Client Alert | International Trade

US Targets Telecommunications Transactions Involving the Information and Communications Technology and Services Supply Chain

May 2019

Authors: **Richard Burke**, **Farhad Jalinous**, **Karalyn Mildorf**, **Keith Schomig**, **Stacia J. Sowerby**, **Cristina Brayton-Lewis**, **Sandra Jorgensen**, **Margaret Spicer**

On May 15, 2019, President Trump issued an executive order (EO), "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," prohibiting certain transactions involving telecommunications equipment or services made or supplied by persons that have been determined by the US Government to be "foreign adversaries"[1] and the transactions are deemed to pose an "unacceptable national security risk".[2] The actual restrictions will apply only after the US Secretary of Commerce determines that particular transactions meet the EO's criteria. The EO does not name specific countries or parties.

1 "Foreign adversaries" is defined in the EO as any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of US persons. The EO does not identify any specific foreign governments or non-government persons as "foreign adversaries."

2 White House, Executive Order, Executive Order on Securing the Information and Communications Technology and Services Supply Chain, *available* here.

Executive Order

Prohibition

The EO prohibits the acquisition, importation, transfer, installation,[3] dealing in, or use of any "information and communications technology or service,"[4] by any person,[5] or with respect to any property, subject to US jurisdiction, involving any property in which any foreign country or national thereof has an interest (including an interest in a contract for the provision of the technology/services) where the transaction is determined by the US Secretary of Commerce to meet the following criteria:

- The transaction involves information and communications technology or services 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 is determined to:
    - Pose an undue risk of sabotage or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communication technology or services in the United States;
    - Pose an undue risk of catastrophic effects on the security or resiliency of US critical infrastructure or the digital economy of the United States; or
    - Otherwise pose an unacceptable risk to the national security of the United States or the security/safety of US persons.

This EO applies to transactions initiated, pending, or to be completed after the date of the EO (May 15, 2019).

Additional Actions

To implement the prohibitions of the EO, the Secretary of Commerce will need to

(1) Determine that particular countries or persons are foreign adversaries; and

(2) Identify persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries.

The prohibitions cannot take effect in practice until the Secretary of Commerce makes these determinations and identifications. The Secretary of Commerce may also establish criteria by which particular technologies or market participants may be categorically included or excluded from the prohibitions.

The Secretary of Commerce may also establish procedures to license transactions otherwise prohibited pursuant to the EO. The EO requires publication of rules and regulations to implement the EO within 150 days from May 15.

US Government Concerns

This is the latest step in US government actions concerning alleged cyber security and economic/industrial espionage. Such allegations came to broad public attention with the interagency enforcement actions against one

[3] Notably, the term "installation" is not used in the International Emergency Economic Powers Act (IEEPA), the statutory authority for the EO.

[4] "Information and communications technology or services" is defined in the EO as any hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including transmission, storage, and display.

[5] "Persons" is defined under the EO as an individual or entity. "Entity" is defined under the EO as a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

of China's largest telecommunications companies first announced in 2016, and with more recent actions such as the Department of Justice's indictment of two Chinese hackers for alleged global computer intrusion campaigns targeting IP and confidential business information of businesses and governments from around the world[6] and the FCC's denial of international Section 214 authority to a Chinese company for the provision of international telecommunications services between the United States and foreign destinations.

This EO also supplements recent changes to the Committee on Foreign Investment in the United States (CFIUS) under the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA). Largely in reaction to particular Chinese investment trends, FIRRMA expanded CFIUS's authority to review additional types of investments by foreign persons into US businesses involved with certain sensitive technology, infrastructure, and data.[7]

While this EO does not specifically name any countries or persons, a number of bills have been introduced in Congress addressing sanctions and export controls restrictions specifically on Chinese information and communication technology companies. At this time, none of these bills has passed through the committee stage, but attention to them would be prudent, as they could pave the way for new sanctions and export/import restrictions on the affected entities and companies that do business with them.

In a related development, on May 16, 2019, the Commerce Department issued a draft notice adding Huawei to the Bureau of Industry and Security (BIS) Entity List. BIS also designated sixty-eight non-US affiliates of Huawei located in twenty-six countries, including Brazil, Canada, China, Hong Kong, Switzerland, Taiwan, the United Kingdom, and Vietnam. All items subject to US export control jurisdiction[8] require a license for export, reexport, and/or transfer to Entity List parties. License applications are subject to a policy of denial. BIS has indicated that these restrictions are effective May 16, 2019.

Conclusion

Companies engaging in business involving information and communications technology or services should monitor the implementation and any determinations under this EO very closely. Persons operating within US jurisdictions should ensure compliance with any forthcoming restrictions under the EO. We will be monitoring how these various provisions are implemented in practice, including any regulations or determinations issued pursuant to this EO.

White & Case LLP
701 Thirteenth Street, NW
Washington, District of Columbia 20005-3807
United States

T +1 202 626 3600

6 For a description of the Department of Justice's action, see here.

7 For a summary of these reforms, see here and here.

8 BIS is the agency responsible for administering export controls on dual-use items that are subject to the Export Administration Regulations (EAR). This includes most goods, software and technology originating from the United States, as well as some items made outside the United States that incorporate specified levels of US-origin content.