal government organizations including the Electricity Information Sharing and Analysis Center ("E-ISAC"), DOE, Department of Homeland Security, and the Federal Bureau of Investigation. Exelon's Intel team also coordinates at the state level in states where Exelon has operations and that includes state level ISACs, Emergency Management teams, and local law enforcement.

Any DOE recommendations should build on and expand these existing information sharing practices. The federal government's National Industrial Security Program ("NISP") ensures that the U.S. defense industry personnel safeguard the classified information in their possession, and work performed in response on contracts, programs, bids, or research and development efforts can be used as a model for these efforts. Information sharing must be conducted in a manner that safeguards the information being shared while preserving business confidentiality, and allowing for the detection, investigation, prevention, and response to cyber threats to the public. A partnership among DOE, industry and other units of government that leverages this model would bolster information sharing related to supply chain and grid security. Improving security of the BPS supply chain requires a strong partnership among electric companies, vendors, policymakers, and regulators at the SLTT government level. This coordination among stakeholders is imperative to ensure alignment on the understanding of grid security to identify appropriate, cost-effective priorities.

Exelon

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

The Department should not only ensure that procurement practices and requirements continue to evolve to match changes in the threat landscape but also provide guidance on supply chain security standards and incident reporting standards. Exelon believes that an effective way to provide guidance would be for DOE to develop a centralized mandatory supply chain security framework. To the extent additional SLTT governments need similar information they could receive it from DOE in a Freedom of Information Act ("FOIA")-exempt information exchange, such as the Critical Electric Infrastructure Information protections provided by Section 215A of the Federal Power Act. This would avoid duplicative and overlapping reports with the same information on the same issues to a multitude of different agencies in unique formats. Information sharing about threats and effective countermeasures would be streamlined through standardization in this area.

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?**

Current industry Supply Chain Risk Models ("SCRMs") do not currently define a process to identify foreign ownership, control, and influence ("FOCI") in purchases, components, or subcomponent parts. While Exelon continues to mitigate potential supply chain risks through a combination of security controls and contract provisions, the industry needs guidance on how to approach this FOCI issue from a more holistic point of view. Exelon's response to this question contains information on the work performed by the industry, and information on the challenges.

In instances where Exelon has asked vendors questions to determine FOCI, we have enforced the controls from our contract language to ask vendors to provide that information rather than conduct an audit of product and components and subcomponents, which are impractical for a single utility to conduct and repetitive if more than one utility would need the same information. In the absence of a centralized common approach, utilities have each begun to develop their own programs to complete evaluations of vendors for unwanted foreign influence on component and subcomponent parts. As the industry shares many of the same vendors, this means that there are multiple evaluations that a single vendor needs to complete to conduct business. This is inefficient and unnecessarily costly for the electric industry and its customers and vendors because of the lack of standardization. Exelon's Security Risk Assessment ("SRA") program for its vendors was

Exelon

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

developed to screen vendors and thereby ensure they meet basic security hygiene requirements. The SRA covers a broad range of questions, including, for example, assessing whether a vendor has implemented:

- an industry recognized Information Security Policy (*e.g.*, NIST CSF or ISO-27001);
- the use of anti-malware to secure devices and ensure malware signatures are regularly updated;
- a practice of conducting employee background investigations, including criminal checks;
- an information access management process;
- steps to protect data at rest, in use, and in transit;
- a program to properly dispose of data;
- a program to define and test business continuity and disaster recovery measures;
- a security incident handling program, which includes customer notification and coordination;
- programs to ensure customer notice and mitigation of vulnerabilities that impact vendor products or services;
- baseline security configuration management;
- security logging and monitoring;
- cyber vulnerability management and patching programs to protect vendor assets;
- a vendor asset management program;
- vendor network protections;
- vendor physical security protections;
- remote access controls on vendor systems; and
- security controls over third-party and fourth party (*i.e.*, sub-tier vendor) engagements.

With respect to this last area of inquiry regarding vendor implementation of security controls governing sub-tier vendors, Exelon's SRA program specifically assesses and determines in advance whether a prospective vendor will use subcontractors in delivering materials or providing services to the Company. If subcontractors are used, vendors must confirm whether the prospective vendor will:

Exelon

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

- ✓ purchase materials or services from companies (or their affiliates) that are not prohibited from doing business with the United States federal government;[13]
- ✓ require subcontractors to comply with the vendor's industry accepted Information Security Policy (*e.g.*, NIST CSF or ISO 27001); and
- ✓ apply and enforce the same or more stringent security controls that the vendor is held to in its contract with Exelon.

A subset of Exelon's SRA questions, including the above sub-tier vendor questions, are non-negotiable "gating" questions. If a prospective vendor provides an unacceptable answer to these questions, Exelon will not do business with them. Based on SRA responses, Exelon maintains metrics in a security profile of its vendors and uses those metrics to identify and minimize security risks as well as to guide future procurement decisions.

While this approach has successfully enhanced Exelon's supply chain cybersecurity posture and weeded out unsuitable vendors, such as vendors unable or unwilling to provide this information, this is Exelon's unique approach. It would be much more cost-effective for industry, vendors and ultimately customers if a single vendor could complete a single common security risk assessment and if that assessment was then accessible by any potential utility buyer. As the industry grapples with developing a standardized approach for the interactions to ensure a secure supply chain, the Department could inform the conversation by centralizing the necessary information, providing a certified approach to a vendor risk assessment, and assisting in the development of a standardized manner to store and access this information.

While the industry has made some significant progress on a security risk assessment in the NATF (identified in our response to Question 1), adoption of the form is not yet widespread enough to reduce the amount of duplicative work that is placed on industry vendors. A standardized approach that identifies the key information that utilities need to make a risk-based procurement decision would be the cornerstone of a successful supply chain security process. DOE should recommend guidelines for security risk assessments that draw on existing approaches developed by the electric industry.

The Department could provide direction to the industry on what information clearly indicates a compromised supply chain. In absence of this guidance, some utilities have begun to

[13] Exelon currently excludes any vendor who obtains products or services from Kaspersky, Huawei Technologies Company, ZTE Corporation, Hytera Communications, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company, or affiliates of these companies.

Exelon

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

request a Bill of Materials ("BOM") from vendors for hardware and software. In our experience described in more detail in response to Question 4 of Section I, the majority of Exelon's vendors are not prepared to provide a BOM for their products, primarily because no agency has ever required this of them. To complicate the problem further, if a vendor does provide a BOM it has proven difficult for a utility buyer to process the document. Because there is no standardized BOM format, the documents vary in length, in level of detail, and can be thousands of pages long for a single device or system. As a result, a BOM can vary in its usefulness, or require significant utility-side work to extract relevant and meaningful information from the sheer volume of data provided.

Finally, the Department can help by identifying a common process for the industry to store, access, and update the security risk assessments of vendors and associated information. It would be beneficial to both DOE and industry to establish an office that could be responsible for handling industry inquiries and ensuring that industry and vendors receive consistent guidance. The goal of a centralized program is to reduce the risk of potential supply chain compromise. A centralized location for this information reduces the risk of supply chain compromise because it provides intelligence to inform risk-based decisions by utilities. In the absence of these steps, many utilities will have to rely upon vendor attestations and certifications to determine compliance.

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?**

Exelon recommends that the Department should initially focus on the Priority BPS Equipment that is within DCEI and currently part of the Bulk Electric System ("BES") as defined by the North American Electric Reliability Corporation ("NERC").[14] This approach follows DOE's priority of focusing first on DCEI while also leveraging certain existing NERC procedures, processes, and consolidated information sources established through the Reliability Standards approved by the Federal Energy Regulatory Commission ("FERC") as mandatory and effective under Section 215 of the Federal Power Act. This would enable utilities to quickly identify an

[14] NERC defines the BES as "all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy." *See* NERC Glossary of Terms Used in NERC Reliability Standards, Note, this definition contains a number of detailed equipment inclusions and exclusions that electric sector entities are currently tracking and could more expeditiously identify and bring into scope for Executive Order rulemaking purposes.

Exelon

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

initial set of critical equipment that should be covered by any forthcoming DOE regulations under the Executive Order.

Consistent with DOE's priorities under the RFI, this initial risk-based approach would leverage existing electric sector programs to identify the equipment and systems that are the most critical to BPS reliability. A phased-in and risk-based approach would allow electric utilities and DOE the time necessary to isolate the equipment at issue, identify the vendors of the equipment, and work to close the gap on information necessary to implement supply chain cybersecurity controls required by any future federal requirement (*i.e.*, corporate ownership and control information and component information), which in many instances may take time and coordination with vendors to identify.

A well-designed rule that leverages a standardized risk assessment methodology and focuses on a small subset of critical equipment can also avoid unintended harm to small businesses in the electric sector. Like many companies, Exelon has promoted strong diversity and inclusion goals and, as a result, uses a significant number of small businesses, particularly women and minority-owned businesses, in its BPS supply chain. These efforts have benefited Exelon and the many communities in which Exelon operates. The support from these small businesses has also improved reliability of the BPS by ensuring Exelon has a broad range of qualified U.S.-based and U.S.-controlled local vendors to call on to support BPS operations. Nevertheless, small businesses have limited personnel and resources. A poorly designed pre-qualification process (*i.e.,* one not designed with small businesses in mind and, therefore, that favors larger vendors with more resources) could easily cause small businesses to drop out of Exelon's supply chain and create permanent barriers to entry. Moreover, small businesses are often the test beds for innovative ideas and technologies. Poorly designed rules also run the risk of stifling product or service innovation. It is important that DOE develop and implement a balanced process that avoids these and other unintended adverse effects. A phased approach as discussed in these comments will allow DOE to address the greatest immediate risks while building a longer-term program that does not adversely impact small business participation, competition, diversity, or innovation.

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?**

Exelon

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

Exelon's experiences over the past year in developing and implementing the compliance controls called for by the Prohibition Order suggest that obtaining the required transparency into sources of components within vendor-supplied equipment cannot be done quickly, and would therefore require a much longer lead-time to implement fully. In addition, certain key provisions within the Prohibition Order contained ambiguity that Exelon needed to interpret when designing and implementing its controls.

Exelon's discussions with its vendors revealed that the vendors themselves have limited visibility into their own supply chains, particularly with respect to software, firmware, and digital subcomponents associated with the electric equipment they sell to Exelon. As a result, those vendors cannot currently provide Exelon with the information needed to verify that their equipment does not contain a single component or subcomponent from foreign-adversary-owned, controlled, directed, or jurisdictional suppliers. Exelon will continue to press our vendors to investigate and determine the identity of their component providers and disclose that information to Exelon expeditiously, but it is unclear how quickly vendors will be able to do this.

In addition to efforts Exelon made to capture data from vendors before the certification date, we also worked with a third-party service to conduct a study of our vendor security questionnaire and issue a request for software BOMs. To conduct this study, we identified a subset of vendors who are potentially subject to Section 889 compliance under the 2020 National Defense Authorization Act. We sent a request to 202 vendors for a BOM as proof that there were no devices that were impacted by the PRC. Of the 202 vendors, only 15 replied with a BOM. Responses from the other 187 vendors ranged from the information not being available, the information being proprietary to no reply. The BOMs we did receive varied greatly in approach, format, and depth of information provided. Some exceeded 1,000 pages, while others were attestations from the vendor certifying our requirements.

As mentioned above, if DOE could define or endorse a common format for BOMs, this would greatly improve process efficiency. Because of the limited availability of information from vendors about their own supply chains, the most effective way to make quick progress toward better securing the electrical industry supply chain is to focus efforts on high-priority, high-risk components, vendors, and facilities.

Starting with a "prohibited list" of vendors or devices that is informed by specific intelligence DOE has received would be an ideal way to begin prohibiting certain equipment. As

Exelon

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

originally raised in our response to the August 24, 2020, RFI[15], Exelon believes a "prohibited list" could be implemented more quickly and effectively than a "prequalified list" for four reasons.

First, the Department can take immediate action to prohibit the use of equipment from specific vendors that the federal government may have already identified as being under the FOCI of one of the foreign adversaries identified in the RFI. The Department can call on the deep expertise of its National Laboratory system and leverage the unique capabilities of the larger U.S. Intelligence Community to rapidly move forward on such prohibitions. Doing so would enable DOE to quickly identify and communicate information regarding vendors under FOCI of a foreign adversary that may be used by the electric sector and exclude those vendors or their products accordingly.

Second, the electric sector already has processes in place to exclude vendors found to be deficient by the Federal Government for security reasons. In the recent instance of foreign adversaries presenting a national security threat to the United States in the information technology and communications services sector, specific entities were identified and Exelon promptly implemented procedures to ensure that equipment from Kaspersky, Huawei Technologies Company, ZTE Corporation, Hytera Communications, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company, or affiliates of these companies are not installed on our systems. Exelon has screening processes to prevent these entities from entering its supply chain. Since the electric sector has experience identifying and excluding federally prohibited vendors from its supply chain, DOE should leverage this experience and start by prohibiting vendors who pose a known risk to the BPS.

Third, screening vendors for a "prequalified list" will take longer to implement. Regardless of the approach DOE ultimately takes with the EO rulemaking, developing a pre-qualified list will take a significant amount of time to curate. Verification of records to rule out FOCI by a foreign adversary down to the component level of BPS equipment will be a massive undertaking for the electric sector and its vendors. During this period, as information is developed to demonstrate that a vendor is under FOCI of a foreign adversary, they can be added to a prohibited vendor list and barred from BPS procurements.

Fourth, the "prohibited list" approach would allow DOE the time needed to develop a

[15] Exelon Response to Request for Information on Executive Order 13920, Securing the United States Bulk-Power System, 85 FR 26595 (May 4, 2020). Submitted August 24, 2020.

Exelon

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

"certification" or "pre-authorization" process while minimizing the potential for severe supply chain disruptions that could seriously impact BPS operations and reliability. Any "pre-qualification" process, if not carefully developed, has the potential to cause serious unintended consequences. One such risk is that small or medium-sized businesses, including women and minority-owned business, might withdraw from electric sector business opportunities due to the cost or time to achieve approval. A poorly designed pre-qualification process could stifle product or service innovation and create barriers to entry for new or smaller entities. Exelon values its policies promoting supplier diversity and inclusion, which have brought both equity and innovation to the electric sector. It is important for DOE to develop and implement a balanced "certification" or "pre-qualification" process that avoids these adverse effects. Taking a stepwise process that begins with a "prohibited list" will allow DOE to address the greatest immediate risks while building a longer term "pre-qualified" program that does not adversely impact vendor participation, competition, diversity, or innovation.

A similar list of "prohibited equipment" will offer twin benefits for grid security. First, the list can help Exelon and other electric utilities efficiently target their search for at-risk equipment in their existing electric systems, and leverage DOE's access to intelligence information not currently available to power companies. Second, the list can help BPS entities as they modernize their systems in coming years. Power companies are making procurement decisions now on transformers that are often purpose-built and may not be delivered and installed until years after they are ordered as these are very expensive, very complex, and custom-designed pieces of equipment. Those extended timelines put companies at risk of buying products that may subsequently be prohibited. By providing a list of prohibited equipment, DOE can help Exelon and other utilities reduce those risks and securely modernize their BPS equipment.

Section II: 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 order to develop an effective prohibition, Exelon urges DOE to incorporate these high-level themes:

Any DOE action should use an approach that leverages information from the Intelligence Community that clearly states the risk that needs to be mitigated where the prohibition is

Exelon

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

determined after feedback from both industry and vendors within the industry. The approach should be a phased implementation plan (start with DCEI, for example) that uses a risk-based framework for a narrowly tailored set of devices that is based on risk intelligence from existing programs including, but not limited to CyTRICS and CRISP. Any prohibition plan should allow for significant lead time to plan and implement security controls and be aligned with the timeline to complete the efforts utilities must undertake. The prohibition should avoid non-critical "rip and replace" requirements as some devices, components or subcomponent parts do not immediately have a U.S.-based supplier or other certified seller. If certain devices became prohibited due to some failed aspect of a FOCI framework, there may not be a market alternative and all utilities have to consider the implications to power delivery and system reliability. However, public-private information sharing can be used to identify potentially hazardous devices on existing networks. Once identified, electric utilities can then work with DOE and other government agencies to remediate those concerns.

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?**

The high-level phased framework presented in response to the preceding question could be used for electric infrastructure serving other critical sectors as well.

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?**

The framework provided in the answer to Question II.1 could also be applied to electric infrastructure enabling the national critical functions.

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

In order to sufficiently identify the critical infrastructure within our service territory we will need to work extensively with our vendors to identify components and subcomponents on devices that support critical pathways, as this continues to be a key difficulty.

Exelon

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

This can be overcome through sufficient scoping guidance from DOE. Any requirements would need to be very specific regarding how to identify prohibited vendors to reduce the time required for analysis of vendors and the type of equipment prohibited. The earlier Prohibition Order was somewhat unclear on whether components and subcomponents were covered and what level of related hardware, firmware, and software associated with prohibited equipment might have been prohibited. With sufficient guidance and adequate time, utilities will be able to identify critical infrastructure within their service territories that would enable compliance with such requirements.

Once the types of prohibited equipment are identified, Exelon will then need to identify where that equipment is installed within its electric networks. The same types of devices are frequently used at substations regardless of whether the substation is DCEI, NERC, etc. When Exelon purchases devices, we do not purchase a NERC widget or a DCEI widget. The Company often purchases devices in bulk and then deploys them as necessary. Exelon understands that utilities are generally similarly situated regarding these issues and will therefore need sufficient lead time to perform walkdowns to identify all the devices that may be impacted.

The Department must also consider that in the absence of a centralized approach, each utility with a substation or other electric facility included in the scope of the order must perform vendor outreach as well and that could take time. In addition, because the industry shares many of the same vendors, we anticipate that the vendors will not be able to respond to all customers simultaneously. It would be more efficient and cost-effective for the vendors to reply with their information to a standardized questionnaire maintained and stored in a secure, centralized repository.

Finally, successful and timely identification of critical infrastructure within Exelon's service territory that would enable compliance with any prohibition order requirements will depend on DOE's adoption of starting with limited types of equipment and vendors identified through a risk-based framework and honing the parameters of the program based on lessons learned prior to expanding the scope of any prohibition. A narrowly tailored rule—at least initially—would be more straightforward to implement than a broad prohibition on transactions involving suppliers subject to some level of control by a foreign adversary. An overbroad initial set of prohibitions is likely to be difficult to implement with certainty on an expedited basis and could have hard-to-predict market impacts, particularly for categories of equipment with limited suppliers.

Exelon

Jacqueline Carney
Director, Federal Government Affairs
101 Constitution Avenue, NW
Suite 400 East
Washington, DC 20001
www.exeloncorp.com

202-637-0347 Office
202-480-4755 Mobile
202-347-7501 Fax
jackie.carney@exeloncorp.com

IV. Conclusion

In conclusion, Exelon appreciates the Department's efforts in working with its federal partners and the energy industry to secure America's Bulk-Power System. We urge DOE to consider these comments and continue to work with industry as it develops implementing regulations for Supply Chain Security. Thank you for the opportunity to provide this input.