Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure

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?

The first priority should be to realize what the DOD has claimed in a press release for unlimited general release as the top need for electric system security, namely the establishment of electromagnetic and cyber resilient microgrids and distributed energy resources that can operate in island mode while the bulk power system becomes unavailable "permanently or for weeks, or months".[1] DOD has determined that the collapse of centralized systems is currently inevitable because of the lack of their electromagnetic protection. (It could be argued that large sprawling centralized infrastructure with relatively few targets required for destruction is nearly impossible to defend against a determined foe compared to highly distributed infrastructure.) DOE in studies such as the 2020 NREL Roadmap for Grid-Forming Inverters now declare that unavoidable and more frequent accidental electromagnetic accidents by the bulk power system on itself and their customers are inevitable due to the bulk power system to integrate intermittent energy sources and distributed energy resources (https://www.nrel.gov/docs/fy21osti/73476.pdf, p. 36, Sec.3.4). Each of these natural and manmade intentional and unintentional electromagnetic interference threats as in their cyber and physical counterparts requires that states, Indian Tribes and local units of government take the responsibility to create or acquire their own electric systems such as the electromagnetic resilient microgrids as recommended by DOD for enough of their electric power requirements so that they can operate indefinitely. Their connections with the bulk power system should be tested to be demonstrated as safe including their use as grid-forming assets to the electric user community as a whole. States, Indian Tribes, local units of government cannot avoid the responsibility to provide electric power themselves even if their utilities fail to do so. They should consider themselves as holding the primary responsibility to do so though they outsource that responsibility to others such as the electric power utilities. In the same way, they should not outsource their security and lifeline infrastructure to foreign entities either incapable of protecting them or who may have moral hazards inclining them to purposely hurt them.

States, Indian Tribes and local units of government can take advantage of SBIR Phase 3 commercialization capabilities that already exist to expeditiously deploy the solutions already available to them such as the completed DTRA contract HDTRA-1-16-P-0025.

---

[1] See: "An electromagnetic (EM) attack (nuclear electromagnetic pulse [EMP] or non-nuclear EMP [e.g., high- power microwave, HPM]) has the potential to degrade or shut down portions of the electric power grid important to the DoD.... Restoring the commercial grid from the still functioning regions may not be possible or could take weeks or months."
https://www.instantaccessnetworks.com/files/131807223.pdf.

2. What specific additional actions could be taken *by regulators to address the security of critical electric infrastructure* and the incorporation of criteria for evaluating *foreign ownership, control, and influence into supply chain risk management*, and how can the Department of Energy best inform those actions?

Security-- Regulators should require utilities to make their bulk power systems resilient to electromagnetic and cyber threats and provide distributed energy resources and microgrids that can serve their customers in island-mode either directly or indirectly through their unregulated affiliated companies. Utilities should also incentivize their customers to establish their own similarly resilient microgrids, or, at least not penalize them for doing so. Those island-mode capable systems should also be effectively grid connected and serve as grid-forming technologies as a way to make it possible for the customer-based systems to become self-funding. These systems should be resilience-tested for both reliability and resilience to pertinent electromagnetic and cyber MIL-STDs with plans to remediate problems shown by independent testing organizations.

Foreign control -- Chips with software and controls from adversarial countries should be banned. The exception might be for chip substrate material onto which other layers with software and controls can be placed in US factories from US sources. The US should consider countering incentives for US companies to have moved offshore to move them back again. It is understandable that this is complicated since US companies were provided financial incentives (since at least the 1980's) including costs to establish factories, minimal environmental protection requirements, low overseas wages and, on occasion, subsidized foreign currencies.

3. What actions can the Department take to facilitate responsible and *effective procurement practices by the private sector*? What are the potential costs and benefits of those actions?

There are several items in procurement which would significantly impact how the private sector can influence the societal and economic impact of any procurement. Costs associated with the use of human and material capital that is directed to train or retrain underserved communities to directly benefit from the procurement. A second consideration is mentioned in the approach to self-funding for underserved communities to participate in energy markets served by the system whether in island mode or when connected to the grid. This would have the effect of acting like an economic multiplier for the communities hosting the distributed generation.

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

In order to develop a long-term strategy for supply chain risk management, priorities in acquiring and installing U.S.-manufactured BPS electric equipment and level of risks of non-U.S. manufactured equipment should be identified. This will allow to accordingly develop and adapt prohibition policy and regulation for electrical equipment supply chain based on level of risks and priorities. Identifying priorities and risk levels requires conducting vulnerability analysis at different levels of power systems to determine the most vulnerable equipment, assess the impact of compromised equipment on security of the U.S. critical electric infrastructure, and prioritizing and classifying them for different level of restrictions. Department of energy as the Sector Risk Management Agency should inform utility industry, and appropriate regulators at all levels of government, including state Public Utility Commissions, and the Federal Energy Regulatory Commission (FERC) about priorities and risk levels. This will help them adjust

their procurement practices and requirements to match the evolving threats and best protect critical electric infrastructure. DOE can best exercise this role by utilizing advanced technologies such as digital twin for electricity grid in order to provide technical assistance and guidance for vulnerability assessment at system level and equipment level.

To close the loop here, the long-term strategy should include a plan for mitigating the risks associated with potentially compromised grid equipment that is already installed on the system. The current power grid structure is vulnerable to compromised grid equipment, as any failure can easily propagate to the entire system. DOE along with its effort on modernizing and enhancing the nation's power grid and infrastructure through reliable supply chain, may want to explore new and transformational cyber-physical power system architecture capable of arresting and isolating the effects of compromised grid equipment locally.