HWG | HARRIS, WILTSHIRE & GRANNIS LLP

REGULATORY ADVISORY | INTERNATIONAL TRADE AND INVESTMENT | AUGUST 15, 2019

2019 Mid-Year Regulatory Preview

Enhanced Supply Chain Scrutiny for Technology and Telecommunications Companies and an Evolving Trade and Security Landscape in Asia Could Complicate the Regulatory Environment

Robert A. Friedman and Colleen A. Sechrest

Technology and telecommunications companies have faced a complex and shifting regulatory environment over the past twelve months. In this climate, companies must grapple with a number of pressing challenges, including the prospect of navigating a patchwork of new trade tariffs on a broad range of products from multiple countries, new restrictions on foreign investment, and an ever-evolving sanctions landscape. These factors have increased both the costs of compliance and the risks of noncompliance for businesses, particularly when viewed against the backdrop of more robust enforcement actions initiated by the U.S. Government—including the Office of Foreign Assets Control and the Committee on Foreign Investment in the United States ("CFIUS").

Supply chain security has been an additional area of enhanced regulatory scrutiny, both for technology and telecommunications companies that do business with the federal government and those that do not. Businesses are under increased pressure from the U.S. Government to ensure that potential supply chain vulnerabilities do not present risks to national security. Depending on the outcome of several rulemakings during the second half of 2019—as well as the Trump administration's approach to certain perceived threats from China, including Huawei Technologies Co. Ltd. ("Huawei"), and events unfolding in Hong Kong—the compliance burden for businesses could intensify further. At the same time, many of these developments provide avenues for investors, companies, and trade associations to shape the regulatory rules of the road.

To help companies make sense of the moving pieces, understand opportunities to shape the regulatory process, and make business plans accordingly, we briefly analyze the following: (1) the Securing the Information and Communications Technology and Services Supply Chain Executive Order (the "Supply Chain Order"); (2) the U.S. Commerce Department's Bureau of Industry and Security ("BIS") designation of Huawei and certain of its affiliates to the BIS Entity List (*i.e.,* a list of certain foreign persons subject to specific license requirements for the export, reexport and/or transfer (in-country) of specific items); and a BIS final rule creating a Temporary General License ("TGL") for the BIS Entity List designation; (3) enactment and implementation of section 889 of the National Defense Authorization Act for Fiscal Year 2019 ("NDAA FY 2019"); (4) draft provisions of the National Defense Authorization Act for Fiscal Year 2020 ("NDAA FY 2020"), Defending America's 5G Future Act, and the Huawei Prohibition Act of 2019; and (5) the evolving treatment of Hong Kong for export control and security purposes.

1. Supply Chain Executive Order

On May 15, 2019 President Trump issued the Supply Chain Order authorizing the Commerce Secretary to prohibit U.S. entities from using any "information and communications technology or services" that are "owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" if the transaction poses an "undue risk" of either sabotage to U.S. information and communications technology or of "catastrophic effects" to critical infrastructure, or, additionally, if the transaction "otherwise poses an unacceptable risk" to U.S. national security.

The Supply Chain Order represents the Executive Branch's most significant and far-reaching effort to date to regulate comprehensively the information and telecommunications supply chain in the United States, but the extent of the compliance burden it imposes on businesses will depend on the implementation process. If the Commerce Department rulemaking is narrow in scope, the Supply Chain Order could simply enable the U.S. Government to review businesses' commercial procurements of technology or services from a targeted group of high-risk vendors. However, if the Commerce Department writes the rules broadly, the Supply Chain Order could lead to an end-to-end regulatory approval process for private sector procurement of products and services in certain sensitive information and telecommunications sectors.

A. Key date: Commerce Secretary Ross announced earlier this summer that the Commerce Department will issue an Interim Final Rule ("IFR") in mid-October to implement the Supply Chain Order. Although there will be a public comment period that could modify the regulations going forward, the IFR will go into effect immediately.

B. What could change: The Supply Chain Order did not impose any immediate regulatory compliance requirements for businesses, and the scope and impact of the action will depend on the answers to a number of open questions, including: (a) which countries and persons are considered "foreign adversaries"; (b) what technology or services will be subject to restrictions; and (c) which products or companies will be deemed to be associated with foreign adversaries and warrant particular scrutiny. The Supply Chain Order should be closely monitored in several key areas:

- The scope of the prohibition extends to products *and* services. This means the U.S. Government can potentially prohibit U.S. companies from using certain service providers, including managed service providers and other third-party service providers in the technology and telecommunications sectors.
- The U.S. Government has the discretion to design and negotiate mitigation measures to address perceived national security threats and condition its regulatory approval of transactions (or groups of transactions) on implementing such mitigation. Elements of this risk mitigation process appear closely analogous to the mitigation processes currently utilized by CFIUS and Team Telecom in the foreign investment and telecommunications review contexts.

2. Huawei's Entity List Designation and Temporary General License

On May 16, 2019 BIS designated Huawei and 68 non-U.S. Huawei affiliates ("Huawei listed entities") to the BIS Entity List. As noted above, this designation imposes additional export license requirements on "exports, reexports, and transfers (in-country)" to Huawei listed entities on any item subject to the U.S. Export Administrations Regulations ("EAR"). Any pre-existing license exceptions under the EAR were

suspended for exports to Huawei and its designated affiliates, and BIS instituted a license review policy of a presumption of denial of export license requests. Furthermore, non-U.S.-made items that contain more than *de minimis* amounts of controlled U.S.-origin content also are subject to the EAR.

On May 20, BIS issued a final rule that created a TGL to partially restore the licensing requirement and policies under the EAR for "exports, reexports, and transfers (in-country)" to the Huawei listed entities within four categories of transactions: (a) continued operation of existing networks and equipment; (b) support to existing handsets; (c) cybersecurity research and vulnerability disclosure; and (d) engagement as necessary for development of 5G standards by a duly recognized standards body.

A. Key date: The TGL will be effective through August 19, 2019, unless extended.

B. What could change: There are several open questions related to implementation of the Entity List designation:

- First, it is unclear how the Trump Administration will implement the Entity List designation, and how strictly or permissively BIS will administer the licensing policy in light of the presumption of denial of export license requests. Commerce Secretary Ross suggested that the U.S Government would issue licenses to companies seeking to sell U.S.-origin goods to Huawei where there is no threat to national security. It is possible that Commerce could issue further policy guidance to the business community with more details on the precise products, technology, and software that do not threaten national security, or that Commerce could extend the TGL beyond August 19, which could be used as leverage in the ongoing trade negotiations with China.

- Second, President Trump has previously tied progress in trade talks with China to sanctions on a major Chinese company. Last year, he reversed a decision to restrict U.S. exports to ZTE Corporation ("ZTE") that could have put the company out of business. There is already some evidence of this tit-for-tat emerging in the Huawei context as well. Public reporting indicates that the White House plans to delay a decision on 50 export license applications that would allow U.S. companies to sell products, software and technology to Huawei in response to China's decision to halt purchases of U.S. agricultural products and amidst fears of a currency war.

3. Government Contractors' Supply Chains Impacted by Section 889 of NDAA FY 2019

The NDAA FY 2019, signed into law in August 2018, includes a number of provisions focused on enhancing supply chain security. Section 889 of NDAA FY 2019 ("section 889") imposes restrictions on federal government procurement and use of certain telecommunications equipment, software, and services from manufacturers owned by, controlled by, or connected to the Chinese government, including Huawei, ZTE, Hytera Communications Corporation Limited ("Hytera"), Hangzhou Hikvision Digital Technology Co., Ltd. ("Hikvision") or Dahua Technology Co., Ltd. ("Dahua") (or any subsidiary or affiliate of such entities). Under section 889, executive branch agencies—including the Departments of State and Defense—may not contract (or extend or renew a contract) with entities that use covered telecommunications equipment or services as a substantial or essential component, or critical technology as part of "any system."

There are two exceptions to section 889's prohibitions. Under the first exception, executive branch agencies may procure services that connect to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements. Thus, section 889 likely will not penalize a telecommunications

provider merely for exchanging traffic and otherwise having common network arrangements with covered telecommunications equipment or services. The second exception excludes any covered telecommunications equipment that "cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles." In other words, section 889 allows for executive branch agencies to contract with entities that use covered telecommunications equipment, so long as that equipment cannot access or interact with the content of the data it handles.

A. Key dates: The U.S. Government will implement section 889 in two phases via the federal acquisition rulemaking process—specifically, through Federal Acquisition Regulation ("FAR") Case 2018-017 and Case 2019-009. Key milestone dates are ***August 13, 2019*** (for prohibitions on direct government procurement of covered telecommunications equipment or services) and ***August 13, 2020*** (for prohibitions on use of covered telecommunications equipment and services by government contractors).

- Phase One—FAR Case 2018-017. On August 7, 2019, the Trump administration published an IFR that bars federal agencies from purchasing equipment and services from five Chinese telecommunications and video surveillance providers that the U.S. has deemed a national security threats (Huawei, ZTE, Hytera, Hikvision and Dahua). The regulation will apply to all new contracts and procurements as well as existing indefinite delivery contracts, and options picked up for existing contracts. The IFR went into effect on August 13, 2019 for federal agencies and there is a 60-day comment period.

- Phase Two—FAR Case 2019-009. This proposed rule will implement a prohibition on the government entering into, extending or renewing a contract with an entity that uses any equipment, system, or service that employs covered telecommunications equipment and services from Huawei, ZTE, Hytera, Hikvision or Dahua, to include any subsidiaries or affiliates. The Notice of Proposed Rulemaking ("NPRM") is slated for publication in December 2019 with the 60-day comment period ending in February 2020.

B. What could change: The August 13, 2019 IFR leaves a number of open questions. Interested parties have 60 days to file public comments and help shape the final rule. Select topics covered in the IFR include:

- Broadly defining "substantial or essential component" as any component necessary for the proper function or performance of a piece of equipment, system, or service; and

- Applying the government procurement restriction broadly to include acquisitions of commercial items, including commercial off-the-shelf items, regardless of the size of the purchase—even though the equipment or service being acquired has been sold or offered for sale to the general public, either in the same form or a modified form as sold to the government.

Further notice and comment rulemaking will precede implementation of Phase Two of Section 889 that will extend prohibitions on the use of covered telecommunications equipment and services to government contractors. We expect that the NPRM will clarify the application of the two exceptions referenced above regarding section 889's prohibitions.

4. Congress Seeks to Scrutinize Further Government Contractors and Codify Supply Chain Security and Limitations on Transactions with Huawei

The NDAA FY 2020 could bring additional scrutiny to government contractors' supply chains. The House version (H.R. 2500)—which passed on a vote of 220-197 on July 12, 2019—includes a provision that would ban or suspend contractors or subcontractors from doing business with the U.S. Government until their video surveillance and telecommunications equipment and services are deemed secure. It would also require a DoD "comprehensive assessment" of the Pentagon's current policies regarding procurement of foreign video surveillance and telecommunications equipment for the defense industrial base.

The Senate version of NDAA FY 2020 (S. 1790)—which passed on June 27, 2019 with an 86-8 vote—also focuses on shoring up the security practices of the U.S. Government's defense acquisition supply base. It would require the Secretary of Defense to "streamline and digitize" the DoD's approach to identifying and mitigating risks to the defense industrial base across the acquisition process. It would also create an "analytical framework" that (1) monitors supply chain, contractor, and current DoD procurement process risks, and (2) ensures collected data is maintained and easily accessible to "key decision-makers" in the DoD.

As these two versions of the bill head to the Conference Committee for reconciliation, the final version of the NDAA FY 2020 will likely contain some permutation of these supply chain security provisions.

Finally, on July 15, 2019, Senators Blumenthal, Cotton, Romney, Rubio, Van Hollen, and Warner introduced legislation to reinforce the Trump administration's efforts to enhance supply chain security and to place trade restrictions on Huawei. The Defending America's 5G Future Act would codify President Trump's Supply Chain Order discussed above and would prohibit the removal of Huawei from the BIS Entity List without an act of Congress. It also would empower Congress to disallow waivers that any administration might grant to U.S. companies engaged in transactions with Huawei. Representatives Gallagher, Panetta, Cheney, and Gallego have introduced companion legislation in the House of Representatives.

Senators Collins, Romney, and Rubio also introduced the Huawei Prohibition Act of 2019, on July 15, 2019 which—like the Defending America's 5G Future Act—would prohibit the removal of Huawei from the BIS Entity List without ensuring that Huawei is no longer a threat to the United States. However, this bill requires the Secretary of Commerce to make this certification instead of Congress.

5. The Evolving Treatment of Hong Kong for Export Control and Security Purposes

The United States-Hong Kong Policy Act of 1992 allows the United States to treat the Hong Kong Special Administrative Region ("Hong Kong") separately from the People's Republic of China ("China") (*i.e.*, the "one country, two systems" framework) on a range of issues, including visas, trade, law enforcement, investment, and export controls. For example, the United States treats Hong Kong and China as two separate destinations for U.S. export control purposes and Hong Kong receives favorable treatment with regard to U.S. export licensing and regulations because of its status as a cooperating country with multilateral export control regimes.

However, recent events—including proposed changes to Hong Kong law that would allow suspects to be extradited to mainland China, clashes between riot police and pro-democracy protesters, and reports of

the Chinese government sending its military to the Hong Kong border—have raised new concerns in the executive and legislative branches about longstanding U.S. policy. In its March 2019 report on the Hong Kong Policy Act, the State Department assessed that Hong Kong maintained a sufficient—although diminished—degree of autonomy under the one country, two systems framework to justify continued special treatment. Further, on June 11, 2019, Speaker of the House Nancy Pelosi noted that if the "horrific" extradition bill passes, Congress would have to reassess whether Hong Kong was "sufficiently autonomous" to justify its current status in trade with America, which sets it apart from China.

Any change in U.S. trade or security policy with Hong Kong could have a significant impact on U.S. businesses. According to the State Department, 85,000 U.S. citizens lived in Hong Kong in 2018 and more than 1,300 U.S. companies operate there, including nearly every major U.S. financial firm. Hong Kong is a major destination for U.S. legal and accounting services and had the largest U.S. bilateral trade-in-goods surplus at $31.1 billion in 2018.

* * * * *

For more information regarding supply chain security or Harris, Wiltshire & Grannis LLP's international trade and investment practice, please contact **Kent Bressie** at +1 202 730 1337 or kbressie@hwglaw.com, **Robert Friedman** at + 1 202 730 1335 or rfriedman@hwglaw.com, or **Colleen Sechrest** at +1 202 730 1308 or csechrest@hwglaw.com.

This advisory is not intended to convey legal advice. It is circulated to our clients and friends as a convenience and is not intended to reflect or create an attorney-client relationship as to its subject matter.