

Foundation for Resilient Societies
24 Front Street, Suite 203
Exeter NH 03833
855-688-2430

June 7, 2021

Michael Coe, Director
Energy Resilience Division of the Office of Electricity
U.S. Department of Energy
Mailstop OE-20, Room 8H-033
1000 Independence Avenue SW, Washington, DC 20585

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

Dear Director Coe:

We appreciate the opportunity to submit comments on this Request for Information (RFI). Security of the U.S. critical electric infrastructure is one of the most important issues for our country. Your RFI had specific queries. We will answer each in turn.

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

While the federal government has technical resources at the National Laboratories, few States, Indian Tribes, and local governments have equivalent capability to research security threats to the electric system. (Some states have research universities that do this type of work.) Accordingly, if the resources of the National Laboratories were to be made available through an organized supply chain certification program for electric system equipment, this could produce efficiencies and economies for governments at the state level. Certifications could be delegated to an independent government recognized certification authority instead of the National Laboratories.

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?

Again, if regulators were to require a supply chain equipment certification program for electric system equipment that is foreign-manufactured (or contains foreign components susceptible to compromise), this would reduce supply chain risks.

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?

Private sector contracts for electric system equipment should contain standard clauses requiring that equipment susceptible to supply chain compromise be certified by a National Laboratory or other government-recognized certification authority.

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?

Examples of electric system equipment that could be compromised include long-lead time items such as large power transformers, high-voltage circuit breakers, and generators. Other examples include equipment vulnerable to cyberattack such as firewalls, switches, routers, and fiber optic transceivers. Even seemingly mundane equipment such as Uninterruptible Power Supplies (UPS) and Heating Ventilation and Air Conditioning Systems (HVAC) can be compromised and cause failure of other electric system equipment. Particular criteria for equipment that could have supply chain compromises should be developed by the National Laboratories. Certification of equipment should be a precondition to installation in an operating electric grid.

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?

Yes. There is no bright line between distribution facilities and transmission facilities. A simultaneous attack on many distribution facilities can destabilize an electric grid and cause outages of similar magnitude as an attack on transmission facilities. Certifications should apply to equipment in microgrids that can interconnect to large-scale electric grids.

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. Compromise of electric grids serving interdependent infrastructures—especially communications, water/wastewater, and transportation systems—can exacerbate electric grid outages.

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. Within the Continental United States, all critical infrastructure and national critical functions ultimately rely on commercial electric grids.

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

No. Many smaller utilities lack the research capabilities to independently determine which equipment may have supply chain compromises.

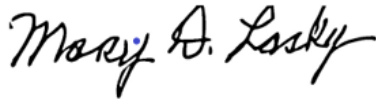
In addition to the above answers to your questions, we would like to stress the importance of ensuring that the U.S. electric power grid is hardened for cyber and electromagnetic security.

Again, thank you for the opportunity to comment on this RFI. We stand ready to provide further information if requested.

Sincerely,

Handwritten signature of Thomas S. Popik in black ink.

Thomas S. Popik, President

Handwritten signature of Mary A. Lasky in black ink.

Mary Lasky, Secretary/Treasurer