Trump Administration Limits Acquisitions and Use of Bulk-Power System Electric Equipment From Foreign Adversaries

Skadden

05 / 07 / 20

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

440 New York Avenue, N.W.
Washington, D.C. 20005
202.371.7000

On Friday, May 1, 2020, the Trump administration issued an executive order prohibiting the acquisition and installation of "bulk-power system electric equipment" (such as generators, circuit breakers, metering equipment, generation turbines and industrial control systems) supplied by foreign adversaries and persons subject to their control and establishing the creation of a task force to monitor threats to the U.S. power system from foreign adversaries. This executive order — which is almost identical to the Trump administration's May 15, 2019, executive order that similarly limited the acquisition and use of certain information and communications technology (the ICT executive order) — requires the secretary of energy to conduct rulemaking within the next 150 days to implement the president's direction and could ultimately have a major impact on the power industry's ability to use China-sourced equipment. Under its broadest reading, the executive order would allow the Department of Energy to prohibit transactions involving bulk-power system electric equipment manufactured or supplied by persons "subject to the jurisdiction of" a foreign adversary if such use "poses an unacceptable risk" to U.S. national security.

Overview of the Executive Order

President Trump's executive order[1] finds a threat to U.S. national security and national emergency arising from the acquisition, importation, transfer or installation of bulk-power system electric equipment supplied by foreign adversaries.[2] To address this concern, the president has authorized the prohibition of any acquisition, importation, transfer or installation of any bulk-power system electric equipment by any person (any of which is a "transaction") if:

- 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
- the transaction:
  - 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;
  - 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
  - otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

We note that like its prior relative (the ICT executive order), the new executive order's geographic limitation on the source of the bulk-power system electric equipment does not apply only to companies formed or organized in the adversarial nation or operating within the adversarial nation. Rather, in the case of a country like China — which is surely the principal focus of the executive order — bulk-power system electric equipment produced by a Chinese company both inside *and* outside China *as well as* bulk-power system electric equipment produced by non-Chinese companies — such as U.S. or Western European companies with facilities in China — who manufacture bulk-power system electric equipment in China would all be subject to the executive order. This breadth

[1] Like his May 15, 2019, executive order as well as other similar actions, the May 1, 2020, executive order rests on the president's constitutional authorities, as well as the International Emergency Economic Powers Act (IEEPA) and the National Emergencies Act (NEA).

[2] Executive Order on Securing the United States Bulk-Power System (May 1, 2020).

might seem surprising, but it lines up with broader U.S. concerns regarding supply chain security, especially for technology developed or manufactured in China or by Chinese companies.

The Department of Energy, in consultation with the Departments of Defense and Homeland Security as well as the Office of the Director of National Intelligence (and other agencies, as appropriate), is responsible for implementing the executive order, including issuing regulations within 150 days (by September 28, 2020). The executive order expressly identifies the following areas as topics for likely regulatory implementation:

- Identification of particular countries or persons to be considered foreign adversaries for the purposes of the executive order;
- Identification of persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary for the purposes of the executive order;
- Identification of particular equipment or countries warranting particular scrutiny under the provisions of the executive order;
- Establishment of procedures to license transactions otherwise prohibited pursuant to the executive order; and
- Identification of a mechanism and relevant factors for the negotiation of agreements to mitigate concerns relating to U.S. acquisition and use of bulk-power system electric equipment provided by foreign adversaries.

Separate from implementing regulations, the Department of Energy is also authorized to establish lists and publish criteria for recognizing particular equipment and particular vendors in the bulk-power system electric equipment market as prequalified for future transactions; however, it is unclear when, how, or if this authority will be exercised.

While the Department of Energy's implementing regulations are likely to provide greater specificity, the executive order includes the following definitions:

- **Bulk-Power System.** Facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof) as well as the electric energy from generation facilities needed to maintain transmission reliability. The executive order specifies that it includes transmission lines rated at 69,000 volts (69 kV) or more, but does not include facilities used in the local distribution of electric energy.
- **Bulk-Power System Electric Equipment.** 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. The executive order specifies that items not included in the preceding list and that have broader application by use beyond the bulk-power system are outside the scope of the executive order.
- **Foreign Adversary.** Any foreign government or foreign nongovernment person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or its allies or the security and safety of United States persons.

We note that the definition of the bulk-power system expressly excludes the distribution system, while including all transmission lines rated at 69 kV or more. While 69 kV has been the presumptive dividing line under controlling precedent between what is considered transmission and what is considered distribution equipment, in certain circumstances electric transmission lines above 69 kV have been found to be part of the distribution system. Additional clarity on this aspect of the definition will be required.

With respect to the last definition — that of a foreign adversary — China *will* be included, and this designation will almost surely have a disproportionate impact as compared to other potentially listed adversaries such as Iran, North Korea or even Russia. In addition, as noted above, the executive order will apply not only to entities controlled by those states or operations taking place within those states, but also to any entities subject to their jurisdiction. This could capture a broad range of companies originating from nonforeign adversary states whose activities, such as manufacturing, occur within a foreign adversary's territory, and thus are subject to its jurisdiction.

Potential Retroactivity Issues

Prohibitions under the executive order apply to any qualifying transaction initiated after May 1, 2020. This contrasts with the ICT executive order, which applied to transactions that were initiated *before* issuance of that order, but were pending or to be completed after its issuance. But the new executive order nonetheless does create uncertainty for transactions initiated between now and the issuance of implementing regulations, including transactions that were in progress as of May 1, 2020. Potentially affected transactions during this window of time could include entering into new contracts to acquire bulk-power system electric equipment, importing already contracted-for bulk-power system electric equipment or installing previously imported bulk-power system electric equipment. It is unclear from the text of the

Trump Administration Limits Acquisitions and Use of Bulk-Power System Electric Equipment From Foreign Adversaries

executive order whether a single contract that provides for the acquisition, importation, transfer and installation of bulk-power system electric equipment potentially constitutes four separate transactions or a single transaction. This is important, among other reasons, for purposes of determining whether a transaction has been "initiated" after May 1, 2020 (*e.g.*, the equipment has been acquired under contract before May 1 but not imported or installed until after May 1). However, consistent with the approach taken in the ICT executive order, it does not appear that direct or indirect transfers of ownership of generation and transmission projects are qualifying transactions subject to any restrictions under the executive order.

The executive order also requires the Department of Energy to develop recommendations to identify, isolate, monitor or replace such items that are already in use (because they were installed prior to May 1, 2020) as soon as practicable. It is not clear what the effect of these recommendations will be, given that this provision — unlike the provisions that explicitly permit cessation or mitigation of transactions — does not provide for any authority other than "develop[ing] recommendations."[3]

Penalties

Preexisting Department of Energy civil penalty authority does not encompass enforcement of the executive order's prohibitions. However, the executive order was issued pursuant to the IEEPA, which itself contains penalties for violating, attempting to violate or conspiring to violate "any license, order, regulation, or prohibition" issued under the IEEPA.[4] Any person who commits an unlawful act under the IEEPA may be subject to a civil penalty of $250,000 or twice the amount of the underlying transaction, whichever is greater.[5] Any person who willfully commits an unlawful act may be subject to criminal penalties of up to $1 million and 20 years imprisonment.[6]

Although these statutory penalty provisions exist now, in other executive orders the administration has made clear that civil administrative penalties should not be imposed without transparency, fair warning and safeguards that go "above and beyond" those found in the Due Process Clause of the Constitution.[7]

Regulations implementing the executive order should provide greater transparency as to what transactions are prohibited and may also include more specific enforcement provisions. For example, the proposed regulations implementing the similar ICT executive order reference Section 1705 of the IEEPA and provide for civil penalties in accordance with those set out in the IEEPA (adjusted upward for inflation), but make no reference to criminal sanctions. Notably, those proposed regulations also provide that transactions completed on or after the date of the ICT executive order and found to be prohibited under the regulations may be subject to mitigation or unwinding.

General Motivating Concerns

The executive order closely tracks broad administration trade and national security concerns regarding China, as well as more specific concerns regarding energy infrastructure security.

China-Related Trade and National Security Concerns

The increasing focus on inbound transactions in the ICT and energy sectors mirrors the more aggressive actions the United States has taken with respect to preventing countries of concern, most notably China, from obtaining U.S.-origin technology. For example, in May 2019, the Bureau of Industry and Security within the U.S. Department of Commerce added Huawei Technologies Co. Ltd., the Chinese telecommunications giant, to the Entity List, which essentially means that any item that is subject to the Export Administration Regulations requires a license, regardless whether a license ordinarily would be required to export the item to China (and applications are subject to a licensing policy presumptive denial). The Commerce Department subsequently added a number of other prominent Chinese technology companies to the Entity List.

The Commerce Department also is engaged in an interagency process to identify specific "emerging technologies" that will be subjected to more stringent export controls with respect to China in accordance with the Export Control Reform Act of 2018 and is expected to publish an advance notice of proposed rulemaking regarding "foundational technologies" that would have the same effect.

Furthermore, the Commerce Department has been considering fundamental changes to the de minimis and foreign direct product rules that would ensnare a greater number of items manufactured or developed outside the United States, including a change that would inhibit the ability of non-U.S. foundries that use U.S.-origin semiconductor manufacturing equipment to supply chips to Huawei.

[3] Interestingly, the language used in the executive order is stronger than that used in the ICT executive order, which merely instructed the secretary of homeland security to "assess and identify entities, hardware, software, and services that present vulnerabilities," and to prepare a report on such vulnerabilities annually.

[4] 50 U.S.C. § 1705(a).

[5] *Id.* § 1705(b).

[6] *Id.* § 1705(c).

[7] *See* Executive Order Promoting the Rule of Law Through Transparency and Fairness in Civil Administrative Enforcement and Adjudication (Oct. 9, 2019); Executive Order on Promoting the Rule of Law Through Improved Agency Guidance Documents (Oct. 9, 2019).

Trump Administration Limits Acquisitions and Use of Bulk-Power System Electric Equipment From Foreign Adversaries

Finally, just last week, the Commerce Department published two final rules[8] and one proposed rule[9] that have the potential to severely curtail export activities with respect to China, among others. These increasingly hawkish steps are being taken to counteract the significant integration of civilian and military technology development in countries of concern, most notably China (the so-called "civil-military fusion" strategy), and may presage additional controls aimed primarily at China. Indeed, according to a statement issued by the secretary of commerce, these rules are intended to thwart the acquisition of U.S. technology through civilian supply chains, or under civilian-use pretenses, that could be used in the development of weapons, military aircraft or surveillance technology for military end uses and users.

Energy Infrastructure Security Concerns

The executive order to protect U.S. energy infrastructure follows years of warnings from the Departments of Homeland Security and Energy about the potentially disastrous impacts successful attacks on the power grid could have on the country and the increasing nation-state cybersecurity threats facing U.S. energy infrastructure. For example, in 2018, the Department of Energy established the Office of Cybersecurity, Energy Security and Emergency Response specifically to prepare for and respond to cybersecurity threats to energy infrastructure and issued the "Multiyear Plan for Energy Security Cybersecurity," which noted dramatic increases in the nation-state-level targeting of U.S. energy infrastructure.[10] The president's National Infrastructure Advisory Council followed with its 2018 report, "Surviving a Catastrophic Power Outage: How To Strengthen the Capabilities of the Nation," which discussed the profound risk a catastrophic power outage would pose to national and economic security and highlighted the role cybersecurity and physical attacks by sophisticated actors could play in such an outage.[11] The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency has also issued numerous alerts about potential cybersecurity attacks on the energy infrastructure sector generally as well as specific aspects of the infrastructure, such as industrial control systems. Further, in June 2019 the Federal Energy Regulatory Commission issued an order directing the North American Electric Reliability Corporation to bolster the cybersecurity of the bulk-power system through expanded reporting requirements for incidents involving attempts to compromise bulk-power system operation.[12] In addition, the Committee on Foreign Investment in the United States (CFIUS), discussed further below, now includes the bulk-power system under its definition of covered critical infrastructure.

Regulatory Analogues

CFIUS. The executive order's mechanisms look — quite roughly — like the national security review process of CFIUS, which evaluates the national security risks arising from foreign investments in U.S. businesses. Like the CFIUS process, the executive order calls for a multiagency review of the national security implications of certain types of cross-border transactions. Secretary of energy-led reviews under the executive order will result in transactions being blocked, permitted or permitted subject to risk-mitigation conditions. It is not, however, yet clear whether the DOE process would comprise a CFIUS-like case-by-case review of transactions, or whether it would more closely resemble categorical prohibitions with limited exceptions more akin to export control licensing. The executive order's provision for a preapproved "white list" of bulk-power system electric equipment and vendors seems to indicate that the approach may be more categorical and less of a case-by-base review than is contemplated in the ICT executive order and the Commerce Department's implementing regulations.

The Commerce Department and ICT. Given the similarities of the two executive orders, the Commerce Department's implementation of the ICT executive order provides some insight into the considerations and challenges that the Department of Energy will have to address in implementing the new executive order. Despite the mandate to issue rulemaking within 150 days, on November 27, 2019, the Commerce Department belatedly published a proposed rule to implement the May 2019 ICT executive order that would establish a new and especially broad power for the U.S. government to review and potentially block or unwind transactions involving foreign ICT.[13] Specifically, the proposed rule would give the Commerce Department (in consultation with several other departments and agencies) discretion to review a broad array of "transactions" on a case-by-case basis, including any "acquisition, importation, transfer, installation, dealing in, or use of any [ICT]" that: (i) involves any person or property subject to U.S. jurisdiction; (ii) involves property, technology or a service in which any foreign country or foreign person has an interest; and (iii) is initiated, pending or will be completed after May 15, 2019.

[8] Expansion of Export, Reexport, and Transfer (in-Country) Controls for Military End Users in the People's Republic of China, Russia, or Venezuela, 85 Fed. Reg. 23,459 (Apr. 28, 2020); Elimination of License Exception Civil End Users (CIV), 85 Fed. Reg. 23,470 (Apr. 28, 2020).

[9] Modification of License Exception Additional Permissive Reexports (APR), 85 Fed. Reg. 23,496 (Apr. 28, 2020).

[10] U.S. Dep't of Energy, Office of Elec. Delivery & Energy Reliability, Multiyear Plan for Energy Sector Cybersecurity (Mar. 2018).

[11] Nat'l Infrastructure Advisory Council, Surviving a Catastrophic Power Outage: How To Strengthen the Capabilities of the Nation (Dec. 2018).

[12] *N. Am. Elec. Reliability Corp.*, 167 FERC ¶ 61,230 (2019).

[13] Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65,316 (proposed Nov. 27, 2019).

Trump Administration Limits Acquisitions and Use of Bulk-Power System Electric Equipment From Foreign Adversaries

Any such review will consider whether the transaction:

- poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation or maintenance of information and communications technology or services in the United States;
- poses an undue risk of catastrophic effects on the security or resiliency of U.S. critical infrastructure or the U.S. digital economy; or
- otherwise poses an unacceptable risk to U.S. national security or to the security and safety of U.S. persons.

As written, however, the proposed rule creates significant uncertainty as to its scope and potential impacts, which were highlighted in the comments received by the Commerce Department. No timetable has been established for issuance of a final rule, but the significant delay since the December 27, 2019, deadline for comments suggests that the department is grappling with the complexities associated with the establishment of an entirely new regulatory regime. Whether the Department of Energy follows the case-by-case approach the Commerce Department followed in the ICT executive order rulemaking or a more categorical approach (akin to its export control regulations) will be a factor in whether similar uncertainty will arise under analogous rulemaking to occur under the new executive order on bulk-power system electric equipment.

Conclusion

Given the widespread use of Chinese equipment in electric industry infrastructure, Friday's executive order will add a material layer of new regulatory oversight of many transactions. The details of the approval procedures obviously are not yet known, but it seems relatively certain that those procedures will force many industry participants to seek alternative equipment choices and the executive order could complicate transactions, particularly during the interim period before regulations are issued. If any party seeks judicial review of the regulations that eventually will be adopted, they will face a challenging road. But the Department of Energy presumably will seek to learn from the Department of Commerce's more advanced and quite similar exercise. Industry feedback, beginning at this early stage, could prove useful to help the regulatory scheme that ultimately results from the executive order meet its goal of protecting national security while avoiding unnecessary commercial disruption.

Contacts

Energy and Infrastructure Projects

Lance T. Brasher
Partner / Washington, D.C.
202.371.7402
lance.brasher@skadden.com

Julia A. Czarniak
Partner / New York
212.735.4194
julia.czarniak@skadden.com

Tatiana Monastyrskaya
Partner / New York
212.735.3582
tatiana.monastyrskaya@skadden.com

Energy Regulation and Litigation

John N. Estes III
Partner / Washington, D.C.
202.371.7950
john.estes@skadden.com

Robert W. Warnement
Counsel / Washington, D.C.
202.371.7507
robert.warnement@skadden.com

Raunaq (Niqui) Kohli
Associate / New York
212.735.2449
niqui.kohli@skadden.com

National Security

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

Daniel J. Gerkin
Counsel / Washington, D.C.
202.371.7194
daniel.gerkin@skadden.com

Nathan L. Mitchell
Associate / Washington, D.C.
202.371.7193
nathan.mitchell@skadden.com