GIBSON DUNN

May 20, 2019

CITING A NATIONAL EMERGENCY, THE TRUMP ADMINISTRATION MOVES TO SECURE U.S. INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICE INFRASTRUCTURE

In a Separate but Related Move, Trump Imposes, Then Partially Suspends, an Export Ban on Huawei

To Our Clients and Friends:

On Wednesday, May 15, 2019, the Trump Administration took two separate, but related moves toward securing the information and communications technology and services (ICT) infrastructure of the United States.[1] The first was the issuance of an executive order ("ICT EO"), declaring a national emergency with respect to the ICT supply chain. The second was the imposition by the Secretary of Commerce's Bureau of Industry and Security ("BIS") of new restrictions on the exports of technology, software, and hardware to Chinese multinational telecommunications equipment and consumer electronics manufacturer Huawei Technologies Co., Ltd. ("Huawei") and its affiliates worldwide. While the first action establishes only a general framework for implementing regulations designed to end what the EO calls "foreign adversary" involvement in ICT networks in and linked to the United States, the second action has known, immediate, and significant impacts on those doing business with Huawei and any of its 68 named affiliates in 26 countries. And while only the second move explicitly impacts a Chinese company, both moves are significant escalations in the current U.S.-China trade war.

Less than two business days after the effective date of its export ban on Huawei, the Trump Administration took an action that illustrates just how far reaching its export ban will be. BIS issued a Temporary General License, issued on May 20, 2019, to allow exports to continue that support Huawei and its listed affiliates in four categories of transactions.

ICT EO - Securing the ICT Supply Chain

The ICT EO gives the Secretary of Commerce the power to prohibit U.S. persons from acquiring, importing, transferring, installing, dealing in, or using any ICT when the transaction involves any foreign person property or interest in property, and the Secretary of Commerce determines that

(1) the ICT is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, and

(2) the transaction

> (a) poses an undue threat of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of ICT in the United States,
>
> (b) poses an undue risk of catastrophic effects on the security or resiliency of the U.S. critical infrastructure or digital economy, *or*
>
> (c) otherwise poses a risk to the national security of the United States or the security and safety of U.S. persons.

These broad criteria lay the groundwork for U.S. agencies to regulate transactions both inside and outside of the United States, especially considering the cybersecurity threats involving ICT infrastructure outside of the United States. The ICT EO defines "foreign adversary" as "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."[2]

The ICT EO diverges from past practice involving trade in two significant ways. First, rather than imposing sanctions on U.S. persons conducting business in particular countries or with particular persons, the ICT EO focuses on a wide range of transaction types, regardless of location, that could impact the ICT infrastructure of the U.S. whenever U.S. persons and foreign person property or property interests are involved. Second, and in contrast with typical U.S. sanctions executive orders, the long list of agencies referenced in the ICT EO suggests that whatever regulatory framework is developed to implement the order will involve significant interagency collaboration and cross-agency functions. The ICT EO specifically foresees the involvement of nine named agencies and offices including the Treasury, State, Defense, Justice, and Homeland Security Departments, the United States Trade Representative, the Director of National Intelligence, the General Services Administration (GSA), and the Federal Communications Commission.[3]

Many of these departments and agencies already exercise authorities that safeguard aspects of the U.S. ICT infrastructure. For example, Treasury's Committee on Foreign Investment in the United States already has authority to block controlling and certain non-controlling investments by foreign persons in the U.S. companies that supply, build, service and manage the ICT infrastructure.[4] Similarly, the GSA and DoD already have authority under the National Defense Authorization Act for FY 2019 to prohibit procurement from a list of ICT companies Congress has deemed threats to U.S. national security and from contractors that rely on them for their ICT infrastructure.[5] Notwithstanding this, the EO's language gives broad authority to the Secretary of Commerce to create an entirely new regulatory framework that could impose new import, export, use, and other transaction-based licensing requirements.

Under the ICT EO, potential prohibitions can be imposed on transactions involving "any acquisition, importation, transfer, installation, dealing in, or use of any [ICT] . . . by any person, or with respect to any property, . . . in which any foreign country or a national thereof has any interest" that is initiated, pending or will be completed as of and after May 15, 2019.[6] Given this broad remit, the new transaction-based licensing requirements may take many forms, including the blocking and forced

unwinding of ongoing transactions, bans on the import of ICT items from particular countries and persons, and controls on U.S. person involvement (including both natural and legal persons) in ICT transactions abroad that involve foreign adversary ICT and that could impact U.S. ICT infrastructure, U.S. critical technology or digital economy, or U.S. national security.

Entity List Designation

Alongside the ICT EO, the Secretary of Commerce announced a more specific action targeting Huawei and 68 non-U.S. affiliates. Specifically, the Secretary announced the decision of the End-User Review Committee ("ERC")[7], which is chaired by BIS, to add Huawei and its named affiliates to the Entity List.[8] Entities are added to the Entity List if and when the ERC deems them to pose a significant risk of involvement in activities contrary to the national security or foreign policy interests of the United States. The principal consequence of being added to the Entity List is the imposition of export licensing requirements for shipments to that foreign company.

The impact of this new end-user licensing requirement can vary depending on the more specific lines BIS draws around the items to which the licensing requirement will apply. For example, some Entity List entries only prohibit the unlicensed export of items described on the Commerce Control List or under specific Export Control Classification Numbers to those identified. In the Huawei case, however, BIS took the most extreme position. Under the terms of an official draft of the Federal Register Notice for the EL listing made public on May 16, 2019, BIS announced its plan to require a license for *all* items subject to the Export Administration Regulations (EAR), even "EAR 99" commodities, software and technology, to Huawei and that it would review license applications for all such exports with a policy presumption of denial.[9]

The ERC's cited basis for its finding that Huawei and its affiliates have been or could be involved in activities that are contrary to the national security or foreign policy interests of the U.S. is a Superseding Indictment in the U.S. District Court for the Eastern District of New York of Huawei which includes among its 13 counts two charges that Huawei knowingly and willfully conspired and caused the export, reexport, sale and supply, directly and indirectly, of goods, technology and services from the United States to Iran and the government of Iran without authorization from the Office of Foreign Assets Control (OFAC).[10] BIS also noted that Huawei's Iran-based affiliate is alleged to have conspired with others "to impair, impede, obstruct, and defeat, through deceitful and dishonest means, the lawful government operations of OFAC."[11]

The issuance of the ICT EO and Huawei's EL listing coincide with a stall in the U.S.-China trade talks, and some may view these actions as creating leverage for the conclusion of a trade agreement between the countries. Regardless, the EL listing, in particular, will have immediate and significantly disruptive effects on Huawei's supply chain. Any Huawei supplier or vendor, including several major U.S. companies, is now required to apply for BIS licenses to transfer any item subject to the EAR to Huawei and its affiliates, and many of Huawei's customers are likely to experience associated repair and support disruption in their ICT infrastructure and services.

Just how disruptive these new export licensing requirements will be became immediately clear in a subsequent action by BIS on May 20, 2019.[12] Less two full business days after the effective date of its EL listing, BIS granted a 90-day temporary license (through August 19, 2019) that partially suspends the effects of the EL listing. The general license will allow Huawei and its listed affiliated to continue receiving exports—subject to any prior applicable licensing requirements—associated with four categories of transactions. These include:

(1) exports necessary to maintain and support existing and fully operational networks and equipment, including software updates and patches, provided they are made pursuant to legally-binding contracts and agreements entered into on or before May 16, 2019;

(2) exports 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;

(3) disclosure to Huawei and the listed affiliates, of information regarding security vulnerabilities in items owned, possessed, or controlled by them 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

(4) exports incident to the engagement with Huawei and the listed affiliates necessary for the development of 5G standards by duly recognized standards bodies.

Exporters that make use of the general license to export, reexport, or transfer items to Huawei must prepare a certification statement explaining how the export, reexport, or transfer fits within the scope of the general license and maintain that certification as a record for five years.

---

[1] President Donald J. Trump, Executive Order on Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019 (available at https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/).

[2] ICT EO, § 3(b).

[3] ICT EO, § 1(a).

[4] 31 C.F.R. Parts 800 and 801.

[5] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Public Law No. 115-232, § 889 (2018).

[6] ICT EO, § 1(a).

[7] The ERC is composed of representatives from the Departments of Commerce, State, Defense, Energy, and Treasury.

[8] 15 C.F.R. § 744.16.

[9] Department of Commerce, BIS, Addition of Entities to the Entity List, May 16, 2019, (available at https://s3.amazonaws.com/public-inspection.federalregister.gov/2019-10616.pdf). Note that this is an unpublished version that is not scheduled to be published in the Federal Register until May 21, 2019.

[10] *Id*. at 3–4.

[11] *Id.* at 4.

[12] Department of Commerce, BIS, Temporary General License, May 20, 2019, (available at https://s3.amazonaws.com/public-inspection.federalregister.gov/2019-10829.pdf). Note that this is an unpublished version that is not scheduled to be published in the Federal Register until May 22, 2019.

The following Gibson Dunn lawyers assisted in preparing this client update: Judith Alison Lee, Adam M. Smith, Christopher Timura, and Laura Cole.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding the above developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any of the following leaders and members of the firm's International Trade practice group:

United States:
Judith Alison Lee - Co-Chair, International Trade Practice, Washington, D.C. (+1 202-887-3591, jalee@gibsondunn.com)
Ronald Kirk - Co-Chair, International Trade Practice, Dallas (+1 214-698-3295, rkirk@gibsondunn.com)
M. Kendall Day - Washington, D.C. (+1 202-955-8220, kday@gibsondunn.com)
Jose W. Fernandez - New York (+1 212-351-2376, jfernandez@gibsondunn.com)
Marcellus A. McRae - Los Angeles (+1 213-229-7675, mmcrae@gibsondunn.com)
Adam M. Smith - Washington, D.C. (+1 202-887-3547, asmith@gibsondunn.com)
Christopher T. Timura - Washington, D.C. (+1 202-887-3690, ctimura@gibsondunn.com)
Ben K. Belair - Washington, D.C. (+1 202-887-3743, bbelair@gibsondunn.com)
Courtney M. Brown - Washington, D.C. (+1 202-955-8685, cmbrown@gibsondunn.com)
Laura R. Cole - Washington, D.C. (+1 202-887-3787, lcole@gibsondunn.com)
Stephanie L. Connor - Washington, D.C. (+1 202-955-8586, sconnor@gibsondunn.com)
Henry C. Phillips - Washington, D.C. (+1 202-955-8535, hphillips@gibsondunn.com)
R.L. Pratt - Washington, D.C. (+1 202-887-3785, rpratt@gibsondunn.com)
Audi K. Syarief - Washington, D.C. (+1 202-955-8266, asyarief@gibsondunn.com)
Scott R. Toussaint - Palo Alto (+1 650-849-5320, stoussaint@gibsondunn.com)

Europe:
Peter Alexiadis - Brussels (+32 2 554 72 00, palexiadis@gibsondunn.com)
Attila Borsos - Brussels (+32 2 554 72 10, aborsos@gibsondunn.com)
Patrick Doris - London (+44 (0)207 071 4276, pdoris@gibsondunn.com)
Sacha Harber-Kelly - London (+44 20 7071 4205, sharber-kelly@gibsondunn.com)
Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Steve Melrose - London (+44 (0)20 7071 4219, smelrose@gibsondunn.com)
Benno Schwarz - Munich (+49 89 189 33 110, bschwarz@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Richard W. Roeder - Munich (+49 89 189 33-160, rroeder@gibsondunn.com)