FinReg
Davis Polk Insights on Financial Regulation

# U.S. Government Takes Aim at China With Entity List Additions and New Executive Order

By John B. Reynolds, Jeanine P. McGuinness & Will Schisa on May 22, 2019

POSTED IN CFIUS, ECONOMIC SANCTIONS, EXECUTIVE ORDER

On May 21, 2019, the Department of Commerce published a **final rule** adding Huawei Technologies Co. Ltd. and 68 of its non-U.S. affiliates located in 26 countries (collectively, "**Huawei**") to the Bureau of Industry and Security's ("**BIS**") **Entity List**. Commerce had previously announced its intention to take this action in a **press release** dated May 15, 2019. In a separate but potentially related action on the same day, the President issued **Executive Order 13873**, "Securing the Information and Communications Technology and Services Supply Chain" (the "**Supply Chain E.O.**") authorizing the Commerce Department to issue regulations that will prohibit U.S. persons from acquiring 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." Although the Supply Chain E.O. does not expressly mention either Huawei or China, **media reports** identified both as likely targets once implementing regulations are developed and issued.

These actions are likely to have a significant impact. If fully implemented, the Entity List designation will effectively cut off supplies of U.S. origin components and other items subject to the Export Administration Regulations ("**EAR**") to one of the world's largest technology companies. To mitigate the impact of the designation, however, BIS has issued a **Temporary General License** that will permit some exports, reexports, and transfers to Huawei to continue for at least 90 days. The effects of the Supply Chain E.O. are less certain, and will depend on the forthcoming regulations the Commerce Department will issue within 150 days and the specific countries and entities identified as "foreign adversaries." On its face, the order's prohibitions are quite broad, but the Commerce Department is also granted broad authority to exempt or authorize categories of transactions deemed not to pose a risk to national security.

We provide below an overview of these two actions, along with an assessment of how they fit into the broader ongoing disputes between the United States and China on trade and national security issues.

**Addition of Huawei to the Entity List**

According to the Commerce Department, Huawei was added to the Entity List pursuant to Section 744.11 of the EAR based on information that provides a reasonable basis to conclude that Huawei is engaged in activities that are contrary to U.S. national security or foreign policy interests, including activities detailed in allegations by the Department of Justice in its recent **indictment** of Huawei for certain alleged sanctions violations and related obstruction of justice.

As a result of Huawei's addition to the Entity List, except as noted below, a license from BIS is required to export, reexport, or transfer (in-country) any item subject to the EAR to Huawei. BIS will apply a presumption of denial to applications for licenses involving Huawei, and no License Exceptions will be available for exports, reexports, or in-country transfers of items subject to the EAR to Huawei. Items subject to the EAR include both U.S.-origin goods, software, and technology, as well as foreign-manufactured goods, software, or technology that incorporate more than a "de minimis" amount of U.S.-origin content (generally, 25 percent by value). Accordingly, even non-U.S. parties dealing with Huawei may have compliance obligations resulting from the Entity List designation, particularly to the extent that such parties are supplying Huawei with products that are U.S. origin or incorporate U.S. content.

However, it is important to note that an Entity List designation is different, and more limited, than other targeted U.S. government actions driven by national security or foreign policy concerns, such as economic sanctions designations administered by the Treasury Department's Office of Foreign Assets Control ("**OFAC**"). The primary obligations imposed as a result of the Entity List designation of Huawei are on persons (U.S. or otherwise) exporting, reexporting, or transferring items subject to the EAR to Huawei, as well as persons engaged in certain related activities as specified in the EAR's General Prohibition 10, which provides that:

> You may not sell, transfer, export, reexport, finance, order, buy, remove, conceal, store, use, loan, dispose of, transport, forward, or otherwise service, in whole or in part, any item subject to the EAR and exported or

> to be exported with knowledge that a violation of the EAR or any order, license, License Exception, or other authorization issued thereunder has occurred, is about to occur, or is intended to occur in connection with the item.

*See* 15 C.F.R. § 736.2(b)(10). Huawei is not, however, subject to broad prohibitions on transactions or dealings by U.S. persons or involving the U.S. financial system. Additionally, the Entity List designation does not necessarily preclude U.S. persons from purchasing goods or services *from* Huawei, although BIS has noted in a **response** to Frequently Asked Questions that purchasers of items from persons listed on the Entity List should conduct due diligence to ensure that the item they purchase was not sent to Huawei in violation of the EAR. As discussed below, additional restrictions on purchasing from Huawei are potentially on the horizon as a result of the Supply Chain E.O.

Huawei's addition to the Entity List was published in the Federal Register on May 21, 2019 with a stated effective date of May 16, 2019. However, BIS has adopted two measures to ameliorate the designation's disruption of certain existing business relationships and in-process transactions. First, the rule adding Huawei to the Entity List contains a limited Savings Clause that provides that shipments of items that were en route aboard a carrier to a port of export or reexport, on May 16, 2019, pursuant to actual orders for export or reexport to a foreign destination, may proceed to that destination if they were previously eligible for a License Exception or export or reexport without a license. Second, BIS issued the Temporary General License, which was published in the Federal Register on May 22, 2019, authorizing the following types of activity from May 20, 2019, through August 19, 2019:

- Engagement in transactions necessary to maintain and support existing and currently fully operational networks and equipment, including software updates and patches, subject to legally binding contracts and agreements executed between Huawei and third parties on or before May 16, 2019;
- Engagement in transactions necessary to provide service and support, including software updates or patches, to existing Huawei handsets that were available to the public on or before May 16, 2019;
- The disclosure to Huawei of information regarding security vulnerabilities in items owned, possessed, or controlled by Huawei when related to the process of providing ongoing security research critical to maintaining the integrity and

reliability of existing and currently fully operational networks and equipment, as well as handsets; and

- Engagement with Huawei as necessary for the development of 5G standards as part of a duly recognized international standards body.

The authorizations contained in the Temporary General License are all subject to other provisions in the EAR, meaning that they do not override other licensing requirements in the EAR that are not tied to Huawei's Entity List designation, such as destination-based licensing requirements. Exporters, reexporters, and transferors of items subject to the EAR that utilize the Temporary General License are required to create and retain for a period of five years a "certification statement" that specifies how the export, reexport, or transfer (in-country) meets the scope of the Temporary General License.

**Supply Chain E.O.**

The Supply Chain E.O. was issued pursuant to the International Emergency Economic Powers Act ("**IEEPA**"), the same statutory authority as underlies most U.S. economic sanctions programs. In the order, President Trump declares a national emergency based on findings that:

- Foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people;
- Unrestricted acquisition or use in the United States of 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 foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States; and
- Maintaining an open investment climate in information and communications technology, and in the United States economy more generally must be

balanced by the need to protect the United States against critical national security threats.

To address the national emergency, section 1 of the Supply Chain E.O. prohibits any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (a "**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), where:

- the transaction was initiated, is pending, or will be completed after May 15, 2019;
- the Secretary of Commerce, in consultation with the Secretary of the Treasury, the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the United States Trade Representative, the Director of National Intelligence, the Administrator of General Services, the Chairman of the Federal Communications Commission, and, as appropriate, the heads of other executive departments and agencies, has determined 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
    - poses an undue risk of sabotage or subversion 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 digital economy, or otherwise poses an unacceptable risk to U.S. national security or the security or safety of U.S. persons.

For purposes of the above prohibition, the Supply Chain E.O. defines the term "**foreign adversary**" to mean "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 United States persons," but does not specifically identify any country as a foreign adversary. Supply Chain E.O., § 3(b). The order also defines the term

"**information and communications technology or service**" 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." *Id.* § 3(c).

Section 2 of the Supply Chain E.O. requires the Secretary of Commerce, in consultation with other agencies, to issue implementing regulations within 150 days of the date of the order, or by October 12, 2019. Among other things, 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 otherwise prohibited transactions;
- Establish criteria by which particular transactions or market participants may be categorically included in or excluded from applicable prohibitions; and
- Identify a mechanism and relevant factors for the negotiation of agreements to mitigate national security concerns related to a transaction or class of transactions, which may be a precondition for authorization of such transaction or class of transactions.

Neither the Commerce Department nor the White House issued immediate guidance concerning the likely timing or content of these forthcoming regulations, although it appears likely that Commerce will not issue any regulations prior to receiving threat and vulnerability assessments from the Office of the Director of National Intelligence and the Department of Homeland Security, which section 5 of the Supply Chain E.O. requires within 40 and 80 days of the date of the order, respectively.

### Looking at the Bigger Picture

The issuance of the Supply Chain E.O. and Huawei's addition to the Entity List are in line with a recent trend of aggressive U.S. government actions with respect to China cutting across a number of trade and national security issues, including:

- The recent conclusion of trade talks between the United States. and China without reaching a resolution, and subsequent **imposition** of substantially increased U.S. tariffs on many Chinese goods pursuant to Section 301 of the Trade Act of 1974;
- The **determination** by the State Department not to renew China's Significant Reduction Exemption permitting continued importation of Iranian oil without risking secondary sanctions;
- Increased scrutiny of Chinese investments in the United States by the Committee on Foreign Investment in the United States ("**CFIUS**"), including recent **high profile** **divestiture orders**; and
- **Reports** of increased scrutiny and restrictions applied to Chinese student and business visa applications.

It is unclear whether the Huawei designation and Supply Chain E.O. are primarily intended to serve as bargaining chips in the context of this broader relationship between the United States and China, or whether they will become permanent fixtures of the national security regulatory environment in the United States. On the one hand, the current administration has not hesitated to use national security tools in furtherance of its trade objectives, as evidenced by its use of **Section 232 investigations** to justify steel and aluminum tariffs, as well as President Trump's **willingness** to use the **ZTE denial order**, briefly imposed in 2018 after ZTE breached requirements under a prior settlement with BIS, OFAC, and the Department of Justice, as a bargaining chip to secure trade concessions. At the same time, U.S. government national security concerns with respect to China generally and Huawei specifically are real and **longstanding**, and have intensified as mobile telecommunications networks are preparing to shift to **new 5G technology**, with Huawei playing a key role globally. It is unclear how these new measures might potentially affect the worldwide development of 5G, or whether they will bolster or harm U.S. government **efforts** to convince allies and partners to exclude Huawei products from their networks. Notably, while both the Entity List

designation and the Supply Chain E.O. will have some extraterritorial impact, neither provides for measures akin to secondary sanctions that could target non-U.S. persons for dealings with Huawei that do not have some jurisdictional nexus to the United States.

Given these competing policy goals, the number of interrelated issues, and this administration's willingness to mix trade and national security issues that previously had been largely handled in separate channels, it is difficult to predict how these new measures will play out in the coming months and years. As affected companies in the United States and worldwide attempt to navigate this policy uncertainty, continued close monitoring of developments will be essential.