INSIGHTS

Client Alert: US Issues Huawei Export Restriction and Executive Order to Secure IT Supply Chain

May 28, 2019

The United States Government recently announced two national security-driven changes with far-reaching impact on trade and technology.

Huawei Restrictions

On May 21, 2019, the US Department of Commerce, Bureau of Industry and Security (BIS) published a final rule amending the Export Administration Regulations ("EAR") to add Chinese telecommunications equipment producer Huawei Technologies Co., Ltd. ("Huawei") and 68 of its non-U.S. affiliates (the "Huawei Entities") to the Entity List (Supplement No. 4 to Part 744), retroactively effective to May 16, 2019. This designation prohibits US and foreign companies from providing the Huawei Entities with "items subject to the EAR" (i.e., effectively, all commodities, goods, and software with more than *de minimis* U.S.-origin content) without a BIS-issued license.

BIS is offering some temporary relief, as it announced a 90-day general license, which temporarily eases the restrictions by authorizing certain exports, reexports, and transfers of EAR-controlled items to Huawei Entities. This temporary license is limited in scope to four types of transactions: (1) maintaining and supporting existing networks and equipment; (2) providing support for existing Huawei handsets; (3) conducting cybersecurity research and disclosing security vulnerabilities in relation to Huawei products; and (4) developing 5G standards as part of a duly recognized international standards body.

IT and Communications Supply Chain Security

In a related action, on May 15, 2019, the Trump Administration issued Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, directing the US Department of Commerce to implement regulations to prohibit US companies from purchasing foreign-made/foreign-provided information and communications products, technologies, and services if the Government determines the transaction poses a risk to the national security, foreign policy, or the economy of the US. While the order is widely believed to target Huawei, it does not specify countries or entities of particular concern, leaving this determination to agency discretion—a task that must be completed within 150 days of the order.

The executive order continues a trend of the current Administration's efforts to address perceived risks and threats to the supply chain supporting the nation's industrial base and critical infrastructure. Such efforts include statutory prohibition of US Government procurements from certain Chinese-sourced equipment), the creation of an Information and Communications Technology Supply Chain Task Force within the Department of Homeland Security, and the establishment of a Federal Acquisition Security Council.

How Ankura Can Help

These recent developments highlight the urgent need for U.S. and international technology and communications companies to have robust, responsive compliance programs for international trade compliance (exports, sanctions, and imports), supply chain and end-use diligence, and cybersecurity. Ankura's unique experience and expertise as former government prosecutors and regulators, in-house compliance executives and counsel, and trusted external advisors allow us to rapidly and efficiently help our clients grapple with and stay ahead of emerging developments in international trade.

Ankura can help companies and counsel:

- *Jurisdictional assessment* –Conduct technology/commodity classifications and *de minimis* analyses, and advise regarding interpretation and application of the EAR and entity list restrictions.
- *Licensing* – Engage with BIS to obtain reexport or transfer licenses, and also helps in interpreting and applying the 90-day temporary general license.
- *Distribution and supply chain diligence* – Identify and mitigate third-party trade compliance, technology, and vendor risks and challenges.
- *Network security diligence* – Leverage expertise in export controls, data analytics, cybersecurity, and national security to help clients assess and mitigate risks.
- *Compliance risk mitigation* – Adapt to changing regulatory environments with smart, managed application of business-integrated controls.
- *Chinese language capability* – Integrate US person team members with fluency in Mandarin.

Contact: Randall H. Cook Waqas Shahid Michael Garson

ankura