International Trade Alert

Akin Gump
STRAUSS HAUER & FELD LLP

President Trump Declares National Emergency to Secure the Information and Communications Technology and Services Supply Chain

May 16, 2019

Key Points

- On May 15, 2019, President Trump issued a long-awaited E.O. designed to curtail the use of telecommunications items and services from certain countries and persons in U.S. networks. The E.O. does not impose immediate restrictions on persons subject to U.S. jurisdiction. Rather, it creates a new regulatory framework that the Department of Commerce (DOC) must implement within 150 days.
- Once implemented, the new regime will broadly allow the government to block any type of transaction that involves information and communications technology or services provided by a "foreign adversary" that, among other considerations, poses an "unacceptable" risk to the national security of the United States or the security and safety of United States persons.
- The E.O. does not set out which countries or entities fall within the scope of a "foreign adversary," instead leaving it to the DOC to define this and other key terms.
- Nevertheless, BIS effectively confirmed that the Order is focused on China and, in particular, Huawei Technologies Co. Ltd. ("Huawei"), the world's largest telecommunications equipment producer, by adding Huawei and a large number of specifically-named affiliates to the "Entity List," a list published by DOC's Bureau of Industry and Security (BIS). As a general matter, the Entity List imposes export restrictions and license requirements on listed persons, effectively restricting their access to U.S.-origin items and other items subject to the Export Administration Regulations (EAR). DOC has not yet issued a final rule to give effect to the designations of Huawei and its affiliates. Accordingly, it is not yet clear what the full scope of the export restrictions will be.
- The breadth of the new Order overlaps with the EAR and the separate foreign investment regime administered by the Committee on Foreign Investment in the United States (CFIUS) – this new regime will create significant compliance challenges for companies in the context of their international business operations. For this reason, companies should begin assessing the potential impact of this new regime and consider engaging with DOC as appropriate, which must publish implementing regulations by October 2019.

Contact Information

If you have any questions concerning this alert, please contact:

Shiva Aminian
Partner
saminian@akingump.com
Los Angeles
+1 310.552.6476

Mahmoud Fadlallah
Partner
mfadlallah@akingump.com
Dubai
+971 4.317.3030

Tom McCarthy
Partner
tmccarthy@akingump.com
Washington, D.C.
+1 202.887.4047

Jon Poling
Partner
jpoling@akingump.com
Washington, D.C.
+1 202.887.4029

Tatman Savio
Registered Foreign Lawyer
tatman.savio@akingump.com
Hong Kong
+852 3694.3015

Kevin Wolf
Partner
kwolf@akingump.com
Washington, D.C.
+1 202.887.4510

Executive Order

Legal Framework

On May 15, 2019, the President issued an Executive Order on Securing the Information and Communications Technology and Services Supply Chain, pursuant to the authority described in the International Emergency Economic Powers Act (IEEPA). This statute allows the President to exercise certain actions to deal with any unusual and extraordinary foreign threat to the national security, foreign policy, or economy of the United States upon the President's declaration of a national emergency with respect to that threat. In the E.O., the President declared a national emergency with respect to the ability of "foreign adversaries" to create and exploit vulnerabilities in information and communications technology and services in order to commit malicious, cyber-enabled acts.

Key Definitions

The E.O. provides a broad definition of the term "foreign adversaries," which includes foreign government or foreign nongovernment persons 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. The Order leaves it to the DOC to identify the countries and persons that fall within the scope of this broad definition. The Order does not mention China, but it is clear from yesterday's parallel action by DOC designating Huawei and certain affiliates on the Entity List that Chinese companies, beginning with Huawei, are the focus of this Order.

The term "information and communications technology or services" is defined equally broadly to mean "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, or display." The Order contemplates that the forthcoming implementing regulations will identify the list of items that warrant particular scrutiny.

Jurisdiction and Prohibitions

The prohibitions of the Order apply broadly to any person, or with respect to any property, subject to the jurisdiction of the United States. Notably, the Order does not impose blanket prohibitions on such persons with respect to their activities with "foreign adversaries." Rather, it creates a regime that is *transaction* based. Specifically, it authorizes the Secretary of Commerce, in consultation with other agencies, to prohibit any transaction (i.e., any acquisition, importation into the United States, transfer, installation, dealing in, or use of any information and communications technology or service) where the transaction involves any property in which any foreign country or foreign national has any interest, if the Secretary determines 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**

Contact Information

If you have any questions concerning this alert, please contact:

Jaelyn Edwards Judelson
Counsel
jjudelson@akingump.com
Washington, D.C.
+1 202.887.4437

Chris Chamberlain
Associate
cchamberlain@akingump.com
Washington, D.C.
+1 202.887.4308

- the transaction 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;
  - 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
  - otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

The E.O. also allows the Secretary of Commerce—at its discretion—to design or negotiate measures to mitigate national security concerns as a precondition to approval of a transaction or a class of transactions that would otherwise be prohibited.

Implementation of the New Regime

The DOC must issue implementing regulations by October 14, 2019, to define the contours and practical workings of the new regime. Among other areas, the implementing regulations will address the following key points pursuant to the E.O.

- identify the countries or persons that are considered "foreign adversaries," as well as the persons owned or controlled or subject to the direction of the designated "foreign adversaries";
- identify particular technologies or countries with respect to which transactions involving information and communications technology or services warrant particular scrutiny;
- establish a procedure to license transactions otherwise prohibited;
- 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 new prohibitions; and
- identify a mechanism and relevant factors for the negotiation of agreements to mitigate concerns raised in connection with the new prohibitions.

Finally, the E.O. calls for recurring and final reports to Congress, as well as assessments and reports conducted by the Director of National Intelligence, on the national emergency declared in the E.O.

What Does This Action Mean for Business?

The new regime imposed by the E.O. will create significant compliance challenges for companies, both in and of itself and in relation to other regimes where there is overlapping jurisdiction in terms of the potential activities covered.

Under the current export control regime, the primary jurisdictional question is whether there is an export, transfer, or reexport of an item subject to the EAR to a non-U.S. person. Under the current CFIUS regime, the key question is whether there is a foreign investment in, or acquisition of, a U.S. business. As a result of the E.O., the threshold question for the new regime is broadly whether a person subject to U.S. jurisdiction is engaged in *any* acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or services, where the

transaction involves any property in which any foreign country or foreign national has any interest.

Entity List Designation of Huawei and Affiliates

Also on May 15, 2019, in an action separate from the issuance of the E.O. but related to U.S. government concerns about national security, DOC announced that it will add Huawei and its affiliates to BIS's Entity List. In a press release, BIS indicated that it had a reasonable basis to conclude that Huawei is engaged in activities that are contrary to U.S. national security or foreign policy interest, specifically citing to alleged sanctions violations, obstruction of justice, and other activities described in the Department of Justice's public superseding indictment of Huawei. In the press release, Secretary of Commerce Wilbur Ross stated that the designations would "prevent American technology from being used by foreign owned entities in ways that potentially undermine U.S. national security or foreign policy interests."

As a general matter, an Entity List designation imposes severe restrictions on the supply of U.S. export controlled items (i.e., "items subject to the EAR") to such designated companies under the EAR. The EAR defines "items subject to the EAR" broadly as all items in, or in transit through, the United States; all U.S.-origin items wherever located; items manufactured outside of the United States incorporating more than de minimis controlled U.S.-origin content; and certain direct products of U.S.-origin technology manufactured outside of the United States. As a result of an Entity List designation, BIS ordinarily requires any person, including U.S. and non-U.S. companies, whether located inside or outside the United States, to obtain a license to export, reexport or transfer items subject to the EAR to the listed company, and imposes a presumption of denial on such license applications.

The Entity List designations of Huawei and its affiliates will become effective once published in the Federal Register. At that time, BIS will specify the full scope of the export restrictions against the companies.

Conclusion and Opportunity to Comment on Rules

As the foregoing suggests, the first hurdle for businesses will be identifying whether a particular "transaction" is subject to review under the new framework. The breadth of jurisdiction of the new regime will require businesses to then examine the business processes associated with the transactions to determine the effects and limitations of the Order and related BIS rules. Following the identification of transactions that could fall within the scope of the prohibitions, businesses will then need to determine whether the prohibitions will apply to the transaction, and if so, how to navigate the new licensing and/or mitigation processes. With BIS already understaffed, it is not clear how or when the licenses will be reviewed or approved—much less how and when pre-conditional mitigation plans will be developed and negotiated. Moreover, for certain transactions, companies will need to contend with the way in which the new regime may overlap with BIS's export control authority and CFIUS's mandate and considering whether multiple approvals may be required for particular transactions.

Given the potential impact of this new regime, companies that have any dealings with China involving information and communications technology or services should create business process flows involving such dealings to identify classes of "transactions" that would impact their business. Once companies assess the impact, they should

consider engaging the DOC during the critical five-month period leading up to the deadline for implementing regulations, as the government builds out this new regulatory regime.

akingump.com