Milbank

Project, Energy & Infrastructure Finance Group and Global Risk & National Security Practice

Client Alert

Cybersecurity, Protecting the Grid & Digital Infrastructure: Executive Order to Counter Threats to U.S. Bulk-Power System

May 4, 2020

Contact

Allan T. Marks, Partner
+1 424.386.4376
atmarks@milbank.com

Dara A. Panahy, Partner
+1 202.835.7521
dpanahy@milbank.com

Sean Heiden, Associate
+1 202.835.7536
sheiden@milbank.com

The Bulk-Power System Executive Order

On May 1, 2020, President Donald Trump signed an Executive Order[1] (the "**Executive Order**") addressing national security threats facing the U.S. bulk-power system,[2] in particular by restricting use of certain imported equipment essential to the power grid. The Executive Order seeks to protect the grid against malicious acts conducted by foreign adversaries that seek to exploit weaknesses in the bulk-power system.

This recent action by the Trump Administration closely tracks its May 15, 2019 executive order,[3] which was designed to protect the nation's information and communications technology and services supply chain. As with the 2019 executive order, this recent action may rely on U.S. government concerns about the cyber activities of Russia and China, as well as Iran and North Korea. Of those countries, only China is a major source of imported equipment used in U.S. power generation and transmission facilities. In the 2019 order on digital infrastructure, the Department of Commerce was responsible for promulgating rules and regulations implementing the order.[4] For the new power sector order, the Department of Energy is delegated the responsibility of implementing the Executive Order in consultation with other federal agencies.

Specifically, the Executive Order prohibits persons subject to U.S. jurisdiction from acquiring, importing, transferring or installing any bulk-power system electric equipment[5] that the Secretary of Energy (the

---

[1] https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/.
[2] The term "bulk-power system" means (i) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (ii) electric energy from generation facilities needed to maintain transmission reliability. Colloquially, the bulk-power system is also referred to as the power grid or the bulk electric system.
[3] https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.
[4] The Department of Commerce did not provide additional guidance on the meaning of "foreign adversary" in its draft implementing regulations published in December 2019.
[5] The term "bulk-power system electric equipment" means items used in bulk-power system substations, control rooms, or power generating stations, including reactors, capacitors, substation transformers, current coupling capacitors, large generators, backup generators, substation voltage regulators, shunt capacitor equipment, automatic circuit reclosers, instrument transformers, coupling capacity voltage transformers, protective relaying, metering

"**Secretary**"), in consultation with the Director of the Office of Management and Budget, the Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, and, where appropriate, the heads of other executive departments and agencies, has determined:

> (i) involves bulk-power system electric equipment designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and
>
> (ii) poses (A) an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of the bulk-power system in the United States; (B) an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the economy of the United States; or (C) an unacceptable risk to the national security of the United States or the security and safety of U.S. persons.

The Executive Order empowers the Secretary to halt pending or future transactions but provides that certain otherwise prohibited transactions may be allowed if effective, Secretary-approved mitigation measures can be negotiated and implemented to minimize the risks to U.S. national security. In addition, the Executive Order allows the Secretary to establish and publish criteria for recognizing specific equipment and vendors in the bulk-power system electric equipment market as pre-qualified for future transactions. The Secretary may then use these criteria to publish a list of pre-qualified equipment and vendors.

The Secretary is required under the Executive Order to publish, within 150 days of the date of the Executive Order, implementing regulations in consultation with other Cabinet Secretaries and the heads of Executive Branch agencies. Such implementing regulations are expected to include identifications, processes or clarifications with respect to:

- Countries or persons that are "foreign adversaries";
- Entities owned by, controlled by or subject to the jurisdiction or direction of "foreign adversaries";
- Procedures to license transactions otherwise prohibited pursuant to the Executive Order; and
- Criteria for the categorical inclusion or exclusion of certain technologies or market participants from the prohibitions of the Executive Order.

Finally, the Executive Order directs the Secretary to, as soon as practicable, identify the bulk-power system electric equipment targeted by the Executive Order and to develop recommendations on ways to identify, isolate, monitor, or replace such items as soon as practicable. For purposes of the Executive Order, the bulk-power system expressly does not include facilities used in the local distribution of electric energy. Thus, distributed generation (like equipment used in residential solar installations) should be outside the scope of the Executive Order.

FERC Delays Implementation of Grid Cybersecurity Reliability Standards

Cybersecurity risks to the nation's bulk-power system have long been a concern. The Energy Policy Act of 2005 gave the Federal Energy Regulatory Commission ("**FERC**") authority to oversee the reliability of the bulk power system, including approval of mandatory cybersecurity Reliability Standards. FERC is statutorily required, under the Federal Power Act, to review and approve mandatory Reliability Standards, which are enforceable in the United States by the North American Electric Reliability Corporation ("**NERC**"), subject to FERC oversight, or by FERC acting independently. NERC is the official Electric Reliability Organization for North America, under the oversight of FERC and Canadian regulatory authorities. NERC has developed Critical Infrastructure Protection ("**CIP**") cybersecurity Reliability

---

equipment, high voltage circuit breakers, generation turbines, industrial control systems, distributed control systems, and safety instrumented systems.

Standards that already are binding on grid operators, utilities, transmission companies, and utility-scale independent power generators. On January 18, 2008, the Commission issued Order No. 706, the Final Rule approving the CIP Reliability Standards, and modifications and updates continue to be made to the requirements.

FERC's assessments and the CIP rules specifically address the concern that, as the electric industry is incorporating information technology systems into increasingly "smart" grid operations to improve reliability and efficiency, the electric grid could become more vulnerable to attacks and loss of service. To address this concern, the Energy Independence and Security Act of 2007 gave FERC and the National Institute of Standards and Technology responsibilities related to coordinating the development and adoption of smart grid guidelines and standards.

In January 2020, FERC approved additional Reliability Standards and issued its NERC 2019 Five-Year Performance Assessment (RR19-7-000), stating "the Commission recognized the NERC continues to demonstrate its ability to develop and enforce Reliability Standards and continues to satisfy the criteria for certification as the ERO that is responsible for developing and enforcing the Commission's mandatory reliability standards."[6]

Of note, a few weeks before the new Executive Order, FERC issued an order granting NERC a deferral of implementation of several FERC-approved Reliability Standards focused on, among other things, grid cybersecurity.[7] Specifically, on April 17, 2020, FERC delayed implementation of Reliability Standard CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)), CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments), and CIP-013-1 (Cyber Security – Supply Chain Risk Management) for three months. FERC also delayed implementation of Reliability Standards PRC-002-2 (Disturbance Monitoring and Reporting Requirements), PRC-025-2 (Generator Relay Loadability), PRC 027-1 (Coordination of Protection Systems for Performance During Faults), and PER-006-1 (Specific Training for Personnel) for six months. In its motion to FERC, NERC stated that the delay was necessary due to the impacts of the COVID-19 pandemic on registered entities' supply chains and staff availability.

In the Reliability Order, FERC noted its previous joint statement with NERC announcing the two entities "would use regulatory discretion when considering the impact of the COVID-19 pandemic on registered entities' ability to comply with Reliability Standards." Accordingly, FERC found that delaying implementation of the subject Reliability Standards is a "reasonable and proportionate" response to the impacts of the COVID-19 pandemic on registered entities. Relying on NERC's representation that delay of the standards would not adversely impact the reliability of the bulk-power system, FERC reasoned that it must balance the role of the standards with the immediate challenges presented by the COVID-19 pandemic. The delayed implementation means that certain of the Reliability Standards will become effective October 1, 2020 (CIP-005-6, CIP-010-3, and CIP-013-1) and others will become effective January 1, 2021 (PRC-002-2 and PRC-025-2) and April 1, 2021 (PRC-027-1 and PER-006-1).

The Executive Order does not address or alter FERC's statutory role in setting and enforcing reliability and efficiency criteria for the power grid to deal with potential cybersecurity threats to the bulk-power system.

Implications of the Executive Order on the U.S. Bulk-Power System

Taken together, the Executive Order on the bulk power system and the 2019 digital infrastructure Executive Order appear to target equipment from certain to-be-determined foreign manufacturers that is incorporated into the backbone of the nation's electricity, telecommunications and information technology networks. The scope and impact of the latest Executive Order on the development, construction, design, planning, modernization and transfer of large power generation facilities, utilities, and the transmission system should become clearer once the Department of Energy begins its rulemaking process. Until then, investment decisions and procurement may face regulatory uncertainty. Key to the implementation of the new regulations to protect the reliability and security of the bulk power system from cyber-threats will be

[6] https://www.ferc.gov/media/news-releases/2020/2020-1/01-23-20-E-20.asp#.XrA3PKhKg2w
[7] 171 FERC ¶ 61,052 (2020) (the "**Reliability Order**").

the complex interplay of jurisdiction between the Department of Energy, FERC, other federal agencies, and Congress, along with state utility regulators and independent transmission system operators. The Executive Order is significant not just as a piece of the puzzle in protecting the power grid from cyber-risks (as already being addressed by FERC and NERC's CIP requirements), but as part of the larger challenge of balancing national security, technology improvements, and trade policy as they impact the reliability and efficiency of the nation's power supply.

*****

This Client Alert provides a summary of certain key elements of the Executive Order and is not comprehensive as to the full scope of the Executive Order or any implementing regulations, or other elements of the legal framework, that may relate to or follow from the Executive Order.

Los Angeles	2029 Century Park East, 33rd Floor, Los Angeles, CA 90067	
Allan T. Marks	atmarks@milbank.com	+1 424.386.4376
Washington, DC	1850 K Street, NW, Suite 1100, Washington, DC 20006	
Dara A. Panahy	dpanahy@milbank.com	+1 202.835.7521
Nicholas A. Smith	nsmith@milbank.com	+1 202.835.7522

Project, Energy & Infrastructure Finance Group and Global Risk & National Security Practice

Please feel free to discuss any aspects of this Client Alert with your regular Milbank contacts or any member of our Global Risk & National Security Practice or Project, Energy & Infrastructure Finance Group.