wiley

ALERT

U.S. Department of Energy Seeks Comments on Securing Electric Infrastructure from Attacks from Foreign Adversaries

April 27, 2021

On April 22, 2021, the U.S. Department of Energy (DOE) called for public comments on policies that the Administration should pursue to secure the U.S. electric grid from exploitation and attack by foreign adversaries. The DOE is seeking policy recommendations to assess threats and develop solutions, including whether to expand its authority to block certain utilities from obtaining electric equipment from adversary nations, such as the People's Republic of China (PRC) and the Russian Federation. As part of its efforts, the DOE is considering requesting blocking authority to cover the electric distribution system and utilities that service critical infrastructure, including defense, communications, energy services, healthcare and public health, information technology, and transportation systems. Comments are due to the DOE by **June 7, 2021**.

The DOE concurrently announced a 100-day plan to address cybersecurity risks in the U.S. electric system, in coordination with the Cybersecurity and Infrastructure Security Agency (CISA), while at the same time suspending a 2020 prohibition order barring a limited number of utilities from obtaining certain electric equipment from the PRC. The initiative seeks to "provide cyber visibility, detection, and response capabilities for industrial control systems of electric utilities."

The request for comments is particularly timely given emerging and developing threats from high-threat actors' access to critical data systems in the United States, as was seen with the Russian SolarWinds attack, as well as the U.S. electric grid. Every critical sector in the United States relies on electricity, and such vulnerabilities have the ability to severely compromise all energy and

Authors

Hon. Nazak Nikakhtar
Partner
202.719.3380
nnikakhtar@wiley.law

Practice Areas

Corporate
Environment & Product Regulation
International Trade
National Security
Telecom, Media & Technology

communication infrastructure nationwide, with crippling consequences for U.S. defense capabilities as well.

Given the importance of the electrical grid, it should come as no surprise that the U.S. government has found that energy companies are the number one target for cyberattacks against critical infrastructure. The Director of National Intelligence's 2021 Annual Threat Assessment noted that the PRC can launch cyberattacks that are capable of, at least temporarily, disrupting critical infrastructure in the United States. Russia also possesses the capabilities to disrupt electric infrastructure, as evidenced by its attack that shut down the Ukrainian electric grid in December 2015.

Beyond cyberthreats, insecure bulk-power equipment poses additional risks for data theft and manipulation, remote access backdoors, and massive surveillance. Chinese transformers make up approximately 10% of all high-voltage transformers in the United States, which makes the elements of the country's energy grid particularly vulnerable.

Much like the Federal Communication Commission's (FCC) efforts to replace unsecure Chinese telecommunications equipment, the DOE's request contemplates providing the government with legal authority to block acquisitions of electric equipment from unreliable sources.

Background

In May 2020, then-President Trump issued an executive order (EO) aimed at securing the U.S. bulk-power system. The 2020 EO authorized the DOE to prohibit the acquisition, transfer, or installation of certain electric equipment that serve "critical defense facilities" sourced from foreign adversary countries. Under this authority, on January 6, 2021, the DOE subsequently issued a prohibition order barring a limited number of utilities from obtaining certain electric equipment from the PRC.

Subsequently on January 20, 2021, President Biden issued a new EO, *Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis*, which suspended the 2020 order and related prohibition order for 90-days while directing the DOE and the Office of Management and Budget (OMB) to develop recommendations for a replacement order. On April 20, 2021 the DOE fully revoked the December 2020 prohibition order.

Request for Comments

Under the Biden Administration's new initiative, the DOE is currently seeking input from electric utilities, academia, research laboratories, government agencies, and other electric infrastructure stakeholders to inform its recommendations on how a replacement executive order can balance national security, economic security, and administrability considerations. Moreover, the DOE is considering expanding its authority to block certain transactions beyond those that service "critical defense facilities" as stipulated in the prior 2020 EO.

Accordingly, it seeks comments on whether the President should authorize the DOE to prohibit certain equipment:

- In parts of the electric distribution system, *i.e.* distribution equipment and facilities;
- That serve other types of critical infrastructure such as communications, emergency services, healthcare and public health, information technology, and transportation systems; and
- That cover electric infrastructure enabling national critical functions.

The DOE also seeks comments on whether utilities are sufficiently able to identify critical infrastructure within their service territories that would enable compliance with such requirements.

Additionally, the DOE is seeking comments to inform its long-term strategy regarding:

- How the Federal Energy Regulatory Commission (FERC) can ensure its procurement practices evolve to match emerging threats;
- How to enable better testing of critical grid equipment, encourage better procurement and risk management practices, and develop a strong manufacturing base; and
- How to mitigate risks associated with potentially compromised grid equipment that is already installed on the system and the costs and benefits to addressing such risks.

Finally, the U.S. government is seeking input on the types of technical assistance states, localities, and tribes require to secure their electric systems; the types of actions regulators could take to address the security of critical infrastructure and the criteria for evaluating foreign ownership, control, and influence within the supply chain; and whether there are particular criteria the DOE could use to inform utility procurement policies, state requirements, or FERC mandatory reliability standards.

A Larger Effort to Secure Critical Infrastructure

The DOE's request is part of a larger U.S. government initiative to address critical infrastructure security. In particular, President Biden issued a separate order in February that requires a comprehensive government examination of domestic production, research and development capabilities, and strategies to strengthen key sectors. The February EO directs the DOE to identify and make recommendations to address risks in the supply chain for high-capacity batteries and, also, within a year to review and make recommendations to improve supply chains for the energy sector industrial base.

Wiley has a robust Supply Chain practice, as well as unparalleled experience and expertise in International Trade, National Security, Government Contracts, Environment & Product Regulation, Telecom, Media & Technology, and Trade Analytics, and can help clients navigate evolving supply chain developments. Wiley's multidisciplinary team has been helping companies with shifting export controls, entity listings, various DOC information and communications technology and services (ICTS) supply chain regulations, the Federal Acquisition Security Council, FCC supply chain activities, and procurement restrictions such as Section 889 and new NDAA restrictions.

Nicole Hager, a Law Clerk at Wiley Rein LLP, contributed to this alert.