UNITED STATES OF AMERICA
BEFORE THE
DEPARTMENT OF ENERGY

Ensuring the Continued Security of the Unites States Critical Electric Infrastructure	)))	6450-01-P

COMMENTS OF THE EDISON ELECTRIC INSTITUTE

The Edison Electric Institute ("EEI") submits these comments in response to the Request for Information ("RFI") issued by the Department of Energy ("the Department" or "DOE") on April 22, 2021.[1] 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. DOE states that these recommendations are intended to enable an approach that builds on, clarifies, and, where appropriate, modifies prior executive and agency actions.

EEI is the association that represents all U.S. investor-owned electric companies. EEI members provide electricity for more than 220 million Americans and operate in all 50 states and the District of Columbia. As a whole, the electric power industry supports more than seven million jobs in communities across the United States. EEI's members are committed to providing affordable, reliable, and increasingly clean electricity to customers now and in the future. Supply chain security is critical, and a long-term strategy that emphasizes identification, analysis, and mitigation for the most potentially vulnerable facilities and equipment whose compromise poses the highest risk of significant grid impacts is an approach EEI's members

[1] 86 FR 21,309.

support. EEI members are well aware of the threats to supply chain security and constantly work to combat those known threats and look forward to working with the Department to learn about additional threats known to government and find ways to mitigate threats to the supply chain. Collaborative methods that prioritize the most critical facilities and assets on the electric grid that complement existing electric company tools will better serve supply chain security as opposed to prescriptive methods which are potentially unfeasible and impractical to implement.

I. INTRODUCTION

EEI and its member companies provide the following comments to help further strengthen supply chain risk management for the electric power system in light of the continued and evolving threat adversaries pose to our critical infrastructure. EEI appreciates the Department's recognition of and interest in coordinating with the utility industry and others to ensure procurement practices and requirements evolve to match changes in the threat landscape and continue to protect critical infrastructure. The electric power sector uses many existing tools, methods, and programs to address grid-related threats but, as end-users of electric equipment in the supply chain, recognizes the continuing need for and assistance from government in finding ways to enhance, adapt, and add to these tools as threats to the supply chain and electric grid evolve. EEI members are subject to supply chain regulations and adhere to a variety of security practices to protect supply chains and the electric grid. These responsibilities, programs, and duties protect the grid and should be considered by the Department as it determines whether any new recommendations or actions are warranted. This includes (1) deploying technologies that improve situational awareness and ensuring actionable intelligence; (2) ensuring threat indicators are communicated at the right time to the right people in industry and government; (3) preparing for and exercising coordinated responses to both

natural and malicious threats to energy grid operations; and (4) working closely with other interdependent infrastructure sectors (communications, downstream natural gas, financial services, and water) to enhance preparation and response to threats against the grid. It is these tools and processes already in place that the Department should consider as a baseline when considering how to implement complementary approaches to enhancing supply chain risk management. This will better aid the Department in achieving its goals with a targeted approach to further enhance supply chain and grid security. Many efficiencies can be gained in leveraging existing cyber and physical security and supply chain processes, as opposed to creating and imposing upon the industry a new set of processes that could disrupt existing measures to combat the threats or access to critical equipment.

EEI supports an approach that enhances resilience: prioritizing and protecting elements that are singularly essential to grid reliability, with a risk-based approach that has the flexibility for electric companies to prepare and plan for and adapt to evolving threats to the grid. The regulations and tools used by EEI members help mitigate potential supply chain risks based on a risk-based, defense-in-depth philosophy, and any additional initiatives the Department takes should recognize the tools that are integrated in electric companies' security posture by prioritizing equipment in the most critical pathways. In support of this prioritization, DOE's approach should be flexible such that it recognizes the unique threats individual electric companies face due to their system design and topology, customer base, and existing security controls.

Prior to the outset of any DOE action, DOE must put a premium on clarity by communicating and coordinating with industry to identify more specifically the highest risks, the nature of the risk, and describe which facilities, equipment, subcomponents, and parts are

susceptible to ensure electric companies – and the government itself – are focused on the actual threats to grid security. Doing so will ensure that the Department has identified a defined list of facilities, equipment and subcomponents based on precise concerns. Prioritizing the highest impact equipment that may be more susceptible to intelligence-based, substantiated risks will allow stakeholders needed flexibility to better to address supply chain concerns without risking the safe, affordable and reliable delivery of electricity. New directives from the Department, whether addressing equipment in the supply chain or already in use, could affect the market for critical equipment, including creating disruptions to the use of existing equipment and availability of replacement equipment, and could have a spillover effect on the day-to-day grid reliability upon which our member companies' communities and customers rely for essential services and may increase the ultimate costs to electric customers.

It is also critical to understand that, even once a particular facility, piece of equipment or subcomponent thereof is identified, the supply chain for electric power equipment is enormous and involves many other stakeholders who develop and build those components and it is not the end-use electric companies who have information about what is inside those pieces of equipment or components. Even then it is fair to assume that suppliers cannot know the source of all the components. Electric companies are only part of the supply chain and as end users naturally have limited visibility into the supply chains of the equipment they purchase. Electric companies have many tools to identify threats to the supply chain and electric grid, but, by definition, these are not all encompassing. Government has access to sensitive information that it should find ways to share so all affected stakeholders understand what equipment is of concern and why it is of concern. We encourage the Department to collaborate with and help electric companies by sharing this information and include other stakeholders who have the knowledge

about the equipment electric companies purchase to identify flexible solutions to grid security supply chain concerns.

II. BACKGROUND AND REQUEST FOR INFORMATION

To strengthen the resilience of America's critical infrastructure, the Administration recently issued Executive Order ("E.O.")14017, America's Supply Chains,[2] which directs the Secretary of Energy, in consultation with the heads of appropriate agencies, to identify and make recommendations to address risks in the supply chain for high-capacity batteries and review and make recommendations to improve supply chains for the energy sector industrial base. The electricity subsector industrial control systems cybersecurity initiative "100-day sprint" announced by the Department is intended to enhance the integrity and security of priority sites' control systems by installing technologies and systems to provide visibility and detection of threats and abnormalities in industrial control and operational technology systems. 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.

E.O. 13920, Securing the United States Bulk-Power System,[3] issued on May 1, 2020, authorized the Secretary of Energy to work with Federal partners and the energy industry to take actions to secure the nation's bulk-power system. Most significantly, E.O. 13920 authorized the Secretary to prohibit the acquisition, transfer, or installation of certain BPS electric equipment sourced from foreign adversary countries. Informed by a July 8, 2020, request for information on

[2] Executive Order 14017, America's Supply Chains, 86 FR 11849 (Mar. 1, 2021).

[3] Executive Order 13920, Securing the United States Bulk-Power System, 85 FR 26595 (May 4, 2020).

implementation of E.O. 13920,[4] on December 17, 2020, the Secretary issued a Prohibition Order invoking the authority of E.O. 13920 ("Prohibition Order"),[5] which applied to a limited number of utilities that were prohibited from acquiring, importing, transferring, or installing certain electric equipment. The Prohibition Order identified equipment manufactured or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the People's Republic of China.

On January 20, 2021, E.O. 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.[6] As the Prohibition Order is 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 expired and, effective April 20, 2021, and the Secretary revoked the Prohibition Order to allow for the Department to conduct the RFI. E.O. 13990 also directed the Secretary and the Office of Management and Budget ("OMB") Director to "jointly consider whether to recommend that a replacement order be issued."[7] In the process of developing such recommendations, the Department is looking for opportunities to strengthen protections for high-risk electric equipment transactions, while providing additional certainty to the electric utility industry and the public and is collecting information through the RFI to inform future actions.

[4] Securing the United States Bulk-Power System: Request for Information, 85 FR 41023 (July 8, 2020).

[5] Prohibition Order Securing Critical Defense Facilities, 86 FR 533 (Jan. 6, 2021).

[6] Executive Order 13990, Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis, 86 FR 7037, 7042 (Jan. 25, 2021).

[7] *Id.*

III. COMMENTS

A. Any Supply Chain and Risk Management Strategy Needs to Prioritize Facilities That Are Most Critical to Grid Reliability.

In the RFI, the Department notes that the Federal Government and industry stakeholders have endorsed the need to strengthen supply chain risk management with respect to the electric system and recognize the threat foreign adversaries pose to critical infrastructure. EEI members address supply chain risk management in a risk-based, defense-in-depth manner using tools that are integrated into electric companies' security culture, most notably by prioritizing protections for supply chain equipment in the most critical pathways. The Department recognizes this approach in the RFI, noting that it "expects that, during the period of time in which further recommendations are being developed, utilities will seek to act in a way that minimizes the risk of installing electric equipment and programmable components that are subject to foreign adversaries' ownership, control, or influence."[8] The Department should integrate this strategic, risk-based approach as it contemplates any future action.

The Department inquires (Question A.1) about the roles states or local government to enhance their security efforts relative to the electric system and whether action the Department takes should apply to equipment installed on parts of the distribution system (Question B.1). In developing a strengthened approach to address the supply chain security of the U.S. electricity subsector, there must be a recognition of states' existing role in working with electric companies on these issues. Many states also have existing regulations that support the industry supply chain security posture. States have regulations that require utilities to work with their state government and their customer base to identify critical facilities may be helpful in accomplishing DOE's intent to holistically protect critical infrastructure. For example, California's SB 699 helped the

[8] 86 FR at 21,310.

California Public Utilities Commission and electric companies work together to identify which customers met certain characteristics to further identify critical customers. These existing, regulatory collaborations should be considered by the Department so that the Federal government can leverage existing work at the state level, rather than introducing potentially duplicative or contradictory regimes at the Federal level. Therefore, it is imperative that, to the extent there are facilities at the state and local level that are critical, the Department should coordinate and communicate with the states and the electric companies to have a clear understanding of, and agreement on, exactly which facilities, assets, equipment, or components are at risk, why they are at risk, and those must be prioritized.

While electric companies have the ability to identify critical infrastructure in their service territories (Question B.4), they do need to know what risks government knows about those critical facilities and whether the Department, based on its intelligence, knows of other facilities that are critical to national security.

Along these lines, the Department asks (Question A.2) what specific additional actions could be taken 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. Without the Department working with electric companies to identify the most critical facilities, assets, and with suppliers to identify source, ownership and control of equipment, or components, protecting everything within the supply chain or on the grid becomes infeasible and impractical, and more importantly, may not meaningfully improve the security of the supply chain. Allowing electric companies to focus finite resources on the highest priority threats will allow electric companies to react with alacrity and minimize unnecessary disruptions to supply chains, the financial and operational impact on electric companies and their customers, and help ensure the

continued reliability and affordability of the nation's energy supply. The greatest security improvements can be achieved by collaborating on identifying and targeting facilities with the greatest risk.

B. Equipment and Components That Affect Critical Facilities Must Be Clearly Identified and Described.

Any measures that are intended to enhance supply chain security must be risk-based and defined with specificity and precision so that all stakeholders can use their resources efficiently. Successful supply chain security measures require precision and clarity with respect to the duties of industry members. After prioritizing which facilities are at risk, there needs to be a mechanism to identify the equipment, components, or subcomponents that actually would have significant impacts to the reliability of the grid if compromised. Specific attention on identifying hard to replace equipment that is part of critical operations is paramount, especially where no alternative suppliers have been found to date. If the Department chooses a prescriptive approach, it must eliminate the ambiguities and uncertainties that existed in the Prohibition Order and the underlying Bulk-Power System Executive Order. Clarity with respect to how far down into the supply chain DOE intends stakeholders to reach, as well as a clear understanding of which equipment is covered (and components within equipment), should come before any additional orders, rules, or regulations ensue. Ideally, the identification of the most critical elements of the supply chain would be determined via a transparent and iterative process that from the outset includes all stakeholders in the supply chain, not just electric companies.

As the Department is aware, a significant amount of facilities and equipment and components in the electric equipment supply chain have no implications for the security of the grid because of how they are used. For example, the Department listed protective relays in the list of equipment in the Prohibition Order; however, this broad class includes several different types of

relays that have very different risk profiles (e.g., a microprocessor relay has a higher risk than a solid state relay). The Prohibition Order also identified certain equipment (such as circuit breakers and reactive power equipment) but did not identify whether or which components or subcomponents inside each were deemed to be included or excluded. The inclusion of subcomponents would change dramatically how – and whether – electric companies would need to comply with such an order. For example, the microprocessors, operating systems, firmware, and software within the control systems for reactive power equipment typically have exponentially longer and more complex supply chains than the supplier of a static VAR compensator or capacitor bank. The impact of components that are susceptible to a security issue are more on the supervisory and control elements of the system and likely not the hardware that makes up the bulk of the system such as poles, underground cable, wire and even distribution transformers. The items of greater significance would be the control systems such as supervisory control and data acquisitions systems, reclosers and advanced management systems along with the communication and relays to remote devices that these system utilize to monitor and control the system.

Even with a level of specificity and clarity, development of a prohibition list may lead to ambiguity for items that are not explicitly included in the list, notably subcomponents for which electric companies as end-users have no knowledge or control over how they are sourced. In nearly every case, the equipment identified comes from suppliers who have their own supply chains. Without the Department clearly delineating how deep into the supply chain entities are expected to reach, and ensuring that the burden does not fall solely on electric companies to determine who is responsible for identifying and sharing what specifically the Department is concerned about, electric companies and their workforce will spend precious time determining scope instead of working to mitigate threats to the highest impact equipment. These are just a few

examples that underscore the ineffectiveness of using blanket prohibitions and demonstrate the challenges that a non-specific list would create in determining whether a piece of equipment is included or excluded.

The Department asks (Question A.4) whether there are particular criteria it could issue to inform procurement policies, that would mitigate foreign ownership, control, and influence risks. DOE would first need to identify what constitutes "foreign ownership, control, and influence." Electric companies need to make decisions with whom to engage, and need clear guidance on what specific factors, such as physical location of manufacturing or level of equity ownership would constitute "foreign ownership, control, and influence." Otherwise, procurement decisions cannot be made with certainty. For example, given the number of equipment suppliers that are publicly traded and the speed at which stocks change hands, electric companies could never be certain whether a supplier has foreign ownership.

C. Intelligence Sharing Is Integral to Strengthen the Security of the Supply Chain.

In Question A.3, the Department asks what action it can take to facilitate responsible and effective procurement practices by the private sector. Use of a risk-based approach as described above will necessarily require DOE to share certain classified information with stakeholders and regulators to address new or emerging risks. Because the majority of critical infrastructure and the components are owned and managed by private industry, DOE will need to further refine and improve its ability to share timely information and intelligence with the private sector to remediate threats to the supply chain.

DOE should continue to partner with the energy sector to enhance classified and unclassified information sharing protocols, and in turn, develop processes for supply chain risk management and evaluating potential foreign ownership, control, and influence concerns. A

nation-of-origin risk assessment for all components of electric grid equipment by electric companies would be burdensome and infeasible as electric equipment end users without a framework and parameters for reasonable application. The federal government's National Industrial Security Program requires that cleared U.S. defense industry stakeholders safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. This model could be a source to develop an appropriate information sharing program with industry stakeholders to further bolster supply chain and grid security. Additionally, DOE could take steps to expand the pool of security-cleared personnel at electric companies to include Chief Procurement Officers or related job classifications to ensure that sensitive threat information is available to those charged with procurement decisions. The continuously evolving nature of the threat landscape underscores the need for flexibility and militates against a rigid approach. As electric companies work with DOE to reduce risk, an intelligent adversary will change its tactics, techniques, and procedures. Therefore, collaboration and coordination between DOE and electric companies must continue to evolve as well.

DOE could improve the sharing of information in other ways, such as expanding remote briefings or adapting existing secure video teleconferencing capabilities beyond their current, limited span. Joint information sharing fora with the Electricity Subsector Coordinating Council ("ESCC"), Oil and Natural Gas Subsector Coordinating Council, and the Critical Manufacturing Sector Coordinating Council would further help to stimulate information sharing between sectors and between industry and government.

Further, the Federal government has established precedent for notifying the private sector of companies that pose significant risk to national and economic security, through Section 889 of the National Defense Authorization Act and the naming of five covered telecommunications providers

on the Department of Commerce's Entity List. As DOE identifies concerns with foreign ownership, control, and influence, it should build upon Commerce's precedent and add companies of concern to the Entity List so that utilities can make the best decisions informed by government intelligence.

Improving the security of the supply chain requires a strong, regular communication and partnership among electric companies, vendors, policymakers, and regulators at all levels. This coordination, coupled with sharing of government intelligence, among stakeholders is imperative to ensure alignment on the understanding of grid security to identify both appropriate and cost-effective priorities.

D. Industry-Government Collaboration Is Critical to Supply Chain Security.

The Department seeks recommendations for how to best exercise its role as the Sector Risk Management Agency to inform and coordinate with the utility industry to ensure their procurement practices and requirements evolve to match changes in the threat landscape and best protect critical infrastructure. As noted throughout these comments, EEI members take supply chain procurement seriously and work in various capacities including compliance with and adherence to North American Electric Reliability Corporation ("NERC") Reliability Standards as well as their own additional tools to protect the supply chain. Electric utilities currently engage in information sharing and testing programs that identify threats and vulnerabilities and incorporation of indicators of compromise, participate in communities for sharing supply chain risks, and facilitate close coordination among industry and government partners at all levels, and through the ESCC in particular. Companies engage in multiple approaches and coordinate with the Electricity Information Sharing and Analysis Center ("E-ISAC"); federal agencies including DOE, the Federal Energy Regulatory Commission ("FERC"), NERC, Department of Homeland Security, the FBI;

and state (and where applicable, local and tribal) governments to identify and mitigate threats.

The ESCC is focused on multiple areas to improve the security posture of the industry and the energy grid, including consideration of how the industry proactively prepares for and responds to threats. This partnership leverages government and industry strengths to develop and deploy new technologies, share information, design and participate in drills and exercises such as the bi-annual Grid Security Exercises ("GridEx"), and facilitate cross-sector coordination.

Another joint effort began recently when the E-ISAC, in partnership with the ESCC, assembled the E-ISAC-ESCC Supply Chain Compromise Tiger Team to convene key industry participants that can leverage perspective and partnerships from within the sector, other sectors, and across government entities. The Tiger Team identified resources that entities could use to mitigate and manage risk associated with supply chain vulnerability and implemented a series of webinars from key electric system vendors to electric asset owner-operators with a focus on reducing security risk related to supply chain compromise. These webinars included presentations from SolarWinds, Microsoft, FireEye, and CrowdStrike on their response experiences.

Strengthening the security of the energy grid through industry-government information sharing includes the Cybersecurity Risk Information Sharing Program ("CRISP"). CRISP enables near real-time machine-to-machine sharing of cyber threat data among government and industry stakeholders. CRISP seeks to facilitate timely bi-directional sharing of actionable unclassified and classified threat information, using advanced collection, analysis, and dissemination tools to identify threat patterns and trends across the electric power industry. Cyber threat information shared through CRISP informs important security decisions not just among participating

companies, but to all E-ISAC members throughout the electric sector, as information obtained by the technology is then shared anonymously through the E-ISAC portal.

The industry has proactively developed and executed collaborative programs designed to enhance security and resilience. Among these is the recently established Energy Cybersecurity Alliance ("ECA" or "the Alliance"). The purpose of the Alliance is to enhance the security and resilience of the North American energy grid by providing a forum for electric companies and service providers, manufacturers, and suppliers of equipment and software to discuss and share potential safety and security-focused solutions. In bringing together these interdependent but distinct communities, the ECA strives to enhance the energy sector's readiness by discussing potential risks, vulnerabilities, and threats; identifying opportunities and possible solutions to reduce such risks, vulnerabilities and threats; and developing and sharing recommendations and potential solutions to enhance the safe and secure delivery of energy across North America. This partnership aims to help electric companies and vendors understand each other's points of view. Although the Alliance is in the early stages of its development and outreach efforts, its structure and activities are designed to protect critical infrastructure by supporting the development of solutions that improve the resilience of the energy sector and are broadly informative to all stakeholders, ultimately to the benefit of consumers. This type of collaborative engagement between suppliers and the electric sector could be leveraged by the Department to serve as a ready resource to provide efficient, relevant, and substantive input into the rulemaking process.[9] DOE should leverage these collaborate programs to enhance supply chain risk management.

[9] Use of a collaborative approach will be beneficial to ensure industry's valuable knowledge and expertise to protect the security and reliability of the electric grid. *See also* the July 16, 2020, letter from Senators Manchin and Risch to then Energy Secretary Brouillette encouraging the Department to engage with electric companies and suppliers of BPS system equipment throughout its efforts to protect the security and reliability of the electric grid, https://www.energy.senate.gov/public/index.cfm?a=files.serve&File_id=C55514F9-1409-406F-A526-618C6BD87F1F.

E. Department Strategy Should Complement Existing Industry Tools.

EEI member electric companies proactively engage in activities that underscore the seriousness with which they take the importance of providing continuous, affordable, reliable, and resilient operation of the electric grid. The risk-based, defense-in-depth approach to grid and supply chain security that is integrated in electric companies' security culture allows electric companies to focus valuable resources on the highest priority threats. EEI members take supply chain procurement seriously by using different tools, tactics, strategies, programs, and partnerships to protect and support grid reliability, but as end users, despite having limited or no control over the upstream supply chain of electrical equipment, electric companies are subject to supply chain regulatory standards and have been proactive in addressing for supply chain security in procurement contracts and facilitation of patching security vulnerabilities in the supply chain.

1. Electric Companies Are Subject to Supply Chain Regulatory Standards Which Are an Important Part of the Industry's Security Posture.

Under FERC oversight, the electric power industry is subject to mandatory and enforceable NERC Reliability Standards that include a robust framework for operations, planning and security. NERC's Critical Infrastructure Protection ("CIP") Reliability Standards include cyber and physical security and supply chain mandates. The NERC CIP Reliability Standards allow responsible entities flexibility in choosing compliance approaches best tailored to their company. The NERC CIP Reliability Standards take a broad and layered approach to cybersecurity for cyber systems and their associated cyber assets, address vendor remote access and software authentication and integrity risks and extend cybersecurity requirements from the internal operational environment to the external procurement of cyber systems. The NERC CIP Reliability Standards addressing the supply chain have been in force a short time, consequently, additional requirements or standards at

this point are premature. Rather time for implementation and gap analysis is warranted to determine whether any changes or additions are needed.

While the NERC CIP Reliability Standards should be viewed holistically for addressing risks from cyber attacks, the following exemplify one part of the many rigorous steps electric companies take to protect the grid both internally and throughout the supply chain lifecycle. The supply chain risk management Reliability Standards require responsible entities to establish organizationally-defined processes that integrate a cybersecurity risk management framework into the system development life cycle.

The NERC CIP Reliability Standards require electric companies to conduct annual cyber vulnerability assessments of critical cyber assets and their networks. Reliability Standard CIP-005 requires electric companies to manage electronic access sessions with vendors, including interactive remote access and system-to-system remote access. It also gives electric companies visibility into all active vendor remote access sessions and the ability to disable any active remote access sessions in case of a system breach. Additionally, Reliability Standard CIP-007 mandates managing system security, including ports and services, patches, malicious code prevention, monitoring and access control. Likewise, Reliability Standard CIP-010 is intended to aid electric companies in preventing and detecting unauthorized changes to certain critical cyber assets by specifying configuration change management and vulnerability assessment requirements in support of protecting the assets from compromise that could lead to misoperation or instability.

Reliability Standard CIP-013-1 requires electric companies to evaluate and address cybersecurity risks from vendor products and services during system planning and procurement. Reliability Standard CIP-013-1 allows electric utilities to take a flexible approach to establish organizationally defined processes that integrate a cybersecurity risk management framework into

the system development lifecycle. This NERC supply chain approach allows electric companies to adapt to ever changing threats without burdensome, antiquated lists of prohibited activity or equipment. Supply chain risk management demands this same type of flexibility as is in the CIP Reliability Standards.

Lastly, supply chain regulation has historically focused directly on regulated electric companies, leaving them solely accountable for all of the upstream development and manufacturing practices; however, this creates an imbalance where electric companies may represent only a fraction of a suppliers' business, leaving them with little leverage to drive meaningful change in product design, manufacturing, or lifecycle management. The Department should consider the precedent set under the recent Executive Order on Improving the Nation's Cybersecurity, whether requirements for software developers and equipment manufacturers should be required to report vulnerabilities, significant incidents, and other helpful security information to the Federal government to ensure that such information gets into the hands of electric companies and who shoulder the majority of the risk on behalf of their customers.

2. Addressing Cybersecurity Supply Chain Risk in Contracts.

EEI members have been proactive in addressing supply chain security in procurement contracts and facilitation of patching security vulnerabilities in the supply chain. EEI has developed a Model Procurement Contract Language document that contains a tailorable set of contract provisions to address cybersecurity supply chain risk and patching vulnerabilities for procurement of assets subject to the NERC CIP Reliability Standards.[10] The model procurement language reflects evolving industry standard practices, including changes that broaden references to

[10] Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk Version 2.0, https://www.eei.org/issuesandpolicy/Documents/EEI%20Law%20-%20Model%20Procurement%20Contract%20Language.pdf.

specific industry standards.

The CIP Reliability Standards require entities to develop documented supply chain cyber security risk management plans to use in cyber system procurement that will require vendor cooperation to protect the security of the cyber system supply chain. Electric companies address these requirements by, among other means, inserting contract terms that address the security controls in agreements with vendors. The model procurement contract language targets the processes required in CIP Reliability Standards, specifically Reliability Standard CIP-013-1, as well as supporting contract terms that address related information and data protection to strengthen cybersecurity overall.

Electric companies and suppliers can use provisions of the model procurement contract to establish, document, and implement risk management practices for supply chain delivery of hardware, software (including patches), and firmware that could impact the energy grid. It includes a suite of provisions for documentation of supplier chain-of-custody practices, inventory management programs (including the location and protection of spare parts), information protection practices, integrity management programs for components provided by sub-suppliers, instructions on how to request replacement parts, and commitments to ensure that spare parts are made available. Other provisions require suppliers to specify means of digital delivery for procured products (e.g., software and data), including how patches will be validated and monitored to ensure the digital delivery remains as specified.

The model procurement document also includes language to aid in identification for country or countries of origin of the procured product, including hardware, software and firmware. This could include identification of the countries where the development, manufacturing, maintenance and service for the product originated, including for sub-components. Provisions

have been added to provide electric companies a software bill of materials for procured products consisting of a list of components and associated metadata that make up a component and inclusion of using trusted channels to ship procured products, and a demonstration of detecting unauthorized access throughout the delivery process can also be part of the contract. There are also provisions for investigation of computer viruses or malware in any software or patches. These model provisions are intended to provide flexibility so that they may be tailored to the individual electric company and supplier risk profiles and exemplify yet another way electric companies are working to combat supply chain risk with vendor partners.

F. EEI Supports Equipment Testing and Domestic Manufacturing.

The Department is also interested in how to enable better testing of critical grid equipment, encourage better procurement and risk management practices, and develop a strong domestic manufacturing base with high levels of security and resilience. DOE should first conduct a rigorous analysis of risk posed by various pieces of equipment whether already in use or in development before implementing any approach intended to further strengthen supply chain risk and share their results with industry. DOE could work with the National Institute of Standards and Technology to develop consistent criteria for hardware and software bill of materials. Doing so would support standardization in these bill of materials, which would make the development and provision of such useful tools for the purposes of identifying provenance and the potential presence of any foreign ownership or control.

With regard to domestic manufacturing, EEI supports efforts to develop a U.S. supply chain for equipment. Domestic supply of this equipment helps to ensure that the protections regarding development practices and foreign ownership controls are applied, reduces the risks from laws such as the Peoples Republic of China's National Intelligence Law, and also makes auditing and in-

person validation of security measures significantly more affordable and more effective. However, in many instances, there are no viable or cost competitive domestic sources for critical electric equipment, leaving utilities either without domestic options or with a significant additional cost, which is ultimately shouldered by ratepayers. From an electric company perspective, equipment procurements involve months, sometimes years, of costly budgeting, engineering, and planning before equipment can be put into production safely and reliably. Before a domestic supply is firmly established, shifting away from certain suppliers in established markets may reduce already limited competition and increase costs for critical equipment during the transition. For example, the process of purchasing large power transformers is largely dependent on a very limited number of foreign manufacturers, and in the case of some equipment, may primarily depend on a single country. Large power transformer production is labor intensive and requires a collection of materials and equipment including conductors, insulations, and different types of steel. The Department should consider the time and rigor involved to qualify alternative suppliers and equipment. DOE is aware of its study (and is working with EEI members to support the study) of the procurement and supply environment for large power transformers.[11] This study outlined the complex and time-consuming procurement cycle for large power transformers.

In addition to transformers, equipment supporting electric generation is particularly sensitive to potential supply chain risks. Power generation that is provided at the transmission level and back-up generation that supports substations are manufactured to customer specifications and have long-lead times that are sensitive to raw material availability and logistics, which represents a significant investment for electric companies.

Given the complexity and length of the procurement and manufacturing process, the

[11] DOE, Office of Electricity Delivery and Energy Reliability, *Large Power Transformers and the U.S. Electricity Grid*, Update (Apr. 2014), https://www.energy.gov/sites/prod/files/2014/04/f15/LPTStudyUpdate-040914.pdf.

Department should recognize that the sources of supplier equipment and the parts that make up the equipment come from diverse locations. Any actions taken by the Department may affect the market for critical equipment and impact day-to-day grid reliability upon which our communities and customers rely for essential services. DOE should avoid implementing prohibitions of equipment that would necessitate immediate and widescale equipment, component or subcomponent replacement or the disruption of imminent deliveries of electrical equipment for time-sensitive electric projects. DOE should explore ways to incentivize the establishment of this domestic supply and consider financial incentives to bridge the cost gap between domestically produced equipment and foreign-sourced critical grid equipment.

To that end, any prohibitions on supply chains using equipment or components sourced from problematic suppliers should include options for electric companies other than complete prohibitions. DOE should consider:

- A process for seeking exceptions for otherwise prohibited equipment that includes criteria for obtaining such exceptions by demonstrating that the risks have been addressed, such as by the adoption of mitigating measures. For example, equipment that is configured in a manner that prevents remote access or control and does not allow it to communicate with an electric company's networks would not present the same supply chain risks that are of concern to DOE.
- A process that allows individual equipment suppliers to be pre-approved by the Department so that electric companies can rely on the Department's verification to validate that suppliers and manufacturers employ robust controls to mitigate supply chain risk based on fundamental security controls, independent assessment and certification.

- A process for investigating and confirming that a piece of equipment is free of threats in situations where the supply chain lacks complete transparency. For example, equipment that includes a microprocessor can be reviewed and scrubbed for malicious code.
- Promoting the creation of a system that identifies criteria across domestic and foreign providers of electric equipment and issuing certifications to those providers that meet certain supply chain standards.

IV. CONCLUSION

EEI encourages the Department to work with industry to clearly identify and prioritize what facilities, equipment and components of equipment could be compromised that, if compromised, would be most impactful to grid operations. A long-term strategy where the most susceptible and highest impact facilities and corresponding equipment are addressed first is more valuable to grid security than prescriptive orders which are potentially unfeasible and impractical to implement. The Department should also avoid actions that could negatively affect the critical equipment market and day-to-day impact on grid reliability and use prudence to avoid an undue cost impact of regulations to electric customers. EEI looks forward to continuing to collaborate with the Department to protect the supply chain for the highest impact critical electric infrastructure.