Edison Electric INSTITUTE

Power by Association℠

August 24, 2020

Mr. Charles Kosak
Deputy Assistant Secretary
Transmission Permitting and Technical Assistance Division, Office of Electricity
Department of Energy
1000 Independence Ave SW,
Washington, DC 20585

[Submitted Electronically]

RE: Comments of the Edison Electric Institute on the Department of Energy's Request for Information on Securing the United States Bulk-Power System

Dear Mr. Kosak:

The Edison Electric Institute ("EEI") appreciates the opportunity to submit comments on the Request for Information issued by the Department of Energy ("the Department" or "DOE") on July 8, 2020, concerning implementation of the Executive Order 13920 issued May 1, 2020, titled, "Securing the United States Bulk-Power System" ("Executive Order"). EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for 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 and its member companies support the national security goals of the Executive Order. Knowing that sophisticated adversaries target exploitable supply chain vulnerabilities with the intent to attack the electric grid, EEI members look forward to working with the Department to develop additional measures that supplement the electric power sector's efforts to address grid-related threats. EEI members continue to gain experience in this area and, as risks evolve, will monitor the scope of covered facilities, systems and resources for grid security purposes.

EEI's comments focus on the industry's existing measures and unique expertise in maintaining the affordable, safe and reliable delivery of energy to the customers and communities they serve. In light of the variety of tools that electric companies use today and the corresponding experience in combating grid threats, EEI urges

the Department to implement the Executive Order surgically and strategically by prioritizing elements that are uniquely essential to the Bulk-Power System.

We understand the importance of these matters and appreciate that DOE has balanced an urgency to implement the Executive Order with a need to hear from stakeholders. To that end, thank you again for the two-week extension to submit these comments; this extra time was helpful in ensuring a broad cross-section of EEI perspectives are reflected in these comments.

Should you have any questions about EEI's comments or perspective on the Executive Order, please do not hesitate to contact me, David Batz (dbatz@eei.org, 202-508-5586), or Bob Stroh (rstroh@eei.org, 202-508-5145).

Sincerely,

Scott Aaronson
Vice President, Security and Preparedness
Edison Electric Institute

UNITED STATES OF AMERICA
BEFORE THE
DEPARTMENT OF ENERGY

Securing the United States Bulk-Power System	)	DOE–HQ–2020–0028

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 July 8, 2020,[1] pursuant to Executive Order 13920 issued May 1, 2020, titled, "Securing the United States Bulk-Power System" ("Executive Order"). The Executive Order directs DOE, in consultation with the heads of several other agencies, to issue regulations implementing the authorities the President delegated to the Secretary of Energy ("Secretary"). Through the RFI, the Department seeks information to understand the energy industry's current practices to identify and mitigate vulnerabilities in the supply chain for components of the bulk-power system ("BPS").[2]

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.

[1] 85 Fed. Reg. 41,023.

[2] 85 Fed. Reg. 26,595.

I. INTRODUCTION

EEI and its member companies support the national security goals of the Executive Order. Knowing that sophisticated adversaries target exploitable supply chain vulnerabilities with the intent to attack the electric grid, EEI members look forward to working with the Department to develop additional measures that supplement the electric power sector's efforts to address grid-related threats. EEI members continue to gain experience in this area and, as risks evolve, will continue to monitor the scope of covered facilities, systems and resources for grid security purposes. EEI member companies play a crucial role in further strengthening the BPS by using a variety of existing tools, methods and programs detailed below, and seeking to enhance, adapt, and add to these tools as threats evolve.

EEI supports the four pillars of the Executive Order. Consistent with the spirit and goals of the Executive Order, these pillars should be implemented in a manner that uses and reflects the industry's existing measures and unique expertise in maintaining the affordable, safe and reliable delivery of energy to the customers and communities they serve. In light of the variety of tools that electric companies use today and the corresponding experience in combating grid threats, EEI urges the Department to implement the Executive Order surgically and strategically, with feedback from industry, by prioritizing elements that are uniquely essential to the BPS so that electric companies have the flexibility to prepare and plan for, absorb, respond, recover from, and adapt to threats to the grid.

In particular, the implementation of the Executive Order should:

- Recognize the existing risk-based, defense-in-depth philosophy and corresponding tools that are integrated in electric companies' security culture by prioritizing equipment in the most critical pathways.

- Allow for flexibility in implementation by recognizing that electric companies face unique threats due to their location, size, system design and topology,

customer base and security controls.

- Understand that the equipment identified in the RFI is complex and interconnected with long lead times for design, procurement, testing and deployment.

- Avoid actions that affect the market for critical equipment, including disruptions to the use of existing equipment and availability of replacement equipment, and consider potential impacts to day-to-day grid reliability upon which our communities and customers rely for essential services.

- Exercise prudence by recognizing that any regulations that affect electric equipment markets may increase the equipment cost and the ultimate costs to electric customers.

Below, EEI describes the security measures electric companies already undertake to protect supply chains and the electric grid. These include North American Electric Reliability Corporation ("NERC") reliability standards; close coordination among industry and government partners at all levels and through the Electricity Subsector Coordinating Council ("ESCC") in particular; and efforts to prepare, respond, and recover should an incident impact the energy grid through cyber mutual assistance (much like assistance after storms); culture of security initiatives, and spare transformer programs. These responsibilities, programs, and duties protect the grid and, coupled with the recommendations set forth above, will better inform the Department in achieving its goals with a targeted approach to further enhance the BPS supply chain and grid security.

Electric companies take security and protection of the grid seriously, and current tools and processes complement the goals that the Department is seeking to achieve. Several of those programs are described below. Rather than create and/or impose an entirely new set of untested processes on the industry that could inadvertently introduce or disrupt existing measurers that combat threats, an alternative would be to leverage existing processes. Maximizing efficiencies in how the Executive Order's directives are addressed and implemented will allow the industry to

achieve the Executive Order's national security objectives faster, with fewer roadblocks. It would also avoid conflicts between the Executive Order and the ongoing, no less important, cyber and physical security work occurring daily at all electric companies across the nation through existing, time-tested processes.

In sum, we encourage the Department to leverage existing tools used by electric companies to partner with and participate in addressing the grid security concerns of the Executive Order in a risk-based manner to prioritize assets on the most critical pathways.

II. BACKGROUND

A. The Executive Order

On May 1, 2020, President Trump issued the Executive Order finding that the nation's BPS is a target for acts that threaten the United States, including by adversaries engaged in malicious cyber activities. The President declared a "national emergency" with respect to threats to the BPS, citing the authority granted to him under the Constitution and two statutes: the International Emergency Economic Powers Act ("IEEPA") and the National Emergencies Act. IEEPA gives the President certain authorities to address "any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States" if a national emergency is declared with respect to such threat. The President determined that the unrestricted foreign supply of "bulk-power system electric equipment" and the resulting potential for foreign adversary exploitation constitute a threat to the national security, foreign policy, and economy of the United States.[3] To address this threat, the President found that additional steps are required to protect the security, integrity, and reliability of BPS electric equipment.

The Executive Order prohibits the installation or acquisition of any BPS equipment if the

[3] 85 Fed. Reg. 26,595.

Secretary, in consultation with other agencies, has determined that the equipment has been "designed, developed, manufactured, or supplied" by persons owned or controlled by a foreign adversary and where the transaction poses an undue risk of:

(i) sabotage or subversion to the U.S. BPS;

(ii) catastrophic effects to the security and resilience of U.S. critical infrastructure; or

(iii) other threats to national security or the security and safety of American citizens.

Notably, the Executive Order gives the Secretary the authority to prohibit the transactions covered by the Order, develop procedures as preconditions for approval of such transactions for the BPS, and to pre-qualify certain equipment, vendors, and manufacturers. The Executive Order explains that rules and regulations developed by the Secretary may define particular countries and persons as foreign adversaries and may identify specific equipment and countries that need scrutiny. The Secretary also is charged with developing procedures to license certain transactions that the Executive Order otherwise would prohibit and other processes for mitigating vulnerabilities posed by the designated equipment and manufacturers.

B. DOE Request for Information

The Department seeks comments on specific equipment as outlined below to enable a phased process by which the Department can prioritize the review of BPS electric equipment by function and potential impact to the overall BPS. Accordingly, in the RFI, the Department states that the Secretary may establish specific pre-qualification criteria for a set of components that support defense critical electric infrastructure ("DCEI") and other critical loads and critical transmission feeders (69 kV and above) reported under critical infrastructure protection reliability standards "as formulated by [NERC] and approved by the Federal Energy Regulatory Commission

("FERC")."[4] The Department states that specific essential reliability services of interest may also include black start systems.

The Department seeks comment on the following types of equipment: transformers (including generation step-up transformers), reactive power equipment (reactors and capacitors), circuit breakers, and generation (including power generation that is provided to the BPS at the transmission level and back-up generation that supports substations). This includes both the hardware and electronics associated with equipment monitoring, intelligent control, and relay protection. Only transformers rated at 20 MVA and with a low-side voltage of 69 kV and above are included.[5] The Department does not plan to develop a supply chain risk management ("SCRM") tool or repeat questions already deemed best practices from well-established SCRM frameworks and tools. The Department states that it is focused on improving utility owner/operators' asset/operations risk assessments by incorporating the identification of enterprise risk associated with supply chain vendor/services into the acquisition systems process. As an example, the Department points to their Cybersecurity Capability Maturity Model ("C2M2") as a tool that an organization might apply to continuously assess its cybersecurity posture.

The industry worked closely in partnership with DOE and other stakeholders to develop the original C2M2 framework. C2M2 has been widely adopted across the energy sector and is used by a number of other critical infrastructure sectors as well. Many electric companies use the C2M2 framework to regularly assess their overall cybersecurity risk management posture and

[4] *See RFI*, 85 Fed. Reg. at 41,024.

[5] Although some of the equipment identified by the Department includes some types of cyber assets, the list of equipment includes more than cyber-focused equipment, including hardware and electronics, that may not include cyber assets. Thus, the Cybersecurity Capability Maturity Model ("C2M2") framework may be useful for some but not all of the equipment.

identify areas for enhancements. In addition, the industry has partnered with DOE to enhance and update the model as the threat landscape has evolved over time.

III. COMMENTS

A. Electric Utilities Have Instituted Significant Measures to Secure the BPS Supply Chain and Actions Taken by the Department Should Complement These Activities.

Collectively, electric companies engage in activities that underscore the seriousness with which they take the importance of providing continuous, reliable and resilient operation of the electric grid. As noted below, EEI members take a risk-based, defense-in-depth philosophy and use corresponding tools that are integrated in electric companies' security culture by prioritizing equipment in the most critical pathways. By implementing a strategic, risk-based approach, the Department will allow electric companies to focus valuable resources on the highest priority threats. Rules or regulations that contradict or duplicate existing tools or processes that are widely used and continue to be developed by industry and government should be avoided.

In addition, electric companies face unique threats due to their location, size, system design and topology, customer base and security controls. For example, the technology deployed to provide for security and communications may be very different in a dense urban environment as opposed to a more rural area.

The Department identifies equipment that are complex pieces of machinery, often interconnected with one another and have long lead times for procurement and deployment. The Department should recognize that electric companies have ongoing projects already in development and any proposed mitigations may take months or years to implement effectively. Many electric companies have system design and enhancement cycles that include equipment within the Executive Order and RFI that last from five to nine years. DOE should provide

reasonable notice to electric companies and their government partners so they can address threats collaboratively. Further, where DOE directs companies to address a specific threat, it also should provide the relevant intelligence and should allow for input from asset owners and operators. Information sharing about the nature of threats is critical when vulnerabilities are identified by the Department and will help electric companies react to and mitigate the threat using any existing and new tools. We encourage the Department to appropriately prioritize the equipment covered by the Executive Order and RFI to identify the appropriate high-risk material items so high-risk mitigation efforts can be created, executed and audited for compliance. This includes clearly identifying material items and subcomponents that are and are not covered so electric companies can focus time, money and efforts on the appropriate items that present true risk vulnerabilities. EEI also recommends that DOE develop a phased approach where the most susceptible equipment and highest impact equipment are addressed first. Once the equipment is identified, addressing potential concerns could come in the form of a process for identifying the vulnerability, testing to determine the likelihood of a misoperation or damage to equipment with replacement being used only when all other options are not viable.

Electric companies undertake considerable and varied measures to protect their supply chains. Consequently, 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. For example, if certain suppliers are prohibited by DOE, but there are few commercially viable alternatives, limited market or production capacity may be stretched thus restricting access to key equipment classes. DOE should avoid implementing rules that would necessitate immediate and widescale equipment replacement without appropriate notice and optionality. Such an action similarly could stress limited market capacity by creating a surge in

demand and could introduce reliability challenges if supply cannot meet this new demand immediately. DOE can expect electric companies to face significant material lead time increases if demand is consolidated to fewer suppliers. Natural events (i.e., catastrophic storms and wildfires) can also instantaneously and dramatically increase demand for critical equipment necessary for system reliability. The Department should consider the time and rigor involved to qualify alternative suppliers and equipment.

Prudent implementation of prospective rules would appropriately recognize that any regulations that affect electric equipment markets affect (and increase) costs to electric customers. Electric equipment suppliers often spend years designing, sourcing, manufacturing, and testing equipment before it is sent to market, which represents a costly development process. 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. Further, removing certain suppliers from established markets may reduce already limited competition and drive up costs for critical equipment. For example, EEI members are in the process of purchasing large power transformers for which some have no domestic manufacturers and a very limited number of foreign manufacturers, and one country on the list of countries identified in the RFI is the primary supplier of phase shift transformers. Construction of a large power transformer is a collection of materials and equipment including conductors, insulations, and different types of steel, and is labor intensive. DOE should ensure that any final rule avoids disrupting these established supply chains and markets and incorporates cost considerations to minimize the financial impact on utilities and their customers to ensure the continued reliability and affordability of the nation's energy supply.

B. The Equipment Identified in the RFI Is Complex and Interconnected with Long Lead Times for Procurement and Deployment.

The RFI identifies, among other things, the following equipment relevant to potential supply chain risks: transformers and generation, including power generation that is provided to the BPS at the transmission level and back-up generation that supports substations. The Department should take note that these types of equipment are manufactured to customer specifications and have long-lead times that are sensitive to raw material availability and logistics and represent a significant investment for electric companies. Many pieces of electrical equipment illustrate these concerns. For example, large power transformers are typically custom made with procurement lead times of at least one year or more, with the manufacturing process adding at least another year. Because large power transformers are so expensive and tailored to customers' specifications, usually they are not easily interchangeable with each other.[6] Timelines are further subject to the manufacturing process, which is similarly complex. In particular, the availability of raw materials can significantly affect manufacturing and delivering transformers once they are ordered by electric companies. Transformers are just one example illustrating the challenges of developing and procuring vital electrical equipment. Any rule the Department fashions needs to consider the time to find and vet new suppliers and allow for production ramp up, testing and start-up requirements. DOE is aware of its study of the procurement and supply environment for large power

[6] STEP and other programs are valuable tools that make transformers available in the event of an emergency, although the assets available in these programs cannot be used universally in all cases (e.g., they are specific to certain voltage classes or may not always be the optimal choice for a particular company's system). These potential risks are mitigated by the number of assets available, and the many companies that participate, in these programs as well as the ability of many companies to use less than optimal assets to restore power while they procure a more permanent solution.

transformers.[7] This study outlined the complex and time-consuming procurement cycle for large power transformers. There are several distinct steps and procedures, including prequalification of manufacturers and a competitive bidding process, before the manufacturing process can begin. The prequalification process is essential to ensure the quality of the final product, which must adhere to company specifications, as the production environment and the capability of the manufacturer can significantly affect the reliability of the large power transformer. While the electric grid is inherently reliable, given the redundancies built into the system and the processes for replacing some equipment in an emergency, disruption of equipment lead times as a result of any DOE regulations risks placing unnecessary stresses on the system.

Given the complexity and length of the procurement and manufacturing process, the Department should recognize that the sources of supplier equipment and the parts that make up the equipment come from diverse locations and maintaining the supply chain is an important tool for mitigating risks that could impact grid security. Accordingly, the Department needs to consider that any rules it imposes could have unintended consequences for electric companies and grid reliability and security and the corresponding supply chains.

C. EEI Member Companies Currently Engage in Many Proactive Approaches to Grid Security.

Protecting the nation's energy grid and ensuring a reliable, resilient, and affordable supply of energy are top priorities for electric companies. Electric companies' customers and the nation depend on it. EEI members take a risk-based "defense-in-depth" approach to protecting critical energy grid assets from threats. This multi-layered approach encompasses compliance with

[7] 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

rigorous, mandatory, and enforceable reliability standards and regulations, and includes activities that surpass the minimum requirements; close coordination among industry and with government partners at all levels; and efforts to prepare, respond, and recover should an incident impact the energy grid. Below EEI describes the different tools, tactics, strategies, programs, and partnerships that the industry currently uses to protect and support grid reliability. 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 the Executive Order.

1. NERC Reliability Standards 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 mandates. The CIP Reliability Standards are moving toward an objective-based outcome that allow responsible entities to choose compliance approaches best tailored to their systems.

Electric companies dedicate resources and personnel to implement processes, procedures and technology to comply the CIP Reliability Standards and other requirements. As the threats to the reliability of the BPS have evolved so too have the Reliability Standards. FERC has directed significant work to address BPS reliability and security through NERC Reliability Standards,

assessments and risk identification. Many of the CIP requirements provide protections so that the BPS can resist, absorb, and rapidly recover from coordinated cyber attacks. The CIP 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.

While the CIP Standards should be viewed holistically for addressing risks from cyber attacks, the following exemplify the 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 CIP standards require annual cyber vulnerability assessments of critical cyber assets and their networks. For example, Reliability Standard CIP-005 requires electric companies to manage electronic access. The standard covers all remote 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. To comply with the standard, electric companies use their supply chain cyber security risk management plans in procurement processes (e.g., request for proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan). Importantly and appropriately, Reliability Standard CIP-013-1 does not require any specific controls or mandate "one-size-fits-all" requirements due to the differences in needs and characteristics of electric companies and the diversity of BPS environments, technologies, and risks. Rather, the standard takes a flexible approach to allow responsible entities to establish organizationally defined processes that integrate a cybersecurity risk management framework into the system development lifecycle. For example, and in response to the Department's inquiry (Question A-3), to comply with CIP-013, some utilities implemented software integrity procedures. Consistent with the "what" not "how" approach in the CIP Reliability Standards, electric companies may tailor these processes to suit their unique corporate risk profile and system design. One example of the procedure for complying with CIP Reliability Standards involves verifying software integrity and authenticity of all software and patches by vendors that can involve periodic security patches and vulnerability fixes. The procedure provides a list of software tools that provide instructions to validate software integrity to confirm the file has not been corrupted or tampered with in any way. Part of the procedure includes a template that is completed to document how, by whom and when the software was validated. This document is attached to the change order that supplements the change management

process. DOE should allow the use of the same type of flexibility as is in the CIP standards in implementing the Executive Order.

The CIP Reliability Standards support grid reliability that indirectly but substantially support all other NERC operations and planning Reliability Standards. The Transmission Planning Standards are designed to ensure that the BPS operates reliably over a broad spectrum of system conditions and follow a wide range of probable contingencies (e.g., severe weather, successful cybersecurity attack, geomagnetic disturbance event). The Emergency Preparedness and Operations Standards ensure entities have plans, facilities, and personnel in place that are capable of recovering rapidly from events (e.g., system restoration, loss of control center functionality), that could impact the reliable operation of the BPS. The Protection Control ("PRC") Standards include standards that ensure that key elements of the BPS will remain in service for short-duration overload conditions, allowing time for system operators to mitigate the situation without unnecessary loss of load or damage to equipment. The PRC Standards also focus on preventing unnecessary tripping due to unstable power swings, which allow the system to absorb and recover without unnecessary loss of load or without contributing to events that might result in much larger power disturbances.

NERC, in coordination with its Regional Entities, has implemented a risk-based compliance oversight framework that incentivizes internal controls to support the reliability and security of the BPS by identifying, assessing, and correcting issues associated with the NERC standards. Registered entities must affirmatively demonstrate to NERC their methods and means of compliance, resulting in utilities having broad, ever maturing internal compliance programs.

The NERC Standards provide a solid foundation for strengthening the industry's supply chain and security posture. As explained below, given the dynamic threat environment, the

industry's efforts have developed layers of protection beyond standards that, despite increasing threats, has shown itself to be reliable.

2. Industry-Government and Cross-Sector Coordination Is Critical to Security of the BPS Supply Chain.

Electric companies do not depend on the CIP standards alone to protect their systems against security threats. Security programs are tailored to each company's unique operating and business environments to mitigate supply chain and security risk as threats and vulnerabilities change.

The Department asks (Questions A-4, A-6) energy sector asset owners and/or vendors to document the level of engagement in information sharing and testing programs that identify threats and vulnerabilities and incorporation of indicators of compromise, describe participation in a community for sharing supply chain risks, and whether the energy sector encourages security related information exchange with external entities, including the federal government. Companies engage in multiple approaches and coordinate with the Electricity Information Sharing and Analysis Center ("E-ISAC"); federal agencies including DOE, FERC/NERC, Department of Homeland Security, the FBI; and state (and where applicable, local) governments to identify and mitigate threats.

Executives from industry and government also coordinate at the most senior levels to identify and mitigate emerging risks and threats. The ESCC serves as the principal liaison between the federal government and the electric power industry, with the mission of coordinating efforts to prepare for, and respond to, among other things, threats to critical infrastructure. The ESCC includes electric company CEOs, the NERC CEO and trade association leaders representing all segments of the industry. The ESCC is a model for how critical infrastructure sectors can more effectively partner with government to mitigate supply chain risk. 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 in strengthening the security of the energy grid through information sharing includes the Cybersecurity Risk Information Sharing Program ("CRISP"). CRISP enables near real-time sharing of cyber threat data among government and industry stakeholders, while supporting machine-to-machine threat mitigation. 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. CRISP is a public-private partnership co-funded by DOE and industry and managed by the E-ISAC. 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.

Utilities' partnering to develop remediation strategies will continue to play a vital role in protecting the BPS supply chain. Following a risk-based approach will necessarily entail the sharing of classified information with stakeholders and regulators to address new or emerging risks. That said, the majority of critical infrastructure and the components listed in the Executive Order and the RFI are owned and managed by private industry and, therefore, a public/private partnership will be essential to address the threat. DOE and EEI members will need to develop classified/unclassified protocols among government and industry to remediate threats to the BPS. Along these lines, EEI recommends that DOE continue to partner with the energy sector to develop

the proper authorities and protocols for EEI members, in turn, to develop processes for SCRM and evaluating potential foreign ownership, control, and influence ("FOCI") concerns.[8] 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 of information to develop an appropriate information sharing program with industry stakeholders to further bolster supply chain and grid security. The threat landscape's continuously evolving nature underscores the need for flexibility. As the energy sector works with DOE to reduce risk, the intelligent adversary will change its tactics, techniques and procedures. Therefore, collaboration and coordination between DOE and EEI members must continue to evolve as well.

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

3. Electric Companies Currently Engage in Response and Recovery Exercises and Participate in Information Sharing Communities with Suppliers.

In addition to the information sharing and the regulatory responsibilities and partnership efforts described above, electric companies participate in and plan regular exercises for a variety of emergency situations that could impact their ability to provide electricity that test BPS electric equipment and analyze their security vulnerabilities, including incident response exercises at the national-level. NERC runs the bi-annual GridEx for utilities to demonstrate how they would

[8] A nation-of-origin risk assessment for all components of BPS equipment by electric companies would be burdensome without some framework for reasonable application.

respond to and recover from simulated coordinated cyber and physical security threats and incidents, strengthen their crisis communications relationships and provide input for lessons learned. Now in its sixth iteration slated for Fall 2021, GridEx is designed to test incident response plans, expand local and regional response, engage interdependent sectors and improve communication among electric companies, federal, state and local government, critical infrastructure cross-sector partners (ISACs and other utilities), and supply chain stakeholder organizations. Other exercises include testing all levels of government, private industry, and nongovernmental organizations to protect against natural disasters and cyber exercises to examine response capabilities and interdependencies between the electric and financial sectors. From these exercises, electric companies develop valuable experience in responding to incidents that affect grid reliability and security and use those experiences in improving recovery and limiting the scope of outages in other instances. These exercises also help participants strengthen their relationships to better coordinate and communicate during crises and develop actionable plans to improve their collective security posture.

Regarding the Department's inquiry about communities for sharing supply chain risks, the industry has proactively developed and executed collaborative programs designed to enhance security and resiliency. 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 energy 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. Although the Alliance is in the early stages of its development and outreach efforts, the structure and activities of the ECA are designed to protect critical infrastructure in a more efficient manner by supporting the development of solutions that improve the resilience of the energy sector, and be broadly informative to all stakeholders all to the ultimate 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 any ultimate rulemaking process.[9]

4. Electric Companies Participate in Mutual Assistance Programs to Counter Cyber Threats Based on Decades of Experience Working Together in Response to Major Incidents and Have Established Initiatives to Improve Security.

For decades, the electric power industry has operated voluntary mutual assistance programs that work collaboratively to restore service following storms, earthquakes, wildfires and other natural disasters. These mutual assistance programs provide a formal, yet flexible, process for companies to request assistance from one another. Building on the industry's culture of mutual assistance and informed by lessons learned from major destructive cyber incidents overseas as well as by exercises held in North America, the ESCC directed the formation of the Cyber Mutual Assistance ("CMA") Program in 2016. CMA is a natural extension of the electric power industry's longstanding approach of sharing critical personnel and equipment when responding to

[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 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

emergencies. By coordinating with the government and providing mutual assistance to address cyber threats, the electric power industry is enhancing our nation's ability to defend and protect against threats and to meet customers' expectations.

CMA is composed of industry cyber experts who provide voluntary assistance to each other in advance of, or in the event of, a disruption of electric or natural gas service, systems, and/or IT infrastructure due to an emergency which may require cyber assistance. Participation in the CMA is open to all entities that provide or materially support the provision of electricity or natural gas service. The CMA Program is designed to enhance the industry's ability to mitigate electric and natural gas service disruptions, and continues to increase engagement between electric companies and other stakeholders, including critical supply chains, through regular meetings, and information sharing and exercises. The CMA Program serves as yet another tool the industry uses to combat the threats contemplated by the Executive Order.

With new and dynamic risks constantly appearing on the horizon, EEI's member companies continually look for innovative approaches to address and mitigate these risks. In support of ongoing industry efforts, the chief executives of electric companies have established an initiative focused on security culture to emphasize better understanding of, and to drive continuing improvements to, security as a fundamental component of electric companies' corporate cultures. A security culture encompasses a set of values and a sense of responsibility and behaviors, demonstrated by an organization's workforce, that contribute to the protection and safeguarding of a company's assets and operations from security threats. Fundamentally, security is an obligation of every employee, executive, contractor, and supplier, and cannot be reserved only for a few personnel. Stakeholders across a broad range of functions and activities within electric companies, including operations, emergency preparedness, information technology, human resources, and

communications, are essential to advancing the development of a security-conscious workforce. Activities under the culture of security initiative are CEO-driven and are used to bolster electric companies' cybersecurity priorities.

Through the culture of security activities, electric companies enhance their organization's security posture and support ongoing company culture efforts to support employee awareness, engagement, and participation in security activities. These engagements help drive enhancements to a company's security practices in the near term and support the continued development of a security-conscious culture in the long term. The culture of security initiative cultivates an environment in which EEI member companies can share their strengths and their challenges, and collectively focus efforts to raise the bar as an industry.

5. Electric Companies Participate in Equipment Sharing Programs to Ensure a Reliable Supply of Electricity.

In addition to the industry's voluntary mutual assistance programs to restore power and respond to cybersecurity threats, electric companies participate in spare-equipment sharing programs to enable rapid recovery from events that render critical pieces of equipment unusable. These programs further backstop the other tools electric companies use to ensure grid reliability.

The Spare Transformer Equipment Program ("STEP") provides a mechanism to share assets when equipment is unusable and is based on a binding contract among participants for access to hard-to-replace transformers. The STEP program affords participants access to large power transformers in various voltage classes and sizes (Megavolt-amperes or MVA) located at participating utilities throughout North America. STEP participants have predefined obligations to commit, and the ability to obtain, spare large power transformers from other STEP participants under predefined conditions (called a triggering event). The STEP program imposes a mandatory obligation to share assets when a triggering event occurs. In addition, the program affords

members the opportunity, and provides a ready mechanism, to voluntarily share assets and provide additional mutual assistance to each other for emergency incidents that do not qualify as a triggering event. The STEP program is also designed to enhance the capability of mitigating energy disruptions by increasing engagement among its participants through regular meetings, information sharing and exercises.

In addition to STEP, the SpareConnect program provides an additional mechanism for BPS asset owners and operators to network with other SpareConnect participants concerning the possible sharing of transmission and generation step-up transformers and related equipment, including bushings, fans and auxiliary components. SpareConnect establishes a confidential, unified platform for the electric industry to communicate equipment needs in the event of an emergency or other non-routine failure. SpareConnect complements existing programs, such as STEP and voluntary mutual assistance programs, by establishing an additional, trusted network of participants who are uniquely capable of providing assistance concerning equipment availability and technical resources. SpareConnect provides decentralized access to points of contact at power companies so that, in the event of an emergency, SpareConnect participants are able to connect quickly with other participants in affected voltage classes. Once connected, those SpareConnect participants who are interested in providing additional information or sharing equipment work directly and privately with each other on the specific terms and conditions of any potential equipment sale or other transaction.

Two other notable industry initiatives include Grid Assurance and Regional Equipment Sharing for Transmission Outage Restoration ("RESTORE"). Grid Assurance is a stand-alone company that focuses on critical transmission equipment procurement, security and strategic equipment warehousing, equipment management, and logistics support to facilitate rapid

deployment of critical long-lead time equipment in light of a grid emergency. The RESTORE program provides additional sources for obtaining critical transmission equipment following disastrous events.[10] The RESTORE program creates a contractual vehicle by which participants may nominate their own spare transformers (and potentially other equipment) to be available to others. Use of these programs is yet another tool electric companies use to recover from cybersecurity events to ensure equipment availability and grid reliability.

6. Contract Language Addressing Cybersecurity Supply Chain Risk

The Department inquired (Questions A-4.d, A-5) about contract language used for 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 CIP Reliability Standards.[11] The model procurement language reflects evolving industry standard practices, including changes which broaden references to 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. Responsible Entities 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

[10] *Jurisdictional Regional Equipment Sharing for Transmission Outage Restoration Participants*, 163 FERC ¶ 61,005 (2018).

[11] 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.

Reliability Standard CIP-013-1, as well as supporting contract terms that address related information and data protection to strengthen cybersecurity overall.

Notable provisions of the model procurement contract can be used by electric companies and suppliers 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 that can be used require suppliers to specify how 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. If a supplier provides software or patches to the electric company, the supplier publishes or provides a hash conforming to the Federal Information Processing Standard Security Requirements for Cryptographic Modules (FIPS 140-2) or similar standard information on the software and patches to enable the electric company to independently verify the integrity of the software and patches.

Recently, model procurement contract provisions have been updated to identify 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.

IV. CONCLUSION

As discussed above, EEI encourages the Department to recognize electric companies' security culture and their existing tools to prioritize equipment in the most critical pathways, allow implementation flexibility based on the unique threats to each electric company, 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 partner with the Department to protect critical electric infrastructure.

August 24, 2020