Published on *The National Law Review* https://natlawreview.com

Latest U.S. Trade Restrictions Target Huawei

Article By:

Kara M. Bombach

Cyril T. Brennan

Renee A. Latour

Sonali Dohale

Melissa P. Prusock

During the week of May 13, 2019, the Trump administration announced two new measures that have the potential to cut off certain foreign companies, particularly Chinese technology company Huawei Technologies Co., Ltd. (Huawei), from the U.S. technology and telecommunications market. These provisions follow legislation passed in 2018 prohibiting U.S. government agencies and contractors from using Huawei products and reflect a heightened concern regarding the national security risks associated with non-U.S. entities' involvement in the U.S. technology and telecommunications sectors.

Entity List Designations

On May 16, 2019, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) filed a Federal Register notice adding Huawei, along with 68 of Huawei's non-U.S. affiliates, to its Entity List. The Entity List identifies companies that BIS reasonably believes to be involved in "activities contrary to the national security or foreign policy interests of the United States."

The inclusion of Huawei and its affiliates on the Entity List has the effect of cutting Huawei off from its U.S. supply chain, and even has the potential to restrict non-U.S. companies' ability to supply Huawei. Businesses worldwide will be prohibited from exporting or re-exporting any goods, technology, or software subject to the U.S. Export Administration Regulations (EAR) to Huawei or any of its 68 affiliates named to the Entity List. All commodities, including goods, technology, and software, manufactured in the United States or exported from the United States are subject to the EAR for the life of the commodity, and even commodities manufactured outside the United States are subject to the EAR if they contain more than a *de minimis* amount of controlled U.S. content or are the product of U.S. technology.

To comply with the requirements of the new Entity List designations, U.S. and non-U.S. companies alike should analyze their supply chains and distribution networks to determine whether any goods, technology, or software they supply directly or indirectly to Huawei or its affiliates are subject to the EAR. If so, companies may be required to halt some or all sales to Huawei and/or its affiliates. Companies in Huawei's supply chain will likely require particularly complex analysis to determine whether the non-U.S. origin goods they supply directly or indirectly to Huawei are subject to the EAR due to their U.S. content.

Temporary General License

BIS has issued a 90-day Temporary General License (TGL) permitting companies to continue supplying Huawei and its listed affiliates with commodities subject to the EAR. The TGL period will allow some affected companies to spend time evaluating their supply chains and implementing new export control policies as needed. Under the TGL, through Aug. 19, 2019, only the following categories of activities continue to be permissible:

1. Transactions "necessary to maintain and support existing and currently fully operational networks and equipment" that were "subject to legally binding contracts or agreements" with Huawei or its affiliates executed on or before May 16, 2019;

2. Transactions "necessary to provide service and support" to existing Huawei handsets that were publicly available on or before May 16, 2019;

3. Disclosure to Huawei or its affiliates of any information regarding security vulnerabilities in Huawei items, when related to "ongoing security research";

4. Engagement with Huawei, "as necessary for the development of 5G standards as part of a duly recognized international standards body," including, for example, the Institute of Electrical and Electronics Engineers or the Internet Engineering Task Force, among others.

?The TGL's limited scope means not all transactions with Huawei involving EAR-controlled commodities will be covered. Parties that wish to continue supplying EAR-controlled commodities to Huawei on a temporary basis should carefully analyze each transaction with Huawei to confirm whether it remains authorized under the TGL. In addition, use of the TGL is subject to certain recordkeeping and certification requirements.

Executive Order

On May 15, 2019, President Donald Trump issued an Executive Order on Securing the Information and Communications Technology and Services Supply Chain. The new Executive Order (E.O.) establishes the legal authority to prohibit certain transactions involving "information and communications technology or services" where a foreign party acquires an interest in property subject to U.S. jurisdiction. While the E.O. does not mention any specific country or company, recent events strongly suggest that Chinese companies generally, and Huawei specifically, may be targets of the new E.O.

Under the E.O., the U.S. government may prohibit U.S. persons from dealing in information and communications technology or services from companies "designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign

adversary." If exercised, these prohibitions could ban targeted companies from doing business in the United States or with U.S. persons.

Existing Restrictions on the U.S. Government and Contractors

This E.O. and Entity List designation add to the restrictions imposed by two pieces of legislation from last year that prohibited the use of technology from Huawei and other Chinese companies in U.S. government contracts and were aimed at reducing espionage threats.

Under Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 (Aug. 13, 2018) (FY 2019 NDAA), U.S. agencies are prohibited from procuring or obtaining, or entering into, extending, or renewing a contract with any entity that uses "any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system." "Covered" telecommunications equipment and services includes telecommunications equipment and services produced or provided by Huawei Technologies Company and other Chinese companies (or any subsidiary or affiliate of such entities) or any other entity that the Secretary of Defense believes is owned, controlled, or connected to the Chinese government. *Id.* The ban will be effective August 2019 for U.S.-government agencies and August 2020 for contractors. The Federal Acquisition Regulation (FAR) Council opened a FAR case (No. 2019-009) to implement FY 2019 NDAA sec. 889, but no implementing regulations have been issued. Although Huawei has filed a lawsuit challenging FY 2019 NDAA § 889, it faces an uphill court battle given the Court of Appeals for the D.C. Circuit's recent precedent in *Kaspersky Lab, Inc. v. United States Dep't of Homeland Sec.*, 909 F.3d 446, 450 (D.C. Cir. 2018).

In addition to expressly banning Huawei products and services, the U.S. government has enacted other measures to exclude Chinese and Russian telecommunications and information technology from the federal supply chain. The Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) permits the government to exclude companies that provide information or communications technology or related services from participating in government contracting at any level of the supply chain (prime contractor, subcontractor, or otherwise) if it believes the company's presence in the supply chain creates a risk of hacking, surveillance, or other cybersecurity risks. *See* Title II of the Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure Technology (SECURE Technology) Act, Pub. L. No. 115-390 (Dec. 21, 2018). The exclusion can be either agency-specific, or government-wide, pursuant to a recommendation by the newly established Federal Acquisition Supply Chain Security Council. The legislative history makes clear that FASCSA is intended to address the threat of cyberattacks and espionage by Russia and China.

FASCSA states that it is effective 90 days after its enactment (i.e., March 21, 2019), and that it applies to "contracts that are awarded before, on, or after that date." However, implementing regulations are required for both government-wide and agency-specific exclusions. An interim final rule on government-wide exclusions (which will be made available for public comment) is due Dec. 21, 2019. The Federal Acquisition Supply Chain Security Council, which will develop government-wide exclusion criteria, held its first meeting May 1, 2019, but the meeting was largely focused on establishing the council's charter and developing a strategic plan. There is no specific deadline for regulations implementing the agency-specific exclusion authority, and no FAR cases have been opened to implement FASCSA.

Anticipated Impact

Taken together, the above measures have the potential to disrupt global supply of telecommunications products by prohibiting both the export of U.S.-origin technology products to Huawei and the import of Huawei products into the United States. While the Entity List designation is already in effect, it remains to be seen whether the U.S. government will impose broader restrictions against Huawei or other companies pursuant to the new E.O. Accordingly, companies in the technology and telecommunications space will need to watch these regulations closely over the next few months to understand exactly what kinds of restrictions may apply to their product supply chains.

The scope of the FY 2019 NDAA's ban on Huawei and other Chinese products is also somewhat unclear. The ban only applies if a Huawei or other specified product or service is used as a "substantial or essential component" or "critical technology as part of" a system. However, the statute does not define any of these terms. In light of the heightened focus on supply chain risk in general and the specific concerns about Huawei and other Chinese companies, companies that do business with the U.S. government (whether as a prime contractor, subcontractor, or otherwise) should assess their supply chains and may wish, as part of their risk-management efforts, to explore alternate sources for products, components, or services currently obtained from these companies.

National Law Review, Volume IX, Number 150