LEGAL UPDATES

PUBLISHED: JANUARY 20, 2021

Commerce Department Publishes Interim Final ICTS "Foreign Adversary" Rules

Key Point: New rules will impact the use of equipment and digital services sourced from China and other “foreign adversaries” in a wide variety of transactions and activities that potentially pose a risk to U.S. national security.

Overview

On January 19, 2021, the U.S. Department of Commerce (Commerce) published a long-awaited interim final rule to address the use of goods or services sourced from “foreign adversaries” in the U.S. supply chain for information communications technology and services (ICTS) transactions. When the interim final rule (ICTS Rules) take effect on March 20, 2021, they will enable the U.S. Secretary of Commerce (the Secretary) to block any ICTS transaction involving goods or services designed, developed, manufactured or supplied from “foreign adversaries” or companies organized in a “foreign adversary” country, conducting operations in a “foreign adversary” country or otherwise subject to the direction or control of a “foreign adversary.” These rules will have especially broad application, but Commerce has also indicated that it will continue to accept comments on the rules for the next 60 days. Commerce will also publish procedures for a “safe harbor” licensing program within the next 60 days and will then implement that licensing program within the next 120 days. Therefore, concerned parties still have an opportunity to submit feedback on the ICTS Rules and also have some remaining time to evaluate whether their transactions or activities might require licensing from Commerce.

Background

Services

Artificial Intelligence

CFIUS

Data Privacy & Cybersecurity

International Trade & Supply Chain

Industry

Technology

Professionals

CORTNEY O'TOOLE MORGAN
WASHINGTON: 202.378.2389
CORTNEY.MORGAN@HUSCHBLACKWELL.COM

GRANT D. LEACH
OMAHA: 402.964.5143
GRANT.LEACH@HUSCHBLACKWELL.COM

The ICTS Rules are required under Executive Order 13873 (EO 13873), which President Trump issued on May 15, 2019, in order to prohibit the U.S. ICTS sector from using goods or services sourced from "foreign adversaries" in transactions with the potential to harm U.S. national security, U.S. critical infrastructure or the U.S. digital economy. Commerce previously issued a proposed version of the ICTS Rules in November 2019 and asked for public comments on those rules. Those comments were originally due on December 27, 2019, but Commerce then extended the comment period until January 10, 2020. Commerce has since considered those comments and made modifications to those previous proposed rules in order to arrive at yesterday's interim final ICTS Rules, which will take effect in their current form on March 20, 2021, but which are also subject to a comment period for the next 60 days. After that comment period expires, Commerce has committed to issue a "subsequent final" version of the ICTS Rules, in which Commerce will address additional comments received during this comment period.

What is the Justification for the ICTS Rules?

EO 13873 observed that "foreign adversaries are increasingly creating and exploiting vulnerabilities in [ICTS], which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people." The January 19, 2021, Federal Register notice explains that "[s]ome foreign adversaries are known to exploit the sale of software and hardware to introduce vulnerabilities that can allow them to steal critical intellectual property, research results (e.g., health data), or government or financial information from users of the software or hardware." Commerce also noted the "widespread use of some consumer devices, networked surveillance, cameras, drones, or interconnection via the internet of computing devices embedded in every day objects" which provide foreign adversaries with the opportunity to collect "swaths of sensitive personal data" which they could use to conduct corporate espionage or compile information for blackmailing purposes.

What Types of Transactions Are Subject to the ICTS Rules?

The ICTS Rules define an "ICTS transaction" as "any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download." However, the ICTS Rules limit the Commerce Secretary's blocking authority to only the following specific types of ICTS transactions:

ICTS transactions in any of the 16 sectors identified in Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience (which consist of the chemical sector, commercial facilities sector, communications sector, critical manufacturing sector, dams sector, defense industrial base

sector, emergency services sector, energy sector, financial services sector, food and agriculture sector, government facilities sector, healthcare and public health sector, information technology sector, nuclear reactors, materials and waste sector, transportation systems sector and water and wastewater systems sector);

ICTS transactions involving a wide variety of specifically identified software, hardware and other products or services integral to data networks and data transmission systems;

ICTS transactions involving products or services for the use, process or retention of "sensitive personal data" on greater than 1 million U.S. persons;

ICTS transactions involving internet-enabled sensors, webcams, and any other end-point surveillance or monitoring device, home networking devices and drones and other unmanned aerial systems if greater than 1 million units have been sold to U.S. persons;

ICTS transactions involving software designed primarily for internet communications such as desktop applications, mobile applications, gaming applications and web-based applications if they are in use by over 1 million U.S. persons; and

ICTS transactions involving artificial intelligence and machine learning, quantum key distribution, quantum computing, drones, autonomous systems or advanced robotics.

Under the third bullet point listed above, "sensitive personal data" consists of: financial data that could indicate an individual's financial distress or hardship, consumer credit reporting data, data sets used in various insurance applications, data relating to an individual's physical, mental, or psychological health condition, private electronic communications such as e-mail, messaging or chat communications, geolocation data, biometric enrollment data (including facial, voice, retina/iris and palm/fingerprint templates), data used for issuing government identification cards, data concerning U.S. government security clearances, and genetic information.

The ICTS rules specifically exempt ICTS transactions that have been authorized under a U.S. government-industrial security program and transactions that are under active review or have been reviewed by the Committee on Foreign Investment in the United States (CFIUS) in connection with the foreign acquisition of a U.S. business or U.S. real estate. However, that CFIUS exemption is not available if the ICTS transaction is distinct from or subsequent to the CFIUS-reviewed transaction.

Who are "Foreign Adversaries" and "Persons Owned By, Controlled by or Subject to the Jurisdiction or Direction of a Foreign Adversary" under the ICTS Rules?

Commerce has identified China (including Hong Kong), Cuba, Iran, North Korea and Russia as "foreign adversary" countries and has also identified acting Venezuelan president Nicolas Maduro individually as a "foreign adversary."

The ICTS Rules define a "person owned by, controlled by, or subject to the jurisdiction of a foreign adversary" as:

any person, who acts as an agent, representative, or employee, or any person otherwise acting at the order, request, or under the direction or control, of a foreign adversary;

any 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 business entity organized under the laws of a nation-state controlled by a foreign adversary; and

any business entity, wherever located, that is owned or controlled by a foreign adversary.

As discussed below, this definition will extend the ICTS Rules' coverage to many ICTS industry supply chains.

What Types of Transactions or Activities are Likely to be Blocked or Restricted Under the ICTS Rules?

The following factors may determine whether an ICTS transaction "involves ICTS designed, developed, manufactured, or supplied, by a person owned by, controlled by, or subject to the jurisdiction of a foreign adversary," which will potentially subject the transaction to blocking under the ICTS Rules:

Whether the person or its suppliers have headquarters, research, development, manufacturing, test, distribution, service facilities or other operations in a foreign country, including one controlled by, or subject to the jurisdiction of, a foreign adversary;

Whether any ties exist between that person and a foreign adversary. For business entities, this includes ties between their officers, directors, employees, consultants or contractors and a business entity;

Laws and regulations of any foreign adversary country in which a person is headquartered or conducts operations, including research and development, manufacturing, packaging and distribution; and

Any other criteria that the Secretary deems appropriate.

As a result, transactions or activities involving suppliers that are domiciled in what would otherwise be considered friendly countries could still be subject to the ICTS Rules if those suppliers or their personnel have operations in or other connections to foreign adversary countries.

However, even if an ICTS transaction meets the above criteria, the ICTS Rules also require that the transaction must present an "undue or unacceptable risk" before the Secretary will be entitled to block the transaction. The ICTS Rules and EO 13873 define an "undue or unacceptable risk" as: (i) an undue risk of sabotage to or subversion of the U.S. ICTS sector, (ii) an undue risk of catastrophic effects on the security or resiliency of U.S. critical infrastructure or the U.S. digital economy, or (iii) an unacceptable risk to U.S. national security or the security and safety of U.S. persons. The ICTS Rules require the Secretary to consider seven specific factors when considering whether a transaction presents an "undue or unacceptable risk." Those factors include threat assessments issued by agencies such as the Office of the Director of National Intelligence, Department of Homeland Security and the Department of Defense and a general consideration of "the nature, degree, and likelihood of consequence to the United States public and private sectors that could occur if ICTS vulnerabilities were to be exploited."

What Process Will the Secretary Use for Applying the ICTS Rules?

The Secretary's review process under the ICTS Rules consists of a referral, an initial review, a first interagency consultation, an initial determination, a second interagency consultation and a final determination. The Secretary may abandon its review of a transaction at various points in this process, but it will retain the right to conduct further review if additional information becomes available. Certain stages require that the Secretary consult with "appropriate agency heads" which consist of the Secretary of the Treasury, Secretary of State, Secretary of Defense, Attorney General, Secretary of Homeland Security, U.S. Trade Representative, Director of National Intelligence, Administrator of General Services, Chairman of the Federal Communications Commission and the heads of any other federal departments or agencies that the Secretary may determine to be appropriate. Throughout the review process the Secretary also enjoys broad authority to seek additional information from transaction parties and the ICTS Rules require transaction parties to comply with any such request.

It appears that the referral, initial review and first interagency consultation stages will have the potential to blur together in practice. During those stages, the ICTS Rules do not require Commerce to

provide companies with any notice that their transactions are under review. Instead, transaction parties are only first entitled to receive notice if the review advances beyond the first interagency consultation and results in an initial determination by the Secretary and the appropriate agency heads that the transaction presents an "undue or unacceptable risk." In that instance, the Secretary will issue an initial written determination which will explain why the transaction is subject to the ICTS Rules and set forth the Secretary's initial determination to either prohibit the transaction or to require that the parties adopt mitigation measures in order to continue with the transaction. The Secretary has the option to notify the parties to a transaction of this initial determination by serving them a copy privately or by publishing the initial determination in the Federal Register.

After the Secretary serves an initial determination notice, the parties to an affected transaction have 30 days to protest the Secretary's determination or propose alternative remedial measures. If the parties submit such a response, then the Secretary shall then conduct a "second interagency consultation" with the appropriate agency heads and attempt to reach a consensus as to whether the transaction should be prohibited, permitted or permitted only pursuant to the adoption of negotiated mitigation measures. If the Secretary and the appropriate agency heads can reach a consensus decision, then they will issue that decision as a "final determination." If they cannot reach a consensus, then the Secretary will refer the transaction to the President and will then issue a final determination according to direction received from the President. All final determinations will be sent to the transaction participants and if the final determination results in a decision to prohibit the transaction then the Secretary will also publish a summary of the final determination result in the Federal Register with any confidential business information omitted.

To the extent that a reviewed transaction will warrant a final determination, the ICTS Rules require the Secretary to issue that final determination within 180 days of commencing its initial review of the transaction. However, the Secretary may unilaterally extend that deadline by making a written determination that additional time is necessary.

How Will the Licensing Program Function Under the ICTS Rules?

Commerce intends to offer a process whereby it will issue licenses for proposed, pending or ongoing ICTS transactions that are "consistent with the national security of the United States." Congress intends to publish these licensing procedures no later than March 20, 2021 (the date occurring 60 days after the Federal Register notice) and will then begin administering the licensing program and accepting license applications no later than May 19, 2021 (the date occurring 120 days after the Federal Register notice). Commerce has announced that it will administer this licensing program on a fixed timeline and will issue licensing decisions within 120 days after accepting a license application. If Commerce does not issue a license decision within that 120-day period, then the application will be deemed granted. Interested parties should be aware that Commerce has a history of missing deadlines

under EO 13873. EO 13873 originally required Commerce to publish the ICTS Rules no later than October 14, 2019, and yesterday's announcement arrives 463 days past that initial deadline. Therefore, if past practices are any indication, some of the ICTS Rules' cut-off dates should be viewed as optimistic targets rather than hard-and-fast deadlines.

Are the ICTS Rules Likely to Change Once the Biden Administration Takes Office?

Commerce published the ICTS Rules on President Trump's second-to-last day in office. Because the ICTS Rules are authorized under EO 13873, President-Elect Biden could theoretically revoke EO 13873 after assuming office and thereby also invalidate the ICTS Rules. However, the ICTS Rules are consistent with several national security initiatives which predate the Trump Administration and we therefore believe it is unlikely that President-Elect Biden will completely revoke the ICTS Rules. Instead, if the Biden Administration does object to the ICTS Rules, we believe that it is much more likely to address those concerns through the forthcoming licensing process or through modifications to the ICTS Rules which could be made after the final comment period concludes. Alternatively, because the ICTS Rules' transaction review process will largely take place outside of the public view, it is also possible that the incoming Biden Administration could choose to leave the ICTS Rules intact while implementing its desired policy objectives behind the scenes through enforcement directives issued to Commerce and the other appropriate agency heads. Considering Commerce's past delays in implementing these rules and the ICTS Rules' short turnaround times for concluding the comment period and establishing the required licensing program, it's also possible that the Biden Administration could take limited action to delay the ICTS Rules' effective date or to extend some of their deadlines while it considers the ICTS Rules' more substantive provisions.

What Should I Be Doing to Prepare for These Rules?

If companies have specific concerns about the ICTS Rules, then they should consider submitting a comment before the comment period expires on March 20, 2021. Otherwise, companies engaged in the specific types of transactions that are covered by the ICTS Rules should begin reviewing their supply chains to determine whether any of their suppliers (or their suppliers' suppliers) might qualify as "persons owned by, controlled by or subject to the jurisdiction or direction of a foreign adversary." Although there is still significant uncertainty around the final form that the ICTS Rules will eventually take and how Commerce will enforce them, companies can at least give themselves a head start by analyzing whether and to what extent the current ICTS Rules might apply to them and whether vendors in their ICTS supply chain might potentially trigger blocking under the current version of the ICTS Rules. By proactively identifying those affected transactions and vendors, companies will be in a better position to apply for licenses (if appropriate) or to adjust their ICTS supply chain (if necessary).

Contact Us

Husch Blackwell's International Trade & Supply Chain team is closely monitoring the development and implications of these ICTS Rules. If you have questions please contact Cortney O'Toole Morgan or Grant D. Leach.