Commerce Department Takes Steps To Thwart Use of Information and Communications Technology and Services Associated With Foreign Adversaries

Skadden

12 / 12 / 19

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

Ivan A. Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

Daniel J. Gerkin
Counsel / Washington, D.C.
202.371.7194
daniel.gerkin@skadden.com

Nicholas A. Klein
Associate / Washington, D.C.
202.371.7211

Four Times Square
New York, NY 10036
212.735.3000

1440 New York Avenue, N.W.
Washington, D.C. 20005
202.371.7000

On November 27, 2019, the U.S. Department of Commerce (Commerce) published a proposed rule that would establish a new and especially broad power for the U.S. government to review and potentially block or unwind transactions involving foreign Information and Communications Technology and Services (ICTS). This sweeping new authority would allow Commerce to unilaterally review and prevent any foreign ICTS-related transaction in the United States or involving U.S. persons. As outlined in our summary of President Trump's May 15, 2019, Executive Order finding a threat to U.S. national security arising from the acquisition and use in the United States of ICTS supplied by "foreign adversaries" (available here), this proposed rule was expected to detail the new review regime, including standards of jurisdiction, procedures for review and criteria for potential exclusions. However, the rule's scope, limitations on authority and review process itself lack detail and clarity — creating significant uncertainty as to the scope and potential impacts of the proposed rule. Importantly for dealmakers and industry, the proposed rule does not include a safe-harbor provision to reduce transactional risk.

Commerce has requested written comments, which must be submitted by December 27, 2019.

Summary of Proposed Rule

Scope of Covered Transactions

The proposed rule would give Commerce (in consultation with several other departments and agencies) discretion to review a broad array of "transactions" on a case-by-case basis, including any "acquisition, importation, transfer, installation, dealing in, or use of any [ICTS]" that: (i) involves any person or property subject to U.S. jurisdiction; (ii) involves property, technology or a service in which any foreign country or foreign person has an interest; and (iii) is initiated, pending or will be completed after May 15, 2019. Notably, ongoing managed services, software updates, or repair services meeting these criteria, even if associated with contracts executed before May 15, 2019, would potentially be subject to review. There are no U.S. dollar or other thresholds that would limit the expansive scope of the transactions potentially subject to review.

Commerce specifically declined to recognize any particular technologies or particular participants in the market for ICTS as categorically included or excluded from the prohibitions established by the Executive Order, opting instead for a case-by-case, fact-specific approach that would enable the targeting and prohibition of transactions "without unintentionally prohibiting other transactions involving similar ICTS that may not rise to the level of presenting an undue risk to critical infrastructure or the digital economy in the United States or an unacceptable risk to national security or the safety of U.S. persons." However, the broad definitions in the proposed rule dramatically expand the scope of potentially covered transactions.

First, ICTS is broadly defined, as in the Executive Order, to include "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 through transmission, storage, or display."

Second, a transaction would be potentially subject to review if it involves ICTS "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary." As drafted,

however, the proposed rule does not specify what constitutes "subject to the jurisdiction of a foreign adversary." Thus at least for now, under a plain reading of the regulation, even a non-U.S. subsidiary that is organized and located in a jurisdiction determined to be a foreign adversary potentially could be implicated. Commerce did, however, enumerate certain factors that would inform its determinations regarding ownership, control and foreign adversary jurisdiction, specifically "the laws and practices of the foreign adversary; equity interest, access rights, seats on a board of directors or other governing body, contractual arrangements, voting rights, and control over design plans, operations, hiring decisions, or business plan development."

Third, Commerce also did not further expand upon the definition of "foreign adversary," which, as in the Executive Order, is characterized as "any foreign government or non-government person determined by the Secretary to have 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." Commerce specifically noted that "foreign adversary" determinations are exclusively a matter of executive branch discretion and therefore declined to identify any such governments or persons. Such an approach would almost certainly apply to China.

As currently contemplated, these definitions and the scope of covered transactions will subject an extremely wide-range of ongoing or contemplated ICTS transactions to review and potential resulting mitigation, including either blocking or unwinding. Commerce has requested comments on whether it should consider categorical exclusions of certain types of ICTS transactions but, as noted above, it has explicitly declined to do so in the proposed rule, opting instead for a case-by-case review.

Initiation and Review Process

The proposed rule grants the Secretary of Commerce (Secretary) complete discretion to determine which transactions to review. Evaluation of a transaction is initiated in three ways: (i) at the Secretary's discretion; (ii) upon request by another U.S. government department or agency; or (iii) based on information provided by private parties via a Commerce web portal. The latter method likely is intended to enable parties to a proposed transaction to have that transaction reviewed before proceeding given that Commerce has made clear that it will not be issuing advisory opinions or declaratory rulings with respect to any particular transaction.

Once Commerce decides to initiate review of a covered transaction, for which no timetable is established, the Secretary (in consultation with several other departments and agencies) will evaluate whether the transaction:

i. poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;
ii. poses an undue risk of catastrophic effects on the security or resiliency of U.S. critical infrastructure or the U.S. digital economy; or
iii. otherwise poses an unacceptable risk to U.S. national security or to the security and safety of U.S. persons.

The Secretary will then issue a preliminary determination of whether an ICTS transaction with a foreign adversary poses a risk to U.S. national security. Although Commerce has the option to contact the parties to a transaction, such a preliminary determination could be the first notice parties receive that a transaction was under review or that a particular foreign party or country is considered a "foreign adversary." Upon receipt of the preliminary determination, parties have the option to submit an "opposition" within 30 days that the Secretary may consider in reaching a final determination on whether to mitigate, unwind or block the transaction. Final determinations are expected within 30 days of the submission of any opposition. No specific guidance exists on the likely nature, scope and duration of any mitigation, though a directive to discontinue using or even to "rip and replace" any offending hardware or software without compensation is possible. Commerce will make public a summary of each final determination.

Violations of any requirement, including failure to abide by the terms of any mitigation agreement, subject the violator to the potential imposition of civil penalties in an amount not to exceed $302,584, as adjusted for inflation, or, depending on circumstances, the value of the underlying transaction or twice the value of the underlying transaction.

Government Approach to ICTS-Related Security Vulnerabilities

The proposed rule is the latest in a years-long U.S. government effort to prevent threats to U.S. telecommunications, network and computing infrastructure. In 2012, the House Permanent Select Committee on Intelligence issued a scathing bipartisan report on efforts by Chinese companies Huawei Technologies

Commerce Department Takes Steps to Thwart Use of Information and Communications Technology and Services Associated With Foreign Adversaries

Co. Ltd. (Huawei) and ZTE Corporation (ZTE) to infiltrate U.S. telecommunications networks and steal U.S. technology. Huawei and ZTE have since faced many legal and regulatory actions by the U.S. government, including currently pending criminal charges against Huawei for corporate espionage, wire fraud and obstruction of justice. In May 2019, Commerce added Huawei to the Entity List, which generally restricts the company's access to U.S. technology. Similarly, Commerce temporarily added ZTE to the Denied Persons List in February 2018 after ZTE violated its 2017 agreement settling civil and criminal allegations of violating U.S. sanctions against Iran and North Korea.

On August 13, 2019, the U.S. Department of Defense, General Services Administration, and National Aeronautics and Space Administration implemented an interim rule under the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA). The rule generally prohibits executive agencies from procuring telecommunications equipment and services from Huawei, ZTE and other named Chinese technology companies and imposes strict reporting and other requirements on U.S. government contractors. This legislation followed a 2018 directive issued by the U.S. Department of Defense prohibiting retail outlets on U.S. military bases from selling Huawei devices and is consistent with an effort by the U.S. government to pressure both U.S. wireless carriers and allied governments from using Huawei hardware.

On November 22, 2019, the Federal Communications Commission (FCC) adopted a Report and Order that bars telecommunications carriers from using U.S. government subsidy funds to purchase equipment and services from companies that are a national security concern — currently including only Huawei and ZTE. Under this rule, the FCC's approximately $8.5 billion Universal Service Fund, available for U.S. carriers to expand rural and remote telecommunications infrastructure, may not be used to purchase, operate or provide services to, or involve equipment or services from, these vendors.

Although likely intended to target Chinese telecommunications equipment companies like Huawei and ZTE, the Commerce ICTS proposed rule is not limited to a particular country or specific companies, and it grants the Secretary broad discretion to designate a foreign government or foreign non-government person as a "foreign adversary." Thus, even if the current administration's short-term objectives are specific to threats posed by Huawei and ZTE, the proposed rule may result in a more expansive application over time.

Troubling Effects of the Proposed Rule

The proposed rule is intended to give the U.S. government a broad and powerful tool to address a problem that — in the government's view — remains vexing despite a range of existing regulatory authorities. For example, although the NDAA and implementing regulations may prevent private parties from doing business with the U.S. government by virtue of the U.S. government's inherent control over its purchasing decisions, those provisions do not control private company decisions to implement foreign ICTS products in their private network infrastructure. Similarly, listing Huawei and ZTE on restricted party lists under U.S. export controls is a party-specific targeting that does not address more strategic concerns, nor do more traditional regulatory tools solve the U.S. government's security challenges. For example, U.S. export controls regulate the provision of U.S. goods or technology to foreign parties but lack oversight of equipment or technology purchases by U.S. persons, and while the Committee on Foreign Investment in the United States (CFIUS) reviews foreign investment in U.S. businesses, it does not have jurisdiction over a U.S. party's acquisition of equipment from a foreign supplier.

Creating a new regulatory regime, however, as demonstrated by the proposed rule itself, poses significant complexities. As drafted, the significant discretion that the proposed rule grants to the Secretary, with few if any executable standards, may become unpredictable and create uncertainty for the telecommunications and information systems industries, leaving companies little choice but to resort to sourcing equipment from western suppliers that are less likely to be deemed adversarial, at considerable time and expense.

Many of the principles of the ICTS review process draw parallels to the CFIUS review process but, unlike the vastly more detailed CFIUS regulations developed over decades, the proposed rule's scant seven pages fail to provide a meaningful basis for such a process. This concern manifests in multiple ways, most prominently in the lack of participation by parties contemplating a transaction. The proposed rule does not include a formal method for parties to submit a notice of a transaction (similar to the voluntary notice provisions of other review regimes, such as CFIUS or Team Telecom).[1] Although the proposed rule

[1] Team Telecom is the colloquial term for the working group of representatives from the federal government charged with ensuring national security — the Departments of Homeland Security, Defense, Justice, State, Treasury, and Commerce, as well as the Office of the United States Trade Representative and the Federal Bureau of Investigation — when a foreign person invests in U.S. communications assets.

affords parties the opportunity to submit an "opposition" after the Secretary has reached a preliminary determination, limited information and virtually no standards are provided currently to guide the Secretary in reaching a final determination.

Next Steps

As noted above, the deadline for commenting on these proposed rules is December 27, 2019. Commerce explicitly has solicited comments regarding, for example, circumstances under which categorical exclusions might be appropriate, thereby suggesting that Commerce is cognizant of the expansive scope of these proposed rules. Based on the comments received, Commerce has discretion to issue a final rule that takes comments into account. No timetable has been established for issuance of a final rule, but potentially impacted companies, including in particular, telecommunications service providers, internet and digital service providers, and vendors and equipment managers, would be well-advised to review their supply chains and forecasted needs for ICTS to evaluate the potential effects of any final rule.