Response to DEPARTMENT OF ENERGY (DOE)'s Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure

"Development of a Long-Term Strategy" implies that the DOE does not have a plan to protect the energy sector. On the contrary, DOE agencies have worked for decades to strengthen security and protect against vulnerabilities to the national grid and nuclear facilities. In 2003, HSPD-7 Infrastructure Identification, Prioritization, and Protection specifically outlined an initiative to protect critical infrastructure including the energy sector and had cross-functional committees to address supply chains. In 2013, PD-21, the Critical Infrastructure Security and Resilience directive superseded HSPD-7 and outlined several initiatives to improve plans and implement better infrastructure protection. These policies helped develop standards that are now used in procurement requirements but are overdue for an update that consolidates the many aspects of hardware, software and services into a simpler trust assurance framework for the electric energy sector to implement.

An example on how to investigate electric grid supply chain security can be found in a recent CISA report developed in cooperation with DOE's Argonne and Sandia National Labs – *Methodology for Assessing the Most Critical Information and Communications Technologies and Services* dated April 2020, in response to EO 13873. It focuses on the IT and communications infrastructure but is applicable to the electric grid infrastructure, which also uses IT equipment in grid operation and administration networks.

Although this RFI does not specifically call out cybersecurity, almost all electric grid operational technology (OT) and integrated information technology (IT) components are vulnerable to cybersecurity attacks. Supply chains must incorporate IT and OT cybersecurity rules and determine existing risks of existing grid equipment so that vulnerabilities are addressed in a prioritized manner. In 2019, the GAO reviewed DOE/FERC policies pertaining to the infrastructure security (updated most recently in March 2021 focusing on electricity distribution) and made recommendations to better address the National Institute of Standards and Technology (NIST) Cybersecurity Framework and evaluate the potential risk of a coordinated cyberattack on geographically distributed targets (i.e., production, transmission, distribution). NIST also has a Zero Trust Framework (SP 800-207) and Supply Chain Risk Management Practices for Federal Information Systems and Organizations (SP 800-161), both of which are applicable to the electric grid and provide more details than the NERC's Supply Chain Risk Management Plan released last year. These GAO recommendations need follow-up and DOE should advocate implementation of Zero Trust Frameworks for the entire energy grid infrastructure.

The point here is to take advantage of applicable and existing policies and best practices that has been implemented for our nuclear and defense infrastructures that are applicable to our critical infrastructure in the electric grid. DOE can leverage this work and determine <u>how</u> energy sector stakeholders should implement security solutions for their supply chains. Existing security risk assessments and Supply Chain Risk Management (SCRM) plans need a top-down review so that risk areas are quantified and prioritized together. Design, construction, and operation can be analyzed with AI and machine learning tools that optimize system efficiencies in dynamic models rather than static compliance reviews that do not keep up with evolving threats to critical infrastructure supply chains. Comments to specific questions:

A. Development of a Long-Term Strategy

Question A1. What technical assistance would States, Indian Tribes, or units of local government need to enhance their security efforts relative to the electric system? First, do <u>not</u> create a completely new

entity to provide technical assistance and expand the energy sector's oversight bureaucracy. There are existing resources throughout DOE and other government agencies that can be coordinated and used to establish guidance, training, and compliance measurement to assist states, Tribal, and local governments. These distributed government entities need a straight-forward SCRM model, criteria, and compliance verification to address the root causes of potential threats – not just the symptoms – and supports their entire electric infrastructure, not just discrete functions. Education and training programs such as the *Critical Infrastructure Protection* course at Idaho National Laboratory (INL) and similar programs can be used to present a path for improved procurement control and the ability to follow through on the strategic and tactical plans mandated by the DOE, industry regulations, and dynamic situational awareness.

Once tactical assistance is applied and being used, strategic support to organize federated regional decision-making can be promoted through Federal leadership. Since the energy grid is not geographically contained along the same borders as Tribes and local governments, this type of strategic planning support can help improve services as well as embedding security into the broader grid design rather than allowing stovepipes to create inherent weakness that affects everyone. For example, political incentives to build a solar or wind facility that requires long distance transmission to customers just adds to the number of transformers, IoT devices, and other equipment that must now be protected from physical and cyber threats as part of our critical infrastructure. A distributed local grid design with shorter distances between energy sources and customers decreases the strategic threat surface and provides a more reliable solution. This can be achieved with small modular nuclear reactors and waste-to-energy (WTE) gasification facilities distributed to meet local population needs (and for WTE, there is the bonus of reducing toxins going into landfills). Wind and solar can contribute as well to small, localized grids.

Question A2. What specific additional actions could be taken by regulators to address the security of critical electric infrastructure and the incorporation of criteria for evaluating foreign ownership, control, and influence into supply chain risk management, and how can the Department of Energy best inform those actions? The U.S. electrical grid is a complex federated community governed by different regulatory bodies. DOE is the lead policy organization; however, it is organized across functional stovepipes where policies differ in almost all business areas and functional domains that create potential security gaps. Therefore, the first step in identifying vulnerabilities surrounding critical infrastructure is to gain an in-depth understanding of the current state of critical assets, capacities, and total life cycle processes, as well as their associated policies and threats. Once the critical assets are prioritized using organizational knowledge sources form industry and government, the supply chains and associated work and data flow can be determined and protected.

The prioritization of critical assets is needed before a more in-depth analysis begins on the critical processes (particularly across grid functions) to maintain or add value to those assets. The processes are organized according to best practice industry frameworks and modeled at a level that sufficiently exposes implementation of overarching governing policies. For the electrical grid supply chain, the critical processes must include the industry's immediate operational processes and those belonging to partners in the extended enterprise. For example, a small component switch or controller, may have a different company other than the manufacturer or OEM to perform its preventive and repair maintenance. These repair companies may vary depending on service function, location, etc. and not necessarily be 'approved' from the same standpoint as a manufacturer but could easily introduce malware (or physical damage) to impair or destroy a service. Therefore, monitoring manufacturers, OEMs, and independent contractors is necessary to ensure supply chain security throughout component lifecycles.

Question A3. What actions can the Department take to facilitate responsible and effective procurement practices by the private sector? What are the potential costs and benefits of those actions? The FERC released a report in July 2020, *Joint Staff White Paper on Supply Chain Vendor Identification - Noninvasive Network Interface Controller*s (NICs), which investigated the means to trace equipment origins and determine risks from untrustworthy sources. However, the scope of the study was limited to vendor identification and did not provide further guidance on broader supply chain policy. DOE must determine the total process to implement procurement and supply chain standards that can be monitored and measured in predictive rather than reactive management approach.

First, identify and prioritize the opportunities for improvement and technology insertion based on greatest performance gain, against cost and time to implement. The results of analyses will pinpoint areas where improvements can be made and reveal areas that are ripe for process and technology insertion. Those opportunities are weighed based on the greatest possible gain in performance. High priority improvement opportunities are translated into requirement statements to drive the selection of best solutions.

Second, implement a supply chain trust model for private industry and local governments to use so that grid systems obtain appropriate assurance levels to operate under all situations. A good practice for this has been presented by MITRE (Martin, 2017, *Integrating Safety with Security in the Industrial IoT Ecosystem*) for various critical infrastructure industries. It is very similar to the systems analyses in submarine construction to ensure the component and system designs meet mission safety requirements including supply chain traceability for critical components (i.e., SUBSAFE) and test certification. Security risks to the grid infrastructure directly impact reliability and public safety thus require broader regulation than just imposing additional procurement rules.

This level of detail provides a more thorough breakdown of grid mission/component criticality to allow for methodical implementation of remediation and justification for Prohibition Authority (see below).

B. Prohibition Authority

Question B1. To ensure the national security, should the Secretary seek to issue a Prohibition Order or other action that applies to equipment installed on parts of the electric distribution system, i.e., distribution equipment and facilities? Determining the probability and severity of any given threat is needed to determine when a Prohibition Order is required. A combined security/system safety analysis feeding into a maturity model for grid infrastructure security (as described for Question A3) can illustrate specific risk areas where the Prohibition Order is activated for high-risk situations.

Question B2. In addition to DCEI, should the Secretary seek to issue a Prohibition Order or other action that covers electric infrastructure serving other critical infrastructure sectors including communications, emergency services, healthcare and public health, information technology, and transportation systems? Yes, see the comment to Question B1. Due to the interconnected aspects of the electrical grid to other critical infrastructure segments, all could have threats that impact the overall ecosystem if electrical power is lost and/or interrupted. The backup capabilities in each sector need to be included in the risk analysis to determine the overall impact of the threat(s) and use the same criteria for risk level thresholds.

Question B3. In addition to critical infrastructure, should the Secretary seek to issue a Prohibition Order or other action that covers electric infrastructure enabling the national critical functions? Yes, see

comments to questions B1 & B2. Once a risk matrix begins to take shape across critical functions, other infrastructure components and operations can apply the model and extend its impact to respective components in their sector.

Question B4. Are utilities sufficiently able to identify critical infrastructure within their service territory that would enable compliance with such requirements? The answer for this question depends on how "sufficiently able" is defined. The maturity level each organizational component has as it operates within their service territory *should* be sufficient to comply with a compliance framework as discussed in comments of previous questions. However, this framework only partially exists such as what has been applied to domains like IT/cyber infrastructure, operational safety, etc., not so much in supply chain operations. Supply chain security policies for critical infrastructure has not been fully implemented so an assessment of capability for industry to comply is premature.

The U.S. has detailed security policies and procedures associated with exports but not much for imports. The International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) are two important U.S. export laws to control the release of sensitive products and services from being sold to adversaries. U.S. Customs manages import policy compliance but does not address security concerns like ITAR and EAR from an import perspective. The Department of Commerce did engage in import oversight for the communications infrastructure but that has only been applied to select technology (e.g., 5G infrastructure). The minimum steps for utilities to identify their critical infrastructure include:

1. Decompose critical assets into enabling business processes and network maps.
2. Map security, compliance, and performance rules to core critical infrastructure processes.
3. Identify process integration, optimization, and risks for critical infrastructure assets.
4. Manage assets in accordance with risk tolerances throughout each asset's lifecycle.

NIST SP 800-30 is a good example of a risk-quantification method for utilities to use in understanding their supply chain and operational risks. DOE can establish the governance and measures to oversee their compliance and use the results to understand regional and national-level risks. However, universal standards for security must be incorporated into grid supply chains such that it makes compliance oversight compatible in dealing with critical infrastructure risks (collectively). To accomplish this , cross-sector collaboration and communication across the total energy supply chain should be promoted as a core business function.

DOE must rely on comprehensive standards, clear measurement criteria, and cross-government and industry collaboration to ensure utilities work together. Other supply chain standards, such as the Cybersecurity Maturity Model Certification, can serve as frameworks for a data-driven approach.

Without a structured approach, resources will be wasted, and time lost in trying to protect vulnerable energy services from another supply chain attack. Stakeholders must coordinate their IT and OT security efforts and address risks throughout system lifecycles including supply chain procurement (imported or not, foreign-owned or not).