wiley

ALERT

Trump Administration Mandates National Security Reviews of Bulk-Energy Supply Chain

May 12, 2020

As part of a continuing effort to harden U.S. critical infrastructure against nefarious cyber activity, on May 1, 2020, President Trump signed an executive order directing the Secretary of Energy (Secretary) to restrict transactions involving the acquisition of U.S. bulk-power system electric equipment from a "foreign adversary." The order provides a new layer of scrutiny and federal regulation around critical energy infrastructure to address national security risks by establishing a legal framework for limiting the foreign supply of bulk-power system electric equipment and directing the Secretary to issue implementing regulations within 150 days of the date of the order, *i.e.*, by September 28, 2020.

Similar...

In many respects, the order is similar to the President's May 15, 2019 executive order restricting transactions involving information and communications technology and services (ICT Supply Chain EO). Like the ICT Supply Chain EO, this order emerges from the United States Government's interest in maintaining an open investment environment while acknowledging that unrestricted acquisition or use of certain equipment, technology or services creates an "unusual and extraordinary threat" to U.S. national security, foreign policy, and the economy. Both ICT Supply Chain and Bulk-Energy Supply Chain orders invoke the President's authority under the International Emergency Economic Powers Act (IEEPA) and the National Emergencies Act, and declare national emergencies to address the specific threats.

The new order broadly prohibits any acquisition, importation, transfer, or installation of any "bulk-power system electric equipment" where the transaction involves any property in which any foreign country or

Authors

Nova J. Daly
Senior Public Policy Advisor
202.719.3282
ndaly@wiley.law

Practice Areas

International Trade
National Security

national has any interest, if the Secretary determines that:

1. The transaction 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
2. The transaction:
    1. poses 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;
    2. poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the economy of the United States; or
    3. otherwise poses an unacceptable risk to the national security of the United States or the security and safety of U.S. persons.

The order broadly defines "bulk-power system electric equipment" to include "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 equipment, high voltage circuit breakers, generation turbines, industrial control systems, distributed control systems, and safety instrumented systems. Items not included in the preceding list and that have a broader application of use beyond the bulk-power system are outside the scope of this order."

Further, the order authorizes the Secretary to issue licenses to permit specific transactions and provides the Secretary with discretion to design or negotiate mitigation measures to address any concerns "as a precondition to the approval . . . of a transaction or of a class of transactions" that would otherwise be prohibited. The ICT Supply Chain EO provides identical authorizations to the Secretary of Commerce.

... But Not the Same

The bulk-power system order differs from the ICT Supply Chain EO in a few important ways. The new order directs the Secretary to identify electronic equipment in the U.S. bulk-power system that is linked to a foreign adversary and poses an undue risk, and to "develop recommendations on ways to identify, isolate, monitor, or replace such items as soon as practicable, taking into consideration overall risk to the bulk-power system."

In addition, the order establishes a Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security, which will coordinate government-wide national security efforts with respect to energy-infrastructure procurement, risk information sharing, and risk management practices. The Task Force is charged with developing a set of energy infrastructure procurement policies and procedures for federal agencies, which it will submit to the Federal Acquisition Regulatory Council (FAR Council). The FAR Council, in turn, will consider implementing the recommendations by amending the Federal Acquisition Regulation

through a notice and comment proceeding.

Further, the order directs the Task Force to "evaluate the methods and criteria used to incorporate national security considerations into energy security and cybersecurity policymaking." The order also highlights the importance of distribution systems to the bulk-power system and directs the Task Force to engage with distribution system industry groups "[b]ecause attacks on the bulk-power system can originate through the distribution system."

The Department of Energy is now responsible for the next steps, including developing and implementing regulations for bulk-power system electric equipment procurement and standing up the procurement policy Task Force.

Wiley's National Security and International Trade practices have represented clients before Team Telecom and CFIUS for decades. We have worked with Congress, the FCC, and other agencies on legal and policy issues affecting investors and companies across the private sector. Should you have any questions, please contact one of the attorneys listed on this alert.