WINSTON & STRAWN LLP

CLIENT ALERT

Developments in Telecom Supply Chain Security Controls

MAY 17, 2019

- BIS Announces Huawei Will Be Added to Entity List

- Executive Order Authorizes Commerce Department to Prohibit Information and Telecom Technology and Services Transactions that Pose a Threat to National Security

On May 16, 2019, the Bureau of Industry and Security (BIS) of the U.S. Commerce Department announced it was adding *Huawei Technologies Co. Ltd.* (Huawei) and its affiliates to the Bureau Entity List. A preview of the Entity List notification to be published in the Federal Register also was available May 16 and identified Huawei and its Chinese address along with 68 of its affiliates in 26 jurisdictions as included on the List. As a result, any business potentially exporting a good, technology, or related services should review its supply to chain to address potential exposure to Huawei and its affiliates. This supply chain transparency and ability to nimbly adjust compliance programs reflects OFAC's recent Framework for a Compliance Program.

On May 15, 2019, President Trump signed Executive Order (E.O.) – "Securing the Information and Communications Technology and Services Supply Chain." The E.O. is designed to protect the United States from threats that have arisen in the information and communications technology supply chain by prohibiting transactions with entities that are owned, controlled, or subject to a jurisdiction deemed a foreign adversary to the United States.

Both actions represent significant tightening by the United States of national security-related controls on the telecommunications supply chain.

Huawei Added to Entity List

A preview of the Federal Register Notice shows the addition of Huawei and its China location to the Entity List along with 68 affiliates in 26 non-U.S. locations. In advance of the publication of the final rule, U.S. persons engaged in transactions involving Huawei, its affiliates, and other Chinese telecommunications companies should implement enhanced due diligence and confirm the end-use and end-user for goods, services, and related technology. U.S. entities with exposure to Huawei and other Chinese telecommunications businesses also should review contracts and other obligations to determine whether each has the appropriate termination provisions in the event that a party

to the contract is added to the Entity List or is subject to other sanctions or export controls restrictions – or should be amended to address the potential export denial.

While Huawei and ZTE have been in the news for years, the recent action may be tied to the U.S.–China trade negotiations. Depending on whether and how those progress, we could see BIS including additional entities to the Entity List – or other agencies including the Office of Foreign Asset Controls could utilize similar foreign policy tools.

BIS Entity List Implication

BIS maintains multiple Lists of Parties of Concern, each list classifying persons and entities subject to different levels of concern regarding BIS interests, including national security and foreign policy concerns. Companies or persons that would do business with entities included on any of the Lists of Parties of Concern are required to perform additional due diligence on the listed entity before proceeding with a transaction.

The Entity List, upon which Huawei and its affiliates will be included, "identifies persons reasonably believed to be involved, or to pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States." Exporters must secure a license from BIS before exporting any item subject to the Export Administration Regulations (EAR). Items subject to the EAR include software, hardware, products with a significant percentage of U.S.-origin products, as well as certain items that are produced outside of the U.S. but are the "direct product" of U.S. technology or software.

The sale or transfer of U.S. technology to an entity identified on the Entity List also requires a license from BIS, and may be denied at the discretion of BIS. BIS considers U.S. national security interests and foreign policy interests in making its licensing determination—subjective factors that may vary significantly depending on the exported product and the familiarity of BIS with the purchasing entity or end user. The recent high-profile arrest of the Huawei CFO in China, pending extradition to the U.S., and suspected retaliatory detainment of Canadian citizens in China indicate that BIS will be closely scrutinizing any organization dealing with Huawei, directly or indirectly. The further formal charging of the Canadian detainees in the hours following the issuance of the BIS addition of Huawei to the Entity List suggests the public profile of this incident will not subside and that BIS will be particularly focused on Huawei for the foreseeable future.

U.S. entities should perform enhanced due diligence both on their direct dealings with Huawei and the dealings of any affiliated entities that may deal with Huawei. BIS prohibitions are not limited to direct interactions, and require companies to identify the ultimate end user of any exported products. Entities may look to the BIS Red Flag Indicators and Know Your Customer (KYC) Guidance for concerning behavior that may indicate a company is dealing with a sanctioned entity. Willful ignorance of a customer's malfeasance and dealing with sanctioned entities will not offer protection from BIS penalties.

Executive Order on Securing the Information and Communications Technology and Services Supply Chain

In the May 15 E.O., President Trump declared that threats to the information and communications technology and services supply chain by foreign adversaries are a national emergency. The E.O. does not impose immediate restrictions but rather establishes the beginning of a new regulatory framework to address these concerns. The E.O. prohibits certain transactions that meet both requirements below:

Any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (transaction) by any person, or with respect to any property, subject to the jurisdiction of the United States, *where the transaction involves any property in which any foreign country or a national thereof has any interest* (including through an interest in a contract for the provision of the technology or service);

And

Where the Secretary of Commerce (in consultation with other key agencies and departments) determines that:

- The transaction involves information and communications technology or services by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and
- Pose any of the following risks:

  (A) 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) 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) an unacceptable risk to the national security of the United States or the security and safety of United States persons.

The key developments to watch following issuance of this E.O. are the procedures developed by the Commerce Department (in consultation with other agencies and departments) to make these critical determinations. The E.O. directs the Secretary of Commerce, within 150 days, to issue implementing regulations that may, but need not, include:

- determining that particular countries or persons are foreign adversaries for the purposes of this order;
- identifying persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries for the purposes of this order;
- identifying particular technologies or countries with respect to which transactions involving information and communications technology or services warrant particular scrutiny under the provisions of this order;
- establishing procedures to license transactions otherwise prohibited pursuant to this order;
- establishing 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 established by this order; and
- identifying a mechanism and relevant factors for the negotiation of agreements to mitigate concerns raised in connection with the E.O.

We anticipate that these regulations will give critical guidance to the business community regarding what specific technology, third parties, and transactions are subject to these new restrictions. In addition, we anticipate that a multi-agency review panel of some form will take on a role in reviewing certain information and telecom transactions. Such a review panel could have some overlap with the current roles played by Team Telecom and the Committee on Foreign Investment in the United States (CFIUS).

This E.O. follows a number of steps taken by the U.S. Government to address concerns with the security of the federal government's information and telecommunications supply chain. This includes a ban on the U.S. Government purchase of products produced by Huawei or ZTE, enacted August 13, 2018, as well as a ban on purchases from Kaspersky Labs, enacted September 13, 2017. This also follows the passage in December 2018 of the Secure Technology Act, which established a Federal Acquisition Security Council and provided executive agencies with the authority to mitigate supply chain risks in the procurement of information technology. With the issuance of this E.O., the U.S. Government is rapidly expanding its focus beyond its own supply chain into the commercial sector as well.

Companies operating in the information and telecommunications space should take careful note of both developments and continue to monitor the roll-out of these new restrictions on information and telecommunications equipment. If you have any questions about these actions, please contact one of the Winston contacts listed below.

7 Min Read

Related Locations

Charlotte | Chicago | Dallas | Houston | Los Angeles | New York | San Francisco | Silicon Valley | Washington, DC

Related Topics

International Trade | Global Privacy & Data Security Task Force | BIS

Related Capabilities

Government Investigations, Enforcement & Compliance | Privacy & Data Security | International Trade

Related Regions

North America

Related Professionals

David Houck

Cari Stinebower