DORSEY
DORSEY+WHITNEY LLP

New U.S. Government Review Process Effective March 22 for Information Communications Technology and Services from China, Russia and Other "Foreign Adversaries"

by Lawrence Ward, Rhona E. Schmidt, Justin T. Huff, Dave Townsend, and T. Augustine Lo

On January 19, 2021, one day before the transition to the new Biden Administration, the U.S. Department of Commerce published its interim final regulations ("Regulations") that will allow the United States to review, block, mitigate, or allow U.S. business transactions relating to any non-U.S.-supplied information communications technology and services (collectively, "ICTS"). Although the Biden Administration has ordered a temporary halt to review other pending regulations from the Trump Administration, that order did not include the Regulations, which are effective as of March 22. Given the potentially broad effects of the Regulations on industry, potentially affecting up to 4.5 million U.S. firms by the Commerce Department's own estimate, many observers had hoped the Biden Administration would at least delay implementation of the Regulations.

Under the Regulations, transactions for ICTS ("ICTS Transactions") within six categories of products and services (as explained below) and that involve a supplier associated with a "foreign adversary" will be subject to special scrutiny by the Commerce Department and are more likely to result in certain blocking or mitigation measures. Currently, the named foreign adversaries include China, Cuba, Iran, North Korea, Russia, and the government of Nicolas Maduro in Venezuela ("Maduro Regime").[1] However, the Commerce Department could add more countries to this list. The Regulations are designed to deter and limit U.S. companies from dealing with any such named foreign adversaries to obtain ICTS.

However, the scope of the Regulations is not limited only to foreign adversaries. As written, all ICTS Transactions within the six listed categories that involve any foreign interests are "covered" and are potentially subject to U.S. Government review. This broad scope is consistent with the Commerce Department's stated goal of addressing all potential risks to critical U.S. communications infrastructure from foreign sources, not just the risks posed by any identified foreign adversaries. Even if the Commerce Department decides not to take action because a foreign adversary is not involved, the new review process could lead to some delays for certain ICTS Transactions with foreign vendors. Even though the Regulations are effective as of March 22, 2021, the Regulations will

Related People

- Lawrence Ward
- Rhona E. Schmidt
- Justin T. Huff
- Dave Townsend
- T. Augustine Lo

Related Capabilities

- National Security Law
- Telecommunications
- Technology Commerce
- Technology
- Corporate Governance & Compliance
- Government Enforcement & Corporate Investigations
- Emerging Companies
- International Trade
- China

retroactively cover such transactions that were pending, initiated, or completed on or after January 19, 2021. Because of this broad scope, the Regulations could potentially impact U.S. companies (especially those that act as U.S. Government contractors) who rely on foreign suppliers in telecommunications, software-as-a-service ("SaaS") products and software development, cloud computing and hosting services, and other ICTS industries.

Recently confirmed Secretary of Commerce Gina Raimondo has not thus far ordered a suspension of the Regulations as of the date of this update. During her U.S. Senate confirmation hearing, Ms. Raimondo had promised to conduct a thorough review of the Regulations. That review will now apparently take place concurrently with a broader review of the U.S. ICTS supply chain ordered by President Biden on February 24 under Executive Order 14017. Given the multiple urgent challenges facing the Biden Administration, however, it is unclear how – and how far the Commerce Department will carry out the Regulations while the promised review is under way.

However, there are early indications that the Biden administration may take the Regulations seriously. On March 17, the Commerce Department announced that it had issued subpoenas to several Chinese companies for potential review of their ICTS products under the Regulations.

Rationale for Regulations.

In its January 19 publication, the Commerce Department stated the Regulations are necessary to safeguard any ICTS being used in the United States, which is "critical to nearly every aspect of U.S. national security." In particular, the Commerce Department cited ICTS supplied from foreign adversaries as potentially creating vulnerabilities to critical U.S. infrastructure, consumer data, healthcare networks and health data, sensitive personal data, and proprietary research and development. The Commerce Department contended that these potential vulnerabilities, if exploited by foreign adversaries, could undermine the confidentiality, integrity, and security of U.S. person data, allow covert data exfiltration to such foreign adversaries, and undermine the operation and profitability of U.S. businesses and critical infrastructure.

The Commerce Department issued the Regulations under Executive Order 13873 signed by President Trump on May 15, 2019 ("EO 13873"), which we summarized in the eUpdate. EO 13873 had declared a national emergency relating to ICTS and had authorized the Commerce Department to name foreign adversaries and to take action to block such ICTS transactions or impose mitigating measures on such transactions if the Department assessed that they could undermine or threaten U.S. national security. EO 13873 was predicated upon the International Emergency Economic Powers Act, the National Emergencies Act, and the President's authority under the U.S. Constitution.

Foreign Adversaries.

The Regulations expressly define a foreign adversary to be a foreign government or non-government entity that has engaged in long-term patterns of conduct adverse to U.S.

national security. The Regulations also state that the U.S. Government considers China, Cuba, Iran, North Korea, Russia, and the Maduro Regime in Venezuela to be such foreign adversaries. The Commerce Department can also designate additional foreign adversaries in the future based on information from U.S. intelligence, law enforcement, and national security agencies.

ICTS Transactions with any entity owned, controlled by, or subject to the jurisdiction of any such foreign adversary will be subject to heightened U.S. Government scrutiny under the Regulations. Such official scrutiny will extend to any of the following entities or individuals associated with a foreign adversary:

- Any person, wherever located, who acts as an agent, representative, or employee, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign adversary or of a person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary;
- Any person, wherever located, who is a citizen or resident of a nation-state controlled by a foreign adversary;
- Any corporation, partnership, association, or other organization organized under the laws of a nation-state controlled by a foreign adversary; or
- Any corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary

Covered ICTS Transactions.

The scope of the Regulations turns on several broadly defined terms. The Regulations will generally cover any ICTS Transaction that: (a) is pending, initiated, or completed on or after January 19, 2021; (b) has a U.S. nexus, (c) involves "any property in which any foreign country or a national thereof has an interest;" and (d) falls under one of six classes of such ICTS Transactions, as detailed below (each a "Covered ICTS Transaction"). Transactions that are intended to evade or avoid EO 13873 also are subject to the Regulations.

Under the Regulations, "ICTS" includes any hardware, software, or other product or service, including cloud-computing services, primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means (including electromagnetic, magnetic, and photonic), including through transmission, storage, or display. Further, under the regulations, "ICTS Transactions" include "any acquisition, importation, transfer, installation, dealing in, or use of any [ICTS], including ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download."

Under the Regulations, the six classes of goods and services are as follows:

Critical Infrastructure. ICTS used in critical infrastructure as identified in Presidential Policy Directive 21 – *Critical Infrastructure Security and Resilience* (2013).

Network Infrastructure. ICTS that are "integral" to networks and network infrastructure, including wireless local area networks ("WLAN"), mobile networks, cable, core networking systems, and satellite payloads and operation.

Sensitive Personal Data. ICTS that involve sensitive personal data of over one million U.S. persons at any point during the 12-month period before the ICTS Transaction, including internet hosting services and cloud based computing and storage.

Widely Distributed ICTS Hardware. Internet-enabled cameras or monitoring systems, home networking devices, routers, modems, and drones, if more than one million units have been sold to U.S. persons over the 12-month period before the ICTS Transaction.

Software for Widely Distributed ICTS Products. Software for Internet-based connection and communications that had over one million U.S. users at any point during the 12-month period before the ICTS Transaction, including desktop applications, mobile applications, gaming applications, and web-based applications.

Emerging Technologies. ICTS involving the following: artificial intelligence and machine learning, quantum key distribution, quantum computing, drones, autonomous systems, or advanced robotics.

The Commerce Department said that the Regulations do not provide categorical exemptions from the scope of covered ICTS Transactions because broader coverage should better mitigate the potential risks to U.S. national security posed by ICTS Transactions. However, the Regulations do provide some narrow carve-outs to reduce the potential burden on U.S. companies. First, ICTS Transactions authorized under U.S. Government-industrial security programs are not included. Second, any ICTS Transaction that is the subject of a pending or completed CFIUS review will not be included (but further ICTS Transactions by the parties after the CFIUS review could still be subject to the Regulations). Furthermore, in its narrative explanation of the Regulations, the Commerce Department stated as a matter of policy that "ICTS Transactions solely involving personal hardware devices, such as handsets, do not warrant particular scrutiny."

The Regulations also provide some affirmative examples of certain ICTS Transactions of particular concern. For example, although a U.S. company may have sourced software from China or Russia in the past, even a mere software update provided on or after January 19, 2021 from those locations "may provide a foreign adversary an opportunity to engage in the types of activities that may threaten U.S. national security." Citing this scenario, the Commerce Department justified its decision not to provide any exclusions for ICTS purchased before the Regulations came into effect.

Review Process for Covered ICTS Transactions.

The Regulations create a review process for the Commerce Department to consider and potentially block or impose mitigating measures relating to ICTS Transactions, which generally should be completed within 180 days. If the Commerce Department finds that

a Covered ICTS Transaction "involves ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary," and likely "poses an undue or unacceptable risk" to U.S. national security, the Commerce Department will begin interagency consultations with other U.S. Government agencies. If the Commerce Department confirms the existence of undue risk to national security and actions are necessary to eliminate or reduce that threat, it will then issue an initial determination setting forth the reasons and proposed prohibition or mitigation measures. Conversely, if the Commerce Department finds that a Covered ICTS Transaction does not involve a foreign adversary or does not otherwise pose a threat to U.S. national security, it may permit that transaction to move forward. If there is an adverse initial determination, the affected parties will have 30 days to respond. The Commerce Department then will conduct a second round of interagency consultations before issuing its final determination.

Under the Regulations, the Commerce Department can draw upon virtually any source of information that it deems appropriate to initiate an ICTS Transaction review and to reach its conclusion as to such transaction's potential risk to U.S. national security. The Regulations expressly provide that the Commerce Department may use information obtained from publicly available sources; U.S. intelligence, national security, and other federal agencies; parties to the transaction; U.S. state, local, or tribal governments; and foreign governments. The Commerce Department is also empowered by the Regulations to require information from the parties to an ICTS Transaction.

In theory, this new Commerce Department review process could have a significant impact on U.S. companies that purchase ICTS from foreign suppliers based in any of the specified foreign adversaries. However, because of the comprehensive sanctions administered by the Office of Foreign Assets Control ("OFAC") in the U.S. Department of the Treasury that already bar almost all U.S. person business or importation of "services" from Cuba, Iran, North Korea, or persons controlled by the Maduro Regime in Venezuela, in practical terms, the new Regulations will fall mostly on commercial ICTS Transactions involving ICTS suppliers in two foreign adversary countries, China and Russia.

Licensing of Covered ICTS Transactions.

The January 19 announcement from the Commerce Department also stated that it will issue additional detailed regulations ("Licensing Regulations") to create a pre-approval licensing process for ICTS Transactions within 60 days of the Regulations. The stated purpose of such a pre-approval mechanism in the Licensing Regulations is to mitigate the potential legal uncertainties, delays, and risks created by the Regulations for U.S. buyers of foreign-supplied ICTS. The Commerce Department said that the new process under the Licensing Regulations will be similar to the process used by the Committee on Foreign Investment in the United States ("CFIUS") to scrutinize foreign acquisitions of or investment in a U.S. business. Under the CFIUS Regulations in 31 CFR Part 800, parties can voluntarily disclose such a transaction to CFIUS, which then has a limited time to decide to whether to block, alter or allow a proposed acquisition of or investment

in a U.S. business to protect U.S. national security interests.

The Licensing Regulations will include criteria by which parties to an ICTS Transaction can seek such licenses from the Commerce Department. The Licensing Regulations will also create a fixed timeline of not longer than 120 days from acceptance of a license application to a Commerce Department decision on the disclosed transaction.

The strongest case for seeking a license under the Licensing Regulations will probably be a situation involving an ICTS vendor who is based in China or Russia, two of the named foreign adversaries in the Regulations, and where the parties to the transaction want to avoid any risk or uncertainty that the Commerce Department would unilaterally intervene in an ICTS Transaction of considerable value. By bringing such a transaction directly to the notice of the Commerce Department and triggering a review under the Licensing Regulations at the outset of a notified ICTS Transaction, at least in theory, the parties should be able to preempt such an intervention and avoid any later delay or disruption of that transaction under the Regulations. However, depending on how broadly the Commerce Department plans to interpret what will be considered Covered ICTS Transactions under the Regulations, there could also potentially be some circumstances to invoke that licensing mechanism even when neither China nor Russia is involved.

Conclusion.

Given their breadth and potentially severe impact on certain transactions, the Regulations are probably going to create a degree of palpable uncertainty for U.S. businesses that rely on global supply chains and foreign outsourcing, particularly in the telecommunications, home devices, and SaaS sectors (e.g., devices that will be connected to one another as part of the “Internet of Things” (“IOT”)). Because IoT and many other technology sectors are so dependent upon computer software, many U.S. companies have come to rely on specialized outsourcing providers to develop such computer software. Consequently, the global outsourcing provider industry has grown significantly over the past two decades. Many of the largest outsourcing providers have substantial U.S. offices but are ultimately owned and controlled by parent entities in countries outside the United States, such as in India, China, Brazil, the Philippines, Russia, and elsewhere in eastern Europe.

A U.S. purchaser of ICTS will probably now need to conduct a new sort of due diligence when it selects any outside ICTS provider, even if that ICTS provider nominally appears to be a U.S. entity (e.g., the U.S. subsidiary of a foreign-based outsourcing parent company). If the provider’s U.S. office is only serving as a convenient “face” for its foreign-based parent entity, and particularly if the bulk of the ICTS is actually to be provided by personnel of that foreign-based parent entity or any other foreign-based affiliate, a U.S. ICTS purchaser should know about that structure and should then take both that structure and the Regulations into account when considering whether to engage such a foreign-based ICTS provider.

The new Commerce Department review is clearly targeted at any ICTS sourced from

China, Russia, and the other named foreign adversaries. For example, a company that imports Chinese-origin products used for information or IoT communications might need to seek a Commerce Department license, or else it could otherwise risk that the Commerce Department might deem the importation of such ICTS as being contrary to U.S. national security interests and thus be prohibited. Likewise, a U.S. company that uses contractors in China or Russia for certain ICTS such as data hosting or software support could face risks under the Regulations. As with the CFIUS regime, such a U.S. ICTS purchaser may make its business more reliable and predictable either by avoiding the use of such an ICTS supplier in a foreign adversary jurisdiction or, if it has a compelling reason to do so, then by seeking a Commerce Department license under the forthcoming Licensing Regulations. Failure to get such a license would risk that the Commerce Department could instead initiate its own later review and subsequently order an unwinding or reversal of an ICTS Transaction.

Moreover, U.S. ICTS purchasers will likely also want now to review and revise their "boilerplate" *force majeure* clauses that might now only refer to "export control" and "economic sanctions" laws and regulations. Here, under the Regulations, the U.S. Government is imposing for the first time controls on the "*import*" or purchase of ICTS in the United States. Most such standard clauses in common U.S. contractual usage have not had to deal with regulatory barriers on "imports" or "services" that could affect dealing with foreign vendors in such a novel way.

Finally, U.S. ICTS purchasers and foreign ICTS vendors will want to watch carefully as the Commerce Department completes its promised review of the Regulations, including the various public comments that have been sent in, and to examine the new proposed Licensing Regulations that should be due out for public comment soon. U.S. ICTS purchasers also should pay close attention to any further developments with respect to the subpoenas issued to Chinese companies on March 17 under the Regulations. As they monitor these legal developments, U.S. ICTS purchasers may also want to begin consideration of alternative foreign ICTS vendors who will offer a lower risk profile in terms of potential negative outcomes, such as vendors who are clearly and unequivocally not connected to any of the named foreign adversary countries, most especially to China or Russia. Foreign ICTS vendors, especially those in the designated foreign adversary countries, will also have to be prepared for more rigorous due diligence requests from their U.S. clients and to be prepared to undergo the Commerce Department's scrutiny in line with the new Licensing Regulations, much as foreign investors have gradually but firmly adjusted to the reality of CFIUS national security reviews in the case of foreign investments or acquisitions in the United States.

# # # # #

Dorsey & Whitney's National Security Group can assist companies with reviewing and analyzing the Regulations and, when issued, the Licensing Regulations, and their impact on any proposed ICTS Transaction. Lawyers in Dorsey's National Security Group have had decades of experience helping companies with complex national security related matters, including licenses from the Commerce Department and other approvals from

CFIUS.

[1] Consistent with the U.S. Government's refusal to recognize Nicolas Maduro as the legitimate president of Venezuela, the Regulations deem the Maduro Regime but not all of Venezuela as a foreign adversary.