wiley

ALERT

President Moves to Restrict Foreign Telecom Deals Under Sweeping Order on Network Supply Chain Security; Congress Poised to Follow

May 16, 2019

The United States government this week is taking major actions affecting the tech and telecom sector. President Trump yesterday signed a long-anticipated executive order directing the Secretary of Commerce to restrict transactions involving information and communications technology and services from a "foreign adversary." The order targets China and Chinese companies Huawei and ZTE. At the same time, the U.S. Department of Commerce's (Commerce) Bureau of Industry and Security (BIS) announced that it will be adding Huawei to its Entity List, as early as this Friday, which will effectively ban nearly all U.S.-origin exports to the Chinese telecommunications giant without a license. Meanwhile, Congress has been looking at 5G security and is considering new legislation. Amidst all this, tariff and other discussions demonstrate the confluence of geopolitical and security considerations about China and the tech sector. Interested parties should consider how these developments and future rules will affect their operations.

A Long-Awaited Executive Order Materializes under IEEPA

The executive order invokes the President's authority under the National Emergencies Act and the International Emergency Economic Powers Act (IEEPA). It declares a national emergency to combat the threat of "malicious cyber-enabled actions" and "economic and industrial espionage." The President is targeting Chinese companies and affiliates that the Administration considers a threat. This is a new area of regulation, separate from existing government review of

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

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

John R. Shane
Partner
202.719.7222
jshane@wiley.law

Lori E. Scheetz
Partner
202.719.7419
lscheetz@wiley.law

Daniel P. Brooks
Partner
202.719.4183
dbrooks@wiley.law

Boyd Garriott
Associate
202.719.4487
bgarriott@wiley.law

Practice Areas

International Trade
National Security
Privacy, Cyber & Data Governance
Telecom, Media & Technology

transactions by the Committee on Foreign Investment in the United States, and there is uncertainty about how the order will affect business until the agency makes rules as directed.

What does the order do? The order broadly prohibits any acquisition, importation, transfer, installation, dealing in, or use of any "information and communications technology or service" where Commerce finds that "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

(A) 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;
(B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or
(C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

The term "information and communications technology or services" is not limited to 5G technology and services but is defined broadly to include "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." The order authorizes Commerce to issue licenses to authorize specific transactions and provides Commerce 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.

There will be agency rules. The order directs Commerce to publish implementing regulations within 150 days of the date of the order, *i.e.*, by October 12, 2019. Such regulations may:

- Determine that particular countries or persons are foreign adversaries;
- Identify persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries;
- Identify particular technologies or countries with respect to which transactions involving information and communications technology or services warrant particular scrutiny;
- Establish procedures to license transactions otherwise prohibited pursuant to the order;
- Establish criteria by which particular technologies or particular participants in the market for information and communications technology or services may be recognized as categorically included in or as categorically excluded from the prohibitions of the order; and
- Identify a mechanism and relevant factors for the negotiation of agreements to mitigate concerns raised in connection with a particular transaction.

Future implementing regulations are likely to include details on penalties. IEEPA, the underlying statutory authority for the executive order, provides for civil penalties of up to the greater of $250,000 or twice the amount of the transaction that is the basis for the violation and provides for criminal penalties of up to $1,000,000 and/or 20 years' imprisonment.

The executive order also directs agencies to produce periodic assessments and reports about threats to the ICT sector, and hardware, software, and services used by critical infrastructure. Federal agencies may need and seek assistance from the private sector with these assessments.

Huawei and Affiliates are Targets for Restriction by BIS

Commerce simultaneously announced that it will impose significant, far-reaching export restrictions on Huawei and its affiliates by adding these companies to its Entity List. Specific export restrictions have not been published and are not yet in effect, but they could effectively ban nearly all U.S.-origin exports to Huawei without a specific license, including common, off-the-shelf electronic components, commercial software, and technology.

If past experience is a guide, the restrictions could have considerable ramifications on Huawei's supply chain as well as the provision of software updates and repair services for Huawei handsets and equipment. Commerce took similar action against ZTE, China's second largest telecommunications equipment manufacturer, back in 2016, a move that sent shockwaves throughout the global telecommunications industry. Wiley Rein is monitoring these developments closely and will provide additional information as it becomes available.

Congress is Considering Legislation to Address 5G Security

These announcements come on the heels of Congressional hearings and new legislation aimed at telecom and Internet supply chain security. The Senate took steps this week to address U.S. telecom supply chain concerns, reflecting ongoing apprehension about Chinese manufacturers.

The Senate Judiciary Committee this week held a hearing on 5G security, at which witnesses from the Department of Homeland Security (DHS) and the State Department, as well as outside experts testified about 5G security, including China. Senators focused on supply chains and security issues and talked about new legislation to address China.

Some legislative efforts reflect broad bipartisan support for addressing Chinese supply chain threats. The China Technology Transfer Control Act of 2019, introduced by Senator Josh Hawley (R-MO), would formally admonish China for "theft of intellectual property" and "manipulation of lawful transfer and uses of technology in ways that directly support its military objectives and threaten the United States." The bill would place "core technologies" (including technologies from the robotics, semiconductors, and transportation industries) from China's "Made in China 2025" initiative on the Department of Commerce's Export Control List (the "List"). To export a technology from the List to China, companies would have to first obtain a license. The

bill would also impose sanctions on foreign entities that violate the new export controls.

The Sharing Urgent, Potentially Problematic Locations that Yield Communications Hazards in the American Internet Networks Act of 2019 ("SUPPLY CHAIN Act")—introduced by Senators Marsha Blackburn (R-TN) and John Cornyn (R-TX)—takes a more high-level approach. Rather than dictating specifics, the SUPPLY CHAIN Act would direct the Commerce Department to work with other federal agencies to (1) "conduct an ongoing review of risks to the communications equipment and services marketplace and the supply chain thereof"; and (2) "develop and issue procedures to regularly facilitate long-term scenario and strategic planning with private entities."

Senator Richard Blumenthal (D-CT) this week was quoted as saying that there "seems to be pretty strong bipartisan alarm about the threat posed by Huawei, which is really the threat posed by China," with Senator Lindsey Graham (R-SC) echoing the sentiment, noting that he has not "seen bipartisanship like this in a long time." However, Senator Diane Feinstein (D-CA) cautioned that she did not think the Senate was "near legislation" just yet.

Take-Aways

In sum, this busy week confirms that the tech and communications sectors face increasing scrutiny and regulation around supply chains as a national security risk. This is no surprise after provisions were included in last year's National Defense Authorization Act to address supply chain security and multiple actions against Huawei and ZTE.

There will be ample opportunities to engage policymakers on these issues, including their impacts and unintended consequences.