**UNITED STATES OF AMERICA**

**BEFORE THE**

**DEPARTMENT OF ENERGY**

|  |  |  |
| --- | --- | --- |
| **Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure** | **)****)****)** |  |
| VIA EMAILElectricSystemEO@hq.doe.gov |  |  |

**COMMENTS OF AMERICAN ELECTRIC POWER SERVICE CORPORATION**

American Electric Power Service Corporation (“AEP”) thanks the Department of Energy (“DOE”) for the opportunity to respond to this Request for Information (“RFI”) and its efforts to get the insight of the entities who will be impacted by any future mandates.

AEP operates a large interconnected network of facilities that generate, transport, and deliver electricity across the United States to serve approximately 5.5 million residential, commercial, industrial, and wholesale customers in 11 states. AEP ranks among the nation’s largest generators of electricity, owning nearly 26,000 megawatts of generating capacity in the United States. AEP also owns the nation’s largest electric transmission system, with more than 40,000 miles of transmission lines and more 765 kilovolt extra-high voltage transmission lines, more than all other U.S. transmission systems combined. AEP’s utility units operate as AEP Ohio, AEP Texas, Appalachian Power (in Virginia and West Virginia), AEP Appalachian Power (in Tennessee), Indiana Michigan Power, Kentucky Power, Public Service Company of Oklahoma and Southwestern Electric Power Company (in Arkansas, Louisiana, and east Texas).

We have developed one of the industry’s most recognized and leading Supply Chain Security Programs utilized to identify potential risk from third parties on who we depend to provide products and services for the day-to-day operation of our business and the provision of electric utility services to our customers.

Making sure we understand the security posture of our providers is critical to ensuring we provide reliable service to those who depend on us. We would like to be an active participant in this process and assist the industry as a whole in attaining a secure and reliable grid. We are heavily involved with many industry organizations and participate in the development of regulatory standards. As the DOE is aware, the electric power system is vital to the Nation’s energy security, supporting national defense, emergency services, critical infrastructure, and the economy.

AEP has made considerable investments to develop one of the industry’s most recognized and leading supply chain security programs over the last 9 years and believe we can (i) provide valuable assistance and insight into any new regulatory process and (ii) help other asset owners implement and or mature their own program. Our existing program is an Enterprise program, which existed before regulatory requirements and has been and continues to be matured as we identify new areas we feel better inform our purchasers of any potential risks. Additionally, recognizing that we share the supply chain with thousands of other utilities, we have established the Asset to Vendor (A2V) network, which collects and shares supply chain cyber risk information with other utility industry entities, reducing their cost to understand risks which may be introduced through a third party relationship and to help other asset owners implement and/or mature their own programs.

Provided below are responses to the questions posed in the RFI:

# Response to Section A. Development of a Long-Term Strategy

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

There may be a need for financial and possibly even technical assistance for utilities who may not have the financial or human resources to develop or acquire the appropriate technologies or data in order to identify and mitigate risks in technologies already deployed. These items often come at significant cost in today’s market and some utilities may not have the ability to obtain the information or resources needed to comply with any order or requirement established by the DOE. AEP’s supply chain cyber risk sharing network, A2V, described above could be leveraged by States, Indian Tribes, or units of local government as technical assistance to enhance their security efforts relative to the electric system.

Additionally, many utilities are already subject to the North American Electric Reliability Corporation (“NERC”) Critical Infrastructure Protection (“CIP”) supply chain standards, which require risk assessments of the providers of products and services for operations which are subject to the standards. Coordination with the Federal Energy Regulatory Commission (“FERC”) and NERC should be part of any requirements or standards, to minimize overlapping or contradictory standards or requirements and that assets that fall under the NERC CIP standards are not subject to duplicative standards.

There must also be consideration given to how any new standards are enforced and audited. As stated in the previous paragraph, many utilities are already subject to NERC CIP standards and are audited on a regular basis by one of the eight Federal Energy Regulatory Commission-approved Regional Entities responsible for ensuring the reliability of the North American Bulk-Power System. These audits are very resource intensive and time consuming and extremely thorough, therefore, adding any new audit requirements would be extremely burdensome to the utilities and likely unnecessary.

1. **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?**
	1. If there is a decision to create additional requirements or standards, ensure they are in coordination with other existing standards currently issued and managed by other regulatory agencies.
	2. Support a database that allows the utilities a single location to get information needed about assets being purchased and deployed in the critical electric infrastructure.
	3. Support a facility or lab where physical components can be tested for potential risk to the critical electric infrastructure.
	4. Support a means and a set of standards for the manufacturers and developers of products used within the critical electric infrastructure, to register the components and source of those components into a central register (Software and Hardware Bills of Materials (S/HBoM)).
	5. Require that all manufacturers and developers of products used within the critical electric infrastructure register their products in the registry and that they maintain the registration as changes are made or recertify the entry on a recurring basis.
	6. Membership in organizations such as Grid Assurance should be encouraged by regulators. Grid Assurance is a fully-operational, stand-alone company founded, owned, and operated by AEP several and other major transmission owning utility companies who understand the challenges to operate and maintain a highly reliable and resilient grid.  Grid Assurance provides subscribing utilities with access to an inventory of spare transmission equipment dedicated to respond to catastrophic grid emergencies.  In particular, Grid Assurance (1) maintains an optimized inventory of newly manufactured critical long lead-time equipment vital to the operation of the bulk electric system, (2) provides secure domestic warehousing of the inventory of spares in strategic locations, and (3) develops and maintains pre-approved transportation and logistics plans to expedite the delivery of the inventory to utility subscribers as needed to respond to emergencies.
		1. Stockpiling dedicated assets is the only sure way to provide the necessary certainty to appropriately plan for recovering from such catastrophic events - certainty of asset availability, certainty of asset location, certainty of rapid delivery and certainty they will operate when installed. The use of dedicated stockpiles of difficult-to-obtain assets is a best practice used by many industries that also provide critical infrastructure and services to ensure they can recover from significant events.
2. **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?**

As stated previously, many utilities are already subject to the NERC CIP Supply Chain Security Standard (CIP-013), which requires certain procurement actions and requirements. Consider the actions required in that standard and determine how that might be extended to utilities who currently do not fall within the standard, if the impact of an incident within those utilities would have significant impact on the critical electric infrastructure.

Additionally, ensure that critical electric infrastructure is formally defined and understood by the utilities who may be subject to any new standards or regulations so that there is no ambiguity in what is expected to be protected and what is not.

Finally, require utilities to obtain information from suppliers so that utilities are able to make their own risk based procurement decisions.

As far as costs and benefits, depending on the depth of assessment required, the number of assets covered, and the specifics of the standards, the costs could be significant, however without any details as to what a standard or regulation may look like, it is impossible to estimate.

Some impacts of a comprehensive testing and registration process, as outlined in this response, could result in higher costs for acquired products, reduced availability of products, increased time to procure products and possibly even reduction in reliability to the grid if replacement parts are not available due to restricted supply chains caused by loss of available components impacted by a prohibition order against certain manufacturer’s source of components. Separately, from a cost of compliance perspective, AEP’s supply chain cyber risk sharing network could be leveraged minimize the burden of complying with the new procurement policies.

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

To be effective any standards or regulations must:

* Be explicit as to which products and services are covered by them.
* Must state without ambiguity the level of component which is subject to them (e.g., chips, boards, subsystems, entire application, modules within an application, open source components used within an application, operating system, firmware, etc.).
* Must include a list of the specific countries, manufacturers, and/or systems which are impacted by the controls established.
* Specific language on who is responsible for the entry and maintenance of information relative to the products and services covered by any new standards or regulations.
* Set specific requirements regarding when information is to be provided by manufacturers and developers to the regulating authority or any system or service for the collection of that information.

# Response to B. Prohibition Authority

1. **To ensure the national security, should the Secretary seek to issue a Prohibition Order or other action that applies to equipment installed on parts of the electric distribution system, i.e., distribution equipment and facilities?**

AEP believes that a specific prohibition order may be overreaching, but receiving guidance based on intelligence would be beneficial. The intelligence coupled with capabilities mentioned in response to the previous section would assist in informing the utility so that they can make an informed and risk based decision. A prohibition order may result in removal of a technology that may be necessary to operate but unavailable from any other source. The utility would be responsible to employ appropriate mitigations where the component may introduce unacceptable risk to the supply of energy to critical facilities. As an alternative, we would suggest a public private partnership to accelerate the private sectors efforts in the area of supply chain security whereby the Federal Government would strengthen current regulations and encourage transparency by suppliers so that asset owners can assess supply chain cyber risk for themselves through existing solutions. Funding would also accelerate these efforts.

1. **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?**

As stated above, a true “Prohibition Order” may be an overreach due to the probable impact on operations due to the loss of availability of product because it falls into the prohibited category and is not available from other non-prohibited sources. However, if a “Prohibition Order” is deemed to be necessary, consideration should be given to all critical assets and not just those that are associated with the public sector. As also stated above, an alternative we would suggest is a public private partnership to accelerate the private sectors efforts in the area of supply chain security.

1. **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?**

See responses to questions 1 and 2 above.

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

Depending on the definition of “Critical Infrastructure”, AEP believes that many if not all utilities should be able to identify critical infrastructure within their service territories, consistent with their existing obligations as utilities.

AEP appreciates the opportunity to provide feedback and information regarding this request and hopes to stay actively involved in the process as it moves forward. We offer ourselves as informed participants in the energy utility supply chain process to you as consultants, assistants or in any capacity in which we may be of service.

Respectfully submitted,

*/s/ Jeffrey J. Sweet*

Jeffrey J. Sweet

Director, Security Assessments

American Electric Power

1 Riverside Plaza

Columbus, Ohio 43215

Telephone: 614-716-3059

Email: jjsweet@aep.com