Hughes Hubbard & Reed

Trump Administration Issues Dual Orders Targeting Huawei and Economic Espionage

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

Last week, the Trump Administration took major steps to reduce the purported influence of "foreign adversaries" in the U.S. telecommunications industry, particularly Chinese telecom giant Huawei Technologies Co., with significant implications for Huawei's U.S. suppliers. The government actions have been viewed by many as an attempt to exclude China broadly and Huawei specifically from the U.S. telecommunications market. These actions follow Congressional action last year that banned Huawei from all U.S. government systems and from use by U.S. government contractors.

Dual Orders

On May 15, 2019, President Trump signed an Executive Order declaring that threats to network security are a national emergency. The order gives the Department of Commerce, in conjunction with other agencies, broad authority to review, cancel, or mitigate "transactions " involving "information or communications technology" that is "designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a "foreign adversary." The potential breadth – and the ambiguity – of the Order is apparent from the definitions of key terms:

- "Information or communications technology" -- "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."
- "Foreign adversary" -- "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."
- "Transaction" – "any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service."

While the order does not name any specific foreign country or company, it is widely understood that the primary targets are Huawei and its Chinese competitor ZTE Corp. The scope of the order remains unclear, and it could potentially give Commerce broad authority to ban even the use by U.S. persons of information or communications technology items from companies like Huawei or ZTE. Indeed, just last year Congress enacted a statutory ban (section 889 of the National Defense Authorization Act for 2019) that prohibits federal government executive agencies from (1) procuring or using Huawei or ZTE equipment, systems, or services, or (2) even entering into a contract with any entity that "uses" any Huawei or ZTE equipment, system, or service "as a substantial or essential component of any system, or as critical technology as part of any system."

President Trump issued the Order pursuant to his authorities under the International Emergency Economic Powers Act (IEEPA), which appears to be the first time the law has been used to target an entire economic sector of the United States. The Executive Order does not set forth a mechanism for parties to report or seek approval for covered transactions, nor does it identify categories of transactions that may be exempted from the Order. Such procedures could be created, however, through regulations that the Order directs Commerce to formulate within 150 days.

In a parallel – and perhaps more provocative – move, Commerce added Huawei to the Entity List, restricting its ability to purchase items or software of U.S. origin for use in its products (such as Google's Android operating system). The Entity listing was contained in a May 16, 2019, Federal Register notice that included 68 of Huawei's non-U.S. affiliates. Pursuant to the Export Administration Regulations (EAR), Commerce's Bureau of Industry and Security (BIS) places foreign entities on the Entity List if it determines that there is reasonable cause to believe that a company is, or will be, "involved in activities that are contrary to the national security or foreign policy interests of the United States."

Why Huawei?

According to the Trump Administration, BIS has placed Huawei on the Entity List after determining that Huawei's activities are contrary to U.S. national security or foreign policy interests. The U.S. Department of Justice (DOJ) announced criminal charges against Huawei in January 2019, alleging nearly two dozen violations in connection with a purported scheme to evade Iranian sanctions. In addition to charging the Company, DOJ also charged Huawei's CFO, Wanzhou Meng, asserting that she played an integral role in obscuring Huawei's relationship with Iran from the U.S. government and global financial institutions.

The Executive Order and the placement of Huawei on the entity list also come as the U.S. seeks to diminish Huawei's influence in the development of 5G wireless technology. Huawei is the world's largest supplier of telecommunications equipment and the second-largest manufacturer of mobile phones, having displaced Apple from the number two position last summer. In recent months, Huawei has been at the forefront of the race between the United States and China to develop 5G technology, which is expected to significantly increase the speed of wireless technology and facilitate the development of next-generation technology such as autonomous driving vehicles. Though the Chinese company describes itself as privately owned by its employees, U.S. officials have openly questioned its ownership structure and have asserted that the Chinese government may have outsized influence in Huawei's operations. The United States has resisted China's influence in the development of 5G, voicing concerns that the Chinese government would be able conduct cyber-espionage in networks developed by Chinese companies.

Implications

The U.S. is not alone in its fears of Chinese cyber-espionage: other countries, including Japan and Australia, have banned Huawei. However, European countries have yet to follow suit, and telecom companies based in Sweden and Finland have been in talks with Huawei to set up 5G networks. The Trump Administration's recent actions

could serve as a warning to European countries to reconsider the costs and risks in developing 5G technology within their borders.

It remains unclear whether Commerce will grant U.S. suppliers licenses to engage in business with Huawei. However, based on the order adding Huawei to the Entity List, it is unlikely that many licenses will be granted, as the order announced "a presumption of denial" in the license review process. Qualcomm and other U.S. microchip manufacturers will likely see the most acute impact, as U.S. companies account for nearly half of the sales of chips worldwide every year, while Chinese manufactures make up only 3% of the global market. Huawei heavily relies on U.S. companies to supply semiconductors necessary for its manufacturing operations; with U.S. companies supplying approximately $11 billion of Huawei's $70 billion procurement spend.

The Executive Order creates more questions than answers, as officials have not specified which entities or countries will be affected, and officials have not indicated how broadly they will make use of the Order. Although Chinese hardware makes up less than 1% of U.S. telecom networks, many rural carriers rely heavily on inexpensive Chinese infrastructure products, which could be banned by Commerce under the Order. Even so, the Order does not specify whether existing information technology would need to be replaced if Commerce determines that such Chinese hardware is a threat to U.S. national security.

Further, the dual actions by the Trump Administration come as the United States and China continue tense – and deteriorating – trade negotiations. In the week before these actions, the Trump Administration increased tariffs on nearly $200 billion in Chinese goods. Now, the Trump Administration is targeting one of China's most important companies, which could further complicate the negotiations and escalate the trade war between the two countries.

Related People

Ryan Fayhee

Alan G. Kashdan

Tyler Grove

Sydney Stringer

Related Areas of Focus

Sanctions, Export Controls & Anti-Money Laundering
International Trade
Data Privacy & Cybersecurity