ALSTON & BIRD

WWW.ALSTON.COM

International Trade & Regulatory ADVISORY ■

DECEMBER 4, 2019

Proposed Rule on ICTS Supply Chain Leaves More Questions Than Answers for Industry

In connection with an Executive Order issued by President Trump earlier this year, the U.S. Department of Commerce published a proposed rule further expanding the powers of the federal government to intervene in certain transactions involving foreign persons where it determines there is a risk to national security. The proposed rule provides for the blocking or restriction of transactions involving "information and communications technology and services" (ICTS) from a "foreign adversary." It would empower the Secretary of Commerce to initiate a review process for foreign transactions in a manner appearing to bear some similarity to that of the Committee on Foreign Investment in the United States (CFIUS), which can block U.S. investments and acquisitions by foreign persons. However, unlike the 300-plus pages of proposed rules expanding CFIUS authority recently published by the U.S. Department of the Treasury, this proposed rule from Commerce provides little to no guidance for U.S. businesses about which ICTS transactions are at-risk of government intervention or how to mitigate that risk.

While Commerce does not identify specific "foreign adversaries," the proposed rule may be viewed in context with ongoing regulatory and policy developments. Just four days before Commerce released the proposed rule, the Federal Communications Commission (FCC) designated Chinese telecommunications giants Huawei Technologies Co. and ZTE Corp. as "national security threats" and banned the use of any of the FCC's $8.5 billion Universal Service Fund for the purchase or maintenance of Huawei and ZTE products. Earlier this year, Commerce placed Huawei and more than a hundred of its affiliates on its Entity List, hindering companies' ability to export and re-export certain hardware and software to Huawei. In addition, the recently proposed CFIUS reform regulations specifically allow for the review of an expanded category of investments by foreign persons in U.S. companies that supply, build, service and manage ICTS infrastructure. So while Commerce's proposed rule itself lacks specificity, U.S. businesses may infer that the proposed rule serves as one of the latest efforts by the U.S. government to guard against the risk of data theft and suspected espionage by China and its perceived proxies and that transactions involving Huawei, ZTE, and other Chinese telecommunication and technology companies will be under scrutiny.

Background and Scope of Proposed Rule

On May 15, 2019, President Trump issued an Executive Order on "Securing the Information and Communications Technology and Services Supply Chain," declaring a national emergency as "foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services … in order to commit malicious cyber-enabled actions, including economic and industrial espionage." The Executive Order seemingly targets a wide range of transaction types involving U.S. and foreign persons, apparently regardless of location, that could impact the ICTS infrastructure of the United States. The Executive Order granted Commerce 150 days to publish proposed regulations implementing the Order's directive, which it belatedly published on November 26.

The proposed rule provides the Secretary of Commerce, in consultation with other regulatory agencies, the power to prohibit or impose conditions on "the acquisition, importation, transfer, installation, dealing in, or use by persons subject to U.S. jurisdiction" of ICTS provided by a "foreign adversary" that the Secretary believes poses: (1) an undue risk of sabotage or subversion of ICTS in the United States; (2) an undue risk of catastrophic effects on the security and resiliency of critical infrastructure or the digital economy in the United States; or (3) an unacceptable risk to national security or to the security and safety of U.S. persons.

Notably, the U.S. government already has authority through CFIUS to block transactions involving foreign persons identified as a national security risk and, similarly, the U.S. General Services Administration and U.S. Department of Defense already have authority under the National Defense Authorization Act of 2019 to prohibit the procurement by certain contractors of ICTS from foreign companies that Congress has deemed threats to U.S. national security. Despite this, the proposed rule creates yet another mechanism through which the U.S. government may regulate ICTS transactions. Thus, while the business community has become increasingly aware of the requirements and potential restrictions that may be imposed by CFIUS in the context of an increasing variety of investments in U.S. businesses by foreign parties, the proposed rule captures a wider range of transactions, including potentially routine U.S. purchase and sourcing transactions never before regulated in this manner.

Given the breadth of transactions potentially captured by the Executive Order, the business community may have expected the proposed regulations to identify (1) the countries or entities considered "foreign adversaries" or, at minimum, the criteria for such a designation; (2) the specific ICTS to be protected; and (3) procedures for licensing U.S. companies to engage in ICTS transactions that could otherwise be prohibited. The proposed rule provides no such information. Instead, it announces a "case-by-case, fact-specific approach" to determine which transactions are to be prohibited or mitigated and explicitly includes that "[t]he Secretary will not issue an advisory opinion or a declaratory ruling with respect to any particular transaction."

Parties have 30 days to provide comments on the proposed rule, a process that could be vital in impressing upon Commerce the need for specific criteria and procedures in the final rule. The following aspects of the proposed rule may highlight the need for further clarity from Commerce but also shed light on the breadth of foreign parties and transactions the U.S. government seeks to regulate:

- **Application of the rule to the "acquisition, importation, transfer, installation, dealing in, or use by persons subject to U.S. jurisdiction" could capture a wide array of sourcing transactions.**

The proposed rule addresses "any acquisition, importation, transfer, installation, dealing in, or use of an information and communications technology or service that has been designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries have on the national security, foreign policy, and economy of the United States." Notably, while there is an array of transactions that could be captured by the rule as proposed, and while the term "dealing in," traditionally used in the context of sanctions and embargoes, can be broadly construed, the rule appears to be limited to transactions involving **supplies of ICTS** from persons subject to the jurisdiction of a foreign adversary and not to sales or deliveries to such persons. Such an interpretation is consistent with the President's determination that the unrestricted acquisition or use of ICTS causes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. It is also consistent with the well-established export regulatory framework which is best equipped to address U.S. national security concerns about sales or deliveries to foreign adversaries.

- **The broad definition of ICTS suggests the rule could impact an almost unlimited number of U.S. businesses.**

The term "information and communications technology or services" is defined as "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." In publishing the proposed rule, Commerce specifically notes, "[t]he proposed rule does not recognize particular technologies or particular participants in the market for ICTS as categorically included or excluded from the prohibitions ...."

Aside from servers, cloud storage, and networks commonly associated with ICTS, today virtually any product – ranging from mobile devices or applications, tablets, watches, remote controls, and even cars – can include information and data processing technologies and communication capabilities.

- **"Foreign Adversaries" are not limited to countries and could be anywhere.**

The proposed rule allows for the review of a transaction that "involves 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**." This language shows significant global reach allowing for the review of any ICTS transaction with U.S. persons (which include non-U.S. persons within the United States or involving U.S. persons abroad) by companies subject to the jurisdiction of a foreign country. Recently, in other contexts, global companies, even U.S.-organized companies ultimately owned by Chinese parent companies, have been alleged to be subject to Chinese laws and jurisdiction. It is unclear whether such a standard will be applied in the context of any final ICTS rule.

A "foreign adversary" is defined as "any foreign government or foreign non-government person" that is "engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security." Prohibitions and restrictions could therefore extend to products and services from specific companies and individuals, as well as specifically identified countries. While other recent regulatory developments provide indication of U.S. government concern about Chinese telecommunications companies, the proposed rule offers no guidance to the industry about the emergence or identification of foreign adversaries in the future.

- **The proposed process does not allow for parties to be proactive but may allow for negotiation.**

Commerce will notify parties to a transaction that an evaluation of a transaction is being conducted *and* that the Secretary has already reached a preliminary determination regarding the transaction. Within 30 days of this notification, the parties may submit an opposition to the preliminary determination or information on proposed measures for mitigation prior to a final determination from Commerce. The proposed rule's allowance for parties to propose mitigation measures may mirror the same process afforded to certain parties during CFIUS review, during which parties may negotiate with CFIUS to devise conditions to the transaction intended to mitigate any identified national security risks. Mitigation measures in the CFIUS context can take many forms, ranging from assurance letters, to agreements that impose governance requirements, to operational restrictions. Whether the proposed rule intended to create a similar platform for parties to negotiate with Commerce remains to be seen. What is clear, however, is that unlike the longstanding export licensing process or CFIUS review process, there is no avenue for parties to voluntarily submit a transaction for review and receive a determination that the transaction is approved. Consequently, parties may have already closed or executed a transaction before receiving notice from Commerce that the transaction must be unwound.

- **A significant, new interagency process will be developed.**

The Executive Order and proposed rule include a long list of agencies with which the Secretary of Commerce is to consult. The proposed rule references the involvement of nine agencies and offices, including the Departments of the Treasury, State, Defense, Justice, and Homeland Security, as well as the United States Trade Representative, the Director of National Intelligence, the General Services Administration, and the Federal Communications Commission.

* * *

In the current environment, it is easy to view the proposed rule through the lens of the ongoing bilateral negotiations between the United States and China and assume that the rule only targets acquisitions from certain Chinese ICTS suppliers. However, on its face the proposed rule lacks the clarity and guidance that most U.S. businesses need and expect to plan their activities, and it leaves more questions than answers. Commerce has invited comments on any aspect of the proposed rule. Parties that believe they could be affected by this new review process for ICTS transactions should strongly consider submitting comments to assist Commerce in narrowing or clarifying aspects of the rule.

You can subscribe to future ***International Trade & Regulatory*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Jason M. Waite
202.239.3455
jason.waite@alston.com

Kenneth G. Weigel
202.239.3431
ken.weigel@alston.com

Brian Frey
202.239.3067
brian.frey@alston.com

Helen Su
650.838.2032
helen.su@alston.com

Lucas Queiroz Pires
202.239.3235
lucas.queirozpires@alston.com

M. Jason Rhoades
202.239.3090
jason.rhoades@alston.com

Chunlian Yang
202.239.3490
lian.yang@alston.com

Helen Galloway
202.239.3794
helen.galloway@alston.com

John O'Hara
202.239.3131
john.ohara@alston.com

Yuzhe PengLing
202.239.3132
yuzhe.pengling@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 950 Page Mill Road ■ Palo Alto, California, USA 94304-1012 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333