wiley

ALERT

Commerce Publishes Proposed Rules Implementing Communications Supply Chain Executive Order

November 26, 2019

On November 26, 2019, the U.S. Commerce Department (Department) released proposed rules implementing President Trump's May 15, 2019 Executive Order (EO) potentially blocking or restricting transactions involving information and communications technology and services (ICTS) from a "foreign adversary." The proposed regulations would create a new process and procedures, and empower the Secretary of Commerce (Secretary) to identify, assess, and address information and communications technology and services transactions initiated, pending or completed after May 15, 2019 (including ongoing activities), that pose an undue risk to U.S. critical infrastructure or the digital economy in the United States, or an unacceptable risk to U.S. national security or the safety of U.S. persons. While the proposed regulations do not identify any countries or companies as "foreign adversaries," the EO is widely viewed as targeted—at least for now—at Chinese equipment manufacturers such as Huawei and ZTE. Comments on the proposed rules will be due December 27, 2019, unless there is an extension.

The proposed rules would directly affect a number of sectors, including:

- Telecommunications service providers, including wireline, wireless, satellite, paging, and resellers;
- Internet and digital service providers, including cloud, data center, and managed security service providers, app developers, and software providers; and

Authors

Nova J. Daly
Senior Public Policy Advisor
202.719.3282
ndaly@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Daniel P. Brooks
Partner
202.719.4183
dbrooks@wiley.law

Practice Areas

Committee on Foreign Investment in the United States (CFIUS)
Corporate
Government Contracts
International Trade
Internet of Things
National Security
Telecom, Media & Technology

- Vendors and equipment manufacturers, including infrastructure vendors, broadcasting and wireless communications equipment manufacturers, and connected device manufacturers.

Review of Transactions

The proposed rules establish a regime for the Secretary to engage in a case-by-case analysis and possibly prohibit or restrict ICTS transactions that may be covered by the EO. In this context, a "transaction" is not just a merger or acquisition, but involves a wide array of business deals and operations, including the acquisition and maintenance of equipment and the provision of services.

The Secretary will determine, in consultation with the heads of other agencies, how to resolve a covered transaction. Prohibiting a transaction may include requiring that the parties engaged in the transaction immediately cease the use of the ICTS that poses the unacceptable risk, even if such ICTS has been installed or was in operation prior to the Secretary's determination. It also permits the Secretary to require the unwinding of a consummated deal. The impact of this new regime will be broadly felt, as it seems applicable to software updates, application development, and myriad other routine business interactions.

The review process would in many ways parallel that of the Committee on Foreign Investment in the United States (CFIUS), which scrutinizes certain foreign investments in U.S. businesses for national security implications. As with the CFIUS process, the proposed rules would allow the Department to evaluate individual transactions on a case-by-case basis and to unwind completed transactions or subject transactions to mitigation. In order to be covered, a transaction would need to (1) involve property in which a foreign country or national has an interest; (2) include 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 (3) pose certain undue risks to critical infrastructure or the digital economy in the United States or certain unacceptable risk to U.S. national security or U.S. persons.

The Department will not issue advisory opinions as to whether any particular transaction would be prohibited under the EO; parties will need to affirmatively request that the Secretary evaluate a transaction (unless the Department or another agency initiates the review). In contrast to the CFIUS process, the proposed regulations do not identify the specific information that parties to a transaction will need to provide. The proposed regulations would also allow parties to challenge any preliminary determinations or penalty notices issued by the Department. The Department will publish summaries of its final determinations in the *Federal Register*.

The Department invites comment on all aspects of the proposed regulation, including:

- Are there instances where the Secretary should consider categorical exclusions or exempt certain classes of persons whose use of ICTS can never violate the EO?
- Are there transactions involving types or classes of ICTS where the acquisition or use in the United States would fall within the terms of the EO's prohibited transactions because the transaction could present an undue or unacceptable risk, but that risk could be reliably and adequately mitigated?

- If mitigation measures are adopted for a transaction, how should the Secretary ensure that parties consistently execute and comply with the agreed-upon mitigation measures?
- How should the EO's definition of "transaction" (in particular, the terms "dealing in" and "use") be interpreted?
- Should the Department require additional recordkeeping requirements for information related to transactions?

The Broader Context

The United States is in the midst of several overlapping and interrelated efforts on telecom and internet security. Last week, the Federal Communications Commission (FCC) took action to address what FCC Chairman Ajit Pai considers dangerous Chinese influence in the nation's communications networks by prohibiting the use of Universal Service Fund (USF) monies by carriers to purchase equipment and services from companies that the FCC determines pose a national security threat. The FCC is considering broader ICT supply chain action, regardless of whether a company receives federal funding, as well. In addition, the Department of Commerce's Bureau of Industry and Security (BIS) has placed Huawei and 114 of its affiliates on BIS's Entity List, severely limiting U.S. companies' ability to transact with the company. The Federal Acquisition Security Council, recently created by Congress, is evaluating how to target suspicious companies and secure supply chains, and the Federal Acquisition Regulatory Council is in the midst of developing contracting restrictions to implement directives in last year's National Defense Authorization Act about permissible equipment. And, the business community is still working through CFIUS reform regulations under the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which broadened the authorities of the President and CFIUS to address national security concerns.

At bottom, the EO's intention to be technologically and country agnostic has resulted in opening the door to government review of a large number of transactions covering numerous industry sectors. Such a review could introduce delay and uncertainty into the timing and approval of transactions involving foreign companies.

Next Steps

Those impacted by these proposed rules should act quickly to help the Department shape the final rules and consider limitation to resolve some uncertainty that may chill business transactions. The Department will be taking meetings on the proposals, and interested parties may submit written comments. Affected parties should also consider what lessons have been learned from engaging in CFIUS and Team Telecom review of transactions that can be extrapolated to narrow or streamline the Department's review process. Given the short period of time for comment, potentially affected parties around the world should consider how this new regime could impact their investments and operations. This is particularly important given the future applicability to companies and countries other than those currently under security scrutiny by the United States. It is likely that the United States government will, in the future, identify other areas or products of concern, with whom business dealings would be subject to uncertainty and potential government superintendence.

Wiley Rein continues to closely monitor regulatory developments affecting the communications supply chain and the impacts of the U.S. government's crackdown on Chinese telecom companies.

Wiley Rein's Telecom, Media & Technology, International Trade, and National Security teams have been collaborating with companies around the world on these fast-moving supply chain issues and government review of transactions and business deals. Given the importance of these issues and our deep expertise with the Commerce Department and national security agencies, we look forward to helping our clients adapt to and shape this new regulatory regime. The time for public comment is unfortunately quite short, so do not hesitate to contact us with questions.

Additional practitioners in this area include:

Ambassador David A. Gross

Kathleen A. Kirby

Eve Klindera Reed

Lori E. Scheetz

Jack Shane

We have hosted several events with senior government officials to shed light on these issues, including this recent webinar with the Acting head of NTIA, Diane Rinaldo, and an update on CFIUS and FIRRMA.