International Trade Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Biden Administration Reviewing Comments on Interim Final ICTS Rule

February 5, 2021

Key Points

- On January 19, 2021, the U.S. Commerce Department published an interim final rule (IFR) to implement Executive Order 13873 of May 15, 2019, on "Securing the Information and Communications Technology and Services Supply Chain" (ICTS EO). The IFR follows Commerce's proposed rule on the same subject, published November 27, 2019, which spurred broad industry commentary on the scope and jurisdiction of the proposed rule.
- The IFR does not impose any immediate prohibitions. Rather, the rule creates a broad framework for the Commerce Department to identify, mitigate, prohibit or unwind covered "ICTS Transactions" involving "foreign adversaries" that pose an undue or unacceptable risk to U.S. national security.
- Importantly, the IFR designated China (including Hong Kong), Cuba, Iran, North Korea, Russia and Venezuela's Maduro regime as "foreign adversaries." This list may evolve in the future.
- The IFR limits the scope of covered transactions to a stated—albeit expansive—list of ICTS products and scenarios, previews the establishment of a "pre-clearance" licensing mechanism and, with some limitations, exempts transactions that Committee on Foreign Investment in the United States (CFIUS) is actively reviewing or has reviewed.
- The rule is effective March 22, 2021. The IFR also seeks industry comments—also due March 22, 2021—which will be used to inform a potential final rule. However, the Biden administration has initiated a review of recent regulatory actions and is assessing its approach on national security and supply chain issues, including the IFR. It remains to be seen whether the Biden administration will alter, revoke or delay the IFR prior to March 22.

Contact Information

If you have any questions concerning this alert, please contact:

Shiva Aminian
Partner
saminian@akingump.com
Los Angeles
+1 310.552.6476

Christian C. Davis
Partner
chdavis@akingump.com
Washington, D.C.
+1 202.887.4529

Hal S. Shapiro
Partner
hshapiro@akingump.com
Washington, D.C.
+1 202.887.4053

Thomas J. McCarthy
Partner
tmccarthy@akingump.com
Washington, D.C.
+1 202.887.4047

Jaelyn Edwards Judelson
Partner
jjudelson@akingump.com
Los Angeles
+1 310.552.6477

Clete R. Willems
Partner
cwillems@akingump.com
Washington, D.C.
+1 202.887.4125

Jonathan C. Poling
Partner
jpoling@akingump.com
Washington, D.C.
+1 202.887.4029

Background

As described in our earlier May 2019 and December 2019 publications on this topic, on May 15, 2019, President Trump issued Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain (the ICTS EO), citing his authority under the International Emergency Economic Powers Act (IEEPA), among other laws. IEEPA allows the President to take actions against any unusual and extraordinary foreign threat to the national security, foreign policy or economy of the United States upon the President's declaration of a national emergency with respect to that threat. In the ICTS EO, the President declared a national emergency with respect to the ability of "foreign adversaries" to create and exploit vulnerabilities in information and communications technology and services in order to commit "malicious cyber-enabled actions."

Interim Final Rule Scope and Procedural Changes

On November 27, 2019, Commerce published a proposed rule to implement the ICTS EO. This rule prompted dozens of comments from companies and associations around the world, many of which criticized the potential scope of the rule and encouraged Commerce to significantly revamp the rule, or even to forego it entirely.

On January 19, 2021, Commerce issued its interim final rule (IFR) to implement the ICTS EO, identifying the processes and procedures that the Secretary of Commerce will use to review and identify prohibited transactions. The IFR generally retains the structure and broad scope of the proposed rule, though it departs from, and narrows, the initial proposal in several important respects. The IFR is set to take effect on March 22, 2021, with a proposed licensing process intended to be in place within 120 days (i.e., May 19, 2021). This timeline is subject to change depending on how the Biden administration chooses to implement this rule, if at all.

A. Scope

The IFR does not categorically prohibit or require a license for any specific activity. Rather, the rule authorizes the Secretary of Commerce, on a case-by-case-basis, to identify, mitigate, prohibit and/or unwind (i) covered "ICTS Transactions" (ii) that involve "ICTS designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a 'foreign adversary'" and (iii), which pose an undue or unacceptable risk. We discuss these concepts further below.

1. ICTS and Covered ICTS Transactions

ICTS means "information and communications technology and services" and includes those products and services that U.S. businesses, governments and consumers use for communications and data transmission, and storage such as cloud and network management services, landline and wireless networks, networked devices (e.g., from drones to mobile phones and Internet-connected household consumer goods) and software that enables those devices and services. The IFR refines the proposed rule's definition of ICTS by noting that it includes "cloud-computing services" and that "electronic means" includes electromagnetic, magnetic and photonic.

To establish the scope of this rule, the IFR creates a new defined term "ICTS Transaction," which means "any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service, including

Kevin J. Wolf
Partner
kwolf@akingump.com
Washington, D.C.
+1 202.887.4051

Robert J. Monjay
Senior Counsel
rmonjay@akingump.com
Washington, D.C.
+1 202.887.4557

Katherine P. Padgett
Counsel
kpadgett@akingump.com
Washington, D.C.
+1 202.887.4079

Ursula R. Rothrock
Associate
urothrock@akingump.com
Los Angeles
+1 310.229.1077

Stephana J. Henry
Associate
shenry@akingump.com
Washington, D.C.
+1 202.887.4546

Chris Chamberlain
Associate
cchamberlain@akingump.com
Washington, D.C.
+1 202.887.4308

Nick Russell
Law Clerk
(not admitted to practice)
nrussell@akingump.com
Washington, D.C.
+1 202.887.4542

ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download." The definition also now includes any other transaction, the structure of which is designed or intended to evade or circumvent the ICTS EO.

Under the IFR, an ICTS Transaction is only "covered" (i.e., potentially within the scope of the IFR) if it:

1. Is conducted by any person subject to the jurisdiction of the United States or involves property subject to the jurisdiction of the United States.
2. Involves any property in which any foreign country or a national thereof has an interest (including through an interest in a contract for the provision of the technology or service).
3. Is initiated, pending or completed on or after January 19, 2021. The proposed rule would have applied to transactions initiated, pending or completed after May 15, 2019, when the ICTS EO was published. Under the IFR, however, only ICTS Transactions that are initiated, pending or completed on or after January 19, 2021 (i.e., the date of publication in the Federal Register) will be subject to these new rules. Still, any subsequent related "act or service" counts as an ICTS Transaction on the date the act or service is performed. As examples of such an "act or service," the IFR cites "execution of any provision of a managed services contract or installation of software updates" regardless of when the contract was entered into.
4. Involves one of the six enumerated ICTS categories. These are:

ICTS Category	Description
Critical Infrastructure	"ICTS that will be used by a party to a transaction in a sector designated as critical infrastructure by Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience, including any subsectors or subsequently designated sectors." The IFR defines a "party or parties to a transaction" to mean a person engaged in an ICTS Transaction, which includes the person "acquiring" the ICTS and the person "from whom the ICTS is acquired," as well as any parties engaging in ICTS Transactions "with the intention" of evading the regulations. However, "parties to a transaction" do not include common carriers transporting ICTS goods, unless they know, or should have known, they were providing transportation services related to a prohibited transaction.
Networking	"Software, hardware, or any other product or service integral to" any of the following (which are accompanied by numerous examples in the IFR): • Wireless local area networks • Mobile networks • Satellite payloads • Satellite operations and control

	• Cable access points • Wireline access point • Core networking systems • Long- and short-haul networks.
Hosting and Storage of Sensitive Personal Data	"Software, hardware, or any other product or service integral to data hosting or computing services, to include software-defined services such as virtual private servers, that uses, processes, or retains, or is expected to use, process, or retain, **sensitive personal data** on greater than one million U.S. persons at any point over the twelve (12) months preceding an ICTS Transaction, including": Internet hosting services, cloud-based or distributed computing and data storage, managed services and content delivery services. The IFR defines the term "sensitive personal data" to mean specified categories of "personally identifiable information" (PII) or "genetic information." The categories of PII track the same PII categories included in the definition of "sensitive personal data" in the Committee on Foreign Investment in the United States (CFIUS) regulations (see 31 C.F.R. section 800.241).
Widely Sold Surveillance, Monitoring, or Networking Devices	Any of the following ICTS products, if greater than one million units, have been sold to U.S. persons at any point over the 12 months prior to an ICTS Transaction: • Internet-enabled sensors, webcams and any other end-point surveillance or monitoring device • Routers, modems and any other home networking device • Drones or any other unmanned aerial system.
Widely Used Internet Communications Applications	Software designed primarily for connecting with and communicating via the Internet that is in use by greater than one million U.S. persons at any point over the 12 months preceding an ICTS Transaction (e.g., desktop applications, mobile applications, gaming applications and web-based applications).
Emerging Technologies	ICTS integral to: artificial intelligence and machine learning, quantum key distribution, quantum computing, drones, autonomous systems or advanced robotics.

2. ICTS designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a "foreign adversary."

As noted above, the Secretary of Commerce can only mitigate, prohibit and/or unwind a "Covered "ICTS Transaction" that involve "ICTS designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a 'foreign adversary.'" The ICTS EO defined "foreign adversaries" as "any foreign government or foreign 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." The ICTS EO and proposed rule did not actually designate any such countries, persons or entities as foreign adversaries.

In a move to provide greater specificity, the IFR designates the following countries and regimes as "foreign adversaries" for purposes of this framework:

- China (including Hong Kong)
- Cuba
- Iran
- North Korea
- Russia
- The Maduro regime in Venezuela.

Furthermore, IFR explains that when assessing whether an ICTS Transaction involves any ICTS that has been designed, developed, manufactured or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries, Commerce will consider the following factors:

- Whether the party or its component suppliers have headquarters, research, development, manufacturing, test, distribution, or service facilities or other operations in a foreign country, including one controlled by a foreign adversary.
- Personal and professional ties between the party—including its officers, directors or similar officials, employees, consultants or contractors—and any foreign adversary.
- Laws and regulations of the foreign adversary in which the party is headquartered or conducts operations, including research and development, manufacturing, packaging and distribution.
- Any other criteria that the Secretary deems appropriate.

Along those lines, the focus of the foreign adversary analysis is on the ICTS itself rather than the parties to the transaction.

3. Undue or Unacceptable Risk

If a Covered ICTS transaction meets the criteria described above, Commerce must determine that the transaction poses an "undue or unacceptable risk" before taking action to mitigate, prohibit and or unwind it. The IFR defines this standard, consistent with the ICTS EO, as follows:

- An undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of ICTS **in the United States**.
- An undue risk of catastrophic effects on the security or resiliency of the **United States critical infrastructure** or the digital economy of the United States.
- Or, an unacceptable risk to the national security of the United States or the security and safety of United States persons.

4. Exclusions and Limitations

CFIUS Overlap – In a significant departure from the proposed rule, the IFR exempts ICTS Transactions that CFIUS is actively reviewing, or that CFIUS has already

reviewed. The IFR cautions, however, that this exemption does not preclude Commerce from reviewing a subsequent ICTS Transaction if it is distinct from the previously CFIUS-reviewed transaction or if new information about the transaction is discovered.

Additional Exclusions – The IFR notes that "personal ICTS hardware devices, such as handsets, do not warrant particular scrutiny," so they are not incorporated into the six categories of covered ICTS. Additionally, unlike in the proposed rule, the IFR does not apply to the acquisition of ICTS items by a United States person as a party to a transaction authorized under a "U.S. government-industrial security program." Although the IFR does not define the term "U.S. government-industrial security program," it likely includes the National Industrial Security Program, a Department of Defense program that helps federal agencies safeguard classified information that is released to federal contractors, licensees and grantees. Finally, as a function of review factors discussed further below, the IFR does not generally capture common carriers transporting ICTS goods, unless they know, or should have known, they were providing transportation services related to prohibited transactions.

B. Procedural Changes

1. Licensing Mechanism

Significantly, the IFR announces that Commerce is developing a pre-clearance licensing mechanism for potentially covered transactions, consistent with section 2(b) of the ICTS EO. Commerce intends to publish additional regulations on procedures for applying for a license before March 22, 2021, with implementation intended to begin within 120 days (i.e., May 19, 2021). However, applying for a license is completely optional. Parties will not create a negative inference or unfavorable presumption with respect to a transaction for not seeking pre-approval.

The IFR previews that the published procedures will establish criteria for seeking a license, including that license applications will be reviewed within 120 days or the license will be deemed granted.

Again, the Biden administration's review and reassessment of the IFR renders this timeline subject to change.

2. Procedures and Factors for Initiation, Evaluation and Determination of Prohibited Transactions

After determining that (1) the transaction is a "Covered ICTS Transaction," as defined above, and (2) the 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, Commerce may commence an initial review of a transaction and assess if it poses an undue or unacceptable risk requiring prohibition or mitigation. The Secretary's assessment will be guided by considerations such as the market share and technical capabilities of the ICTS product or service at issue, the degree of influence the foreign adversary has over the design, manufacture and supply of the ICTS product or service, and the nature of the vulnerability and degree of threat implicated by the ICTS Transaction.

Parties to a transaction under review will only be informed that the Secretary is reviewing their transaction and that it should be prohibited or requires mitigation when

they are provided copies of Commerce's initial written determination explaining its rationale. The parties will then have 30 days to respond to the initial written determination. Following consideration of the parties' submissions and further interagency consultations, and within 180 days of accepting the referral and commencing its initial review, the Secretary will make a final determination as to whether the ICTS Transaction is: (1) prohibited; (2) not prohibited; or (3) permitted pursuant to the adoption of negotiated mitigation measures. Final determinations are to be published in the Federal Register, omitting any confidential business information.

Opportunity to Comment on the IFR

According to the IFR, interested parties may submit comments on the IFR on or before March 22, 2021, via the Federal eRulemaking Portal or by emailing ICTsupplychain@doc.gov. Because the Biden administration is actively reconsidering the IFR, any interested parties should consider filing public comment to influence the administration's decision on how to proceed with implementation of the rule.

Conclusion

The implementation of the ICTS EO laid out in the IFR creates uncertainty with respect to many transactions involving the ICTS sector and bestows broad authority on Commerce to review and prohibit ICTS-related transactions. Companies will have limited information to identify potentially relevant national security concerns or to know when they are triggered. Given the broad implications and the fact that the Biden administration is reconsidering this rule, we recommend that affected parties carefully consider the implications on their business and whether to submit public comments in order to influence that review.

akingump.com