O'Melveny

Alerts & Publications

The Government Is Wielding Sticks and Carrots to Address National Security Concerns in the Telecommunications Sector

October 3, 2019

KEY CONTACTS

John Dermody
Washington, DC
D: +1-202-383-5306

Theodore W. Kassinger
Washington, DC
D: +1-202-383-5170

Greta Lichtenbaum
Washington, DC
D: +1-202-383-5249

The security of information and communications technology, and particularly the supply chain that supports that technology, has become a major focus of the national security community. Recent reports suggest that the Department of Commerce will soon announce a ban on the acquisition and use of Huawei products and services by industries and consumers in the United States. This ban would be in addition to existing prohibitions on the federal government's acquisition and use of technology produced by Huawei and other Chinese technology manufacturers. Beyond this specific anticipated action, senior government leaders have been pushing for greater engagement with the information and communications technology industry, with Senator Mark Warner recently calling for a reevaluation of US industrial policy to provide direct support to develop a secure and trusted telecommunications infrastructure. As the national security community continues to extend its influence into economic matters, companies and consumers will need to be prepared to swiftly adjust their technology supply chain and acquisition strategies, and develop processes for ensuring compliance with new restrictions.

Sticks

On October 12, the Department of Commerce is set to issue guidance implementing the Executive Order on Securing the Information and Communications Technology and Services Supply Chain (Supply Chain Executive Order). Relying on the International Emergency Economic Powers Act (IEEPA), the Supply Chain Executive Order prohibits transactions that the Secretary of Commerce determines involve "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 that pose an undue or unacceptable risk to national security. The scope of the Supply Chain Executive Order's application is potentially quite broad, and early signs indicate that it will be used to prohibit the purchase and use of certain Chinese technology by companies and consumers in the US. Commerce's implementing guidance will be an indication of how the administration will wield this significant authority and whether they will establish an information and communication technology review process similar to the processes used by the Committee on Foreign Investment in the United States.

Such measures would mirror Commerce's actions in the area of export controls. In May, it placed Huawei on the Entity List, effectively limiting companies' ability to export, re-export, or transfer US-origin hardware, software, and technology to listed Huawei entities. While a general license allows limited transactions to support some continued operations of networks, equipment, and personal consumer electronics devices among other limited purposes, that license expires on November 17, 2019, and the likelihood of its extension is unclear.

The federal government has already taken steps to restrict the use of Huawei and other Chinese technology in its own systems. In August, the Department of Defense, the General Services Administration, and the National Aeronautics and Space Administration issued an interim rule implementing section 889 of the National Defense Authorization Act for Fiscal Year 2019. Section 889 prohibits the government's acquisition of certain "telecommunications equipment or services" provided by Huawei, ZTE, Hytera Communications, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, or any entity that the Secretary of Defense reasonably determines is owned, controlled by, or otherwise connected to the government of China. The interim rule includes a number of broad provisions and adopts the definition of "critical technologies" from the Foreign Investment Risk Review Modernization Act. The interim rule, however, does not address subsection (a)(1)(b) of section 889—set to go into effect in August of 2020—which would prohibit the government from entering into a contract with any entity that merely uses prohibited telecommunications equipment or services (even if that company is not

providing that technology or service to the government). Although these restrictions are focused on government contracting, they could have significant ripple effects and may foreshadow how the government will act in other areas related to information and communications technology.

Carrots

There are other indications that the federal government may offer carrots to go along with these sticks. There is bipartisan support for financial incentives to improve security, and Congress has proposed several pieces of legislation. Senators Warner and Crapo have co-sponsored S.2316, the Manufacturing, Investment, and Controls Review for Computer Hardware, Intellectual Property, and Supply Act of 2019. In addition to establishing a new National Supply Chain Intelligence Center within the Office of the Director of National Intelligence, the bill would amend section 303 of the Defense Production Act of 1950 to allow the President to make payments to eligible entities "to increase the security of supply chains and supply chain activities." An "eligible entity" is any entity that "(A) is organized under the laws of the United States or any jurisdiction within the United States; and (B) produces (i) one or more critical components; (ii) critical technology; or (iii) one or more products for the increased security of supply chains or supply chain activities."

In the House, Representatives Frank Pallone and Greg Walden recently introduced a bi-partisan bill that would "provide for the establishment of a reimbursement program for the replacement of communications equipment or services posing [national security risks]." The bill would authorize the Federal Communications Commission (FCC) to reimburse communications service providers with fewer than 2 million customers for the costs of permanently removing and replacing communications equipment determined by the FCC to pose "an unacceptable risk to the national security of the United States or the security and safety of United States persons." Although the likelihood of either bill advancing remains unclear, they echo a key goal of the administration's National Cyber Strategy, which is to "[p]romote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation."

Implications for the Future

The rules applicable to information and communications technology are rapidly evolving. This will have significant ramifications for the telecommunications industry, as well as companies seeking to take advantage of emerging communications technology, like 5G mobile communications. Industry will need to account for continued volatility and develop processes to evaluate and potentially modify their information and communications technology supply chains. The intense focus on the security of information and communications technology will likely be an enduring trend, as efforts in this area have spanned both the Obama and Trump administrations. The interdependence of government and private sector communications technology will attract a wide array of executive and legislative branch actors, each bringing their particular national security, international trade, or domestic policy perspectives. Regardless of whether the federal government pursues these national security issues with sticks or carrots, the law applicable to information and communications technology is becoming increasingly complex.

This memorandum is a summary for general information and discussion only and may be considered an advertisement for certain purposes. It is not a full analysis of the matters presented, may not be relied upon as legal advice, and does not purport to represent the views of our clients or the Firm. Steve Bunnell, an O'Melveny partner licensed to practice law in the District of Columbia, Theodore W. Kassinger, an O'Melveny partner licensed to practice law in the District of Columbia and Georgia, Greta Lichtenbaum, an O'Melveny partner licensed to practice law in the District of Columbia, Lisa Monaco, an O'Melveny partner licensed to practice law in New York, and John Dermody, an O'Melveny counsel licensed to practice law in California, contributed to the content of this newsletter. The views expressed in this newsletter are the views of the authors except as otherwise noted.