January 27, 2021

Commerce Publishes Information and Communications Technology and Services (ICTS) Interim Rule in the Final Days of the Trump Administration

On January 14, 2021, the U.S. Department of Commerce ("Commerce") announced that it had issued an interim final rule (the "Rule") to implement President Trump's Information and Communications Technology and Services ("ICTS") Executive Order of May 2019,[1] which was aimed at threats posed to U.S. national security and the U.S. digital economy by the involvement of certain non-U.S. technology providers from "foreign adversary" jurisdictions in the U.S. ICTS supply chain.[2] Commerce had previously issued a proposed rule to implement the ICTS Executive Order in late 2019, but ultimately withdrew the proposed rule after significant comments from U.S. industry. The Rule is one of a series of actions targeting China and its tech sector that the Trump Administration took in its final days. Relying on the International Emergency Economic Powers Act ("IEEPA"), the President's primary economic sanctions authority, the Rule empowers Commerce to review—and prohibit or impose mitigation on—a range of technology products and services transactions involving U.S. companies and ICTS designed, developed, manufactured, or supplied by Chinese companies, among others.

The Rule states that it will take effect 60 days after its publication in the *Federal Register* on January 19, 2021 (*i.e.*, on March 22, 2021), and asks the public to provide further comments on the Rule prior to its effective date. The Rule, however, appears to be captured by the Biden Administration's rulemaking "freeze" order,[3] meaning that the Rule's effective date could be delayed. More generally, it is currently unclear whether or how the Biden Administration will continue to move forward with implementing the Rule, particularly given U.S. industry's significant opposition to the ICTS initiative to date for, among other things, casting significant uncertainty over U.S. companies' transactions with Chinese ICTS providers. During a recent Senate confirmation hearing, Commerce Secretary-Designate Gina Raimondo stated that she would "use the full toolkit at my disposal. . .to protect Americans and our network from Chinese interference or any kind of backdoor influence into our network."[4] However, at another point in the hearing, Raimondo declined to commit to continue keeping Huawei and other Chinese companies on the Entity List going forward.[5]

The Rule also states that it is generally focused on purchases of or dealings in ICTS and that investments by non-U.S. persons in U.S. businesses or U.S. real estate is still the province of the Committee on Foreign Investment in the United States ("CFIUS"). Notifying an investment by a non-U.S. person to CFIUS and obtaining CFIUS "safe harbor" will not, however, insulate the parties from a future Commerce ICTS review

with respect to ICTS-related transactions or dealings by the parties that are beyond the scope of an investment previously notified to CFIUS.

If the Rule does come into effect, it would provide Commerce with very broad authority to review—and, with broad discretion, to prohibit or impose mitigation on—a range of transactions involving ICTS products and services (which themselves are also broadly defined in the Rule to include a variety of hardware, software, apps, internet hosting services, and cloud-based computing services, as well as products and services related to local area networks, mobile networks, and core networking systems). The Rule applies to U.S. transactions involving ICTS that is "designed, developed, manufactured, or supplied by" persons (individuals and entities) who are subject to the jurisdiction of six designated "foreign adversaries" for purposes of the Rule: China, Cuba, Iran, North Korea, Russia, and the Maduro regime in Venezuela. Covered ICTS transactions that are initiated, pending, or completed on or after the date of the Rule's publication in the *Federal Register* (*i.e.*, January 19, 2021) would be subject to the Rule. Given the sanctions that currently target Cuba, Iran, North Korea, and the Maduro regime, the Rule is largely aimed at Chinese and (to a lesser extent) Russian ICTS companies.

Key Definitions

The Rule applies to certain listed categories of ICTS that have been "designed, developed, manufactured, or supplied by. . .persons owned by, controlled by, or subject to the jurisdiction or direction of a 'foreign adversary.'" These key terms are defined as follows:

- "ICTS" means "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."

- "ICTS Transaction" means "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."

- "Persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" means "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; and any corporation, partnership, association, or

other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary."

- This definition is very broad and could, for example include all companies (including Chinese-incorporated subsidiaries of U.S. companies) located in or organized under the laws of China, as well as subsidiaries of Chinese state-owned entities located anywhere in the world. While this definition would not necessarily capture U.S. subsidiaries of private Chinese companies, intracompany transfers of Chinese-origin ICTS between Chinese parent entities and their U.S. subsidiaries would likely be subject to the Rule.

Scope of the Rule

Despite these broad definitions, the Rule does not empower the Secretary of Commerce (or the Secretary's designee, collectively the "Secretary") to review all ICTS Transactions. Rather, the Rule only permits the Secretary to review "Covered ICTS Transactions." A Covered ICTS Transaction is an ICTS Transaction that:

1. Is conducted by any person or property "subject to the jurisdiction of the United States;"

2. Involves any property in which any non-U.S. 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 the date of the Rule's publication in the *Federal Register* (*i.e.*, January 19, 2021);

4. Involves any of the following six broad classes of ICTS; and

    a. ICTS to be used in a sector designated as "critical infrastructure" by Presidential Policy Directive 21 ("Critical Infrastructure Security and Resilience")[6], including any sub-sectors thereof or subsequently designated sectors. These sectors include, among others, the electric grid and water systems of the United States, certain transportation sectors (including airports and certain designated rail lines), a number of subsectors of the U.S. energy sector, including interstate petroleum and gas pipelines, and U.S. military installations.

    b. Software, hardware, or any other product or service integral to: (i) wireless local area networks; (ii) mobile networks; (iii) satellite payloads; (iv) satellite operations and control; (v) cable access points; (vi) wireline access points; (vii) core networking systems; or (viii) long- and short-haul networks.

c. Software, hardware, or any other product or service integral to data hosting or computing services (including software-defined services such as virtual private servers), that uses, processes, or retains (or is expected to use, process, or retain) "sensitive personal data" (broadly defined[7]) on more than one million U.S. persons[8] at any point over the 12 months prior to an ICTS Transaction.

d. Certain types of ICTS products (including, among other things, internet-enabled sensors, webcams, and other surveillance or monitoring devise; as well as routers, modems, and drones), if more than one million units have been sold to U.S. persons at any point over the 12 months prior to an ICTS Transaction.

e. Software designed primarily for connecting with and communicating via the Internet that is in use by more than one million U.S. persons at any point over the 12 months preceding an ICTS Transaction.

f. ICTS integral to: (i) artificial intelligence and machine learning; (ii) quantum key distribution; (iii) quantum computing; (iv) drones; (v) autonomous systems; or (vi) advanced robotics.

5. Involves ICTS that the Secretary determines is "designed, developed, manufactured, or supplied by. . . persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary." To make this determination, the Rule states that the Secretary should consider:

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

b. Ties between the person (including its officers, directors, or similar officials, employees, consultants, or contractors) and a "foreign adversary;"

c. Laws and regulations of any foreign adversary in which the person is headquartered or conducts operations, including research and development, manufacturing, packing, and distribution; and

d. Any other criteria that the Secretary deems appropriate.

Exceptions and Relation to CFIUS

The Rule includes a small list of exceptions to its scope that include exceptions for ICTS Transactions that (i) involve the acquisition of ICTS by a U.S. person as a party to a transaction authorized under a U.S.

government-industrial security program; or (ii) CFIUS is actively reviewing, or has reviewed, as a covered investment by a non-U.S. person in a U.S. business or U.S. real estate. However, the Rule notes that the CFIUS-related exception does not apply to ICTS Transactions conducted by parties to transactions notified to CFIUS that were not part of the covered investment by a non-U.S. person in a U.S. business or U.S. real estate notified to CFIUS. The Rule makes clear that ICTS-related concerns within the context of a given transaction notified to CFIUS will be handled through the CFIUS process, but because CFIUS focuses on investments by non-U.S. persons in U.S. businesses (and U.S. real estate) and the Rule focuses on generally smaller and more specific dealings in particular types of ICTS, Covered ICTS Transactions unrelated to a transaction notified to CFIUS (or that arise after CFIUS has completed its review, if the facts and circumstances have changed from the time of the CFIUS review) will still be subject to the Rule.

Powers of the Secretary Under the Rule

Under the Rule, the Secretary is empowered to undertake, on a "case-by-case basis," a review of a Covered ICTS Transaction to determine whether a Covered ICTS Transaction involves 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 and whether, as a result, the Covered ICTS Transaction poses certain (i) "undue" risks to U.S. ICTS, U.S. critical infrastructure, or the digital economy of the United States; or (ii) "unacceptable risks" to the national security of the United States or the security and safety of U.S. persons.[9] The focus of the Secretary's review is primarily on the ICTS itself (although if a transaction party is also the manufacturer, developer, or designer of the ICTS in question, any such review would include a related risk assessment of the party itself) and whether the ICTS could pose risks to U.S. national security.

If the Secretary determines that such risks exist with respect to a Covered ICTS Transaction, the Rule empowers the Secretary to either: (i) prohibit the Covered ICTS Transaction, (ii) direct the timing and manner of the cessation of the Covered ICTS Transaction (for a Covered ICTS Transaction that may already be pending or underway); or (iii) to consider factors to mitigate the risks of the Covered ICTS Transaction and to impose such mitigation as a condition of permitting the Covered ICTS Transaction to go forward.

The Secretary's Review: Process and Procedures

The Rule establishes a framework under which other U.S. agencies can refer an ICTS Transaction about which they have concerns to Commerce for a review and determination by the Secretary (and the Rule does not appear to prohibit Commerce from "self-referring" a transaction to itself as well). The Secretary then must perform an intake analysis to determine whether the ICTS Transaction referred is a Covered ICTS Transaction and then, based upon the results of this analysis, accept or reject the referral or request additional information from the referring agency.

If the Secretary accepts a referral, the Secretary must then complete a series of steps that can culminate in prohibiting or conditioning the transactions, and these steps must be performed within 180 days (although the Secretary has discretion to take more time).

Upon accepting a referral, the Secretary must perform an initial review of the Covered ICTS Transaction to assess whether the transaction poses an "undue" or "unacceptable" risk. The Secretary may require that the parties to the Covered ICTS Transaction produce information and documents on these topics. The Rule includes a number of criteria that the Secretary may consider as a part of this assessment, including, among others: (i) the nature and characteristics of the ICTS at issue, including technical capabilities, applications, and market share considerations; (ii) the nature and degree of the ownership, control, direction, or jurisdiction exercised by a "foreign adversary" over the design, development, manufacture, or supply at issue in the Covered ICTS Transaction; (iii) the statements and actions of the "foreign adversary" at issue in the Covered ICTS Transaction (*i.e.*, the "foreign adversary" government itself); (iv) the statements and actions of the parties to the Covered ICTS Transaction; and (v) the nature of the vulnerability implicated by the Covered ICTS Transaction. With respect to China, the Trump Administration had made repeated broad statements regarding the Chinese government's intent to use the private sector in China to further China's national security goals and the alleged duty of Chinese companies to provide information (including private data) and assistance to the government as requested. Similar statements are included in the preamble of the Rule with respect to "foreign adversaries" more generally.[10]

If the Secretary finds that the Covered ICTS Transaction "likely" poses "undue" or "unacceptable" risks, the Rule requires Commerce to consult with other relevant agencies (including, presumably, the referring agency) to make an initial determination as to whether the Covered ICTS Transaction does indeed pose such risks. Notably, if after the Secretary's initial review and consultation, the Secretary determines that no such risks exist, the Secretary may end the review, but the Secretary is not required to inform the parties about the review having been conducted (unless the Secretary contacted the parties or required the parties to provide information or documents).

If the Secretary's initial determination is instead that "undue" or "unacceptable" risks are presented by the Covered ICTS Transaction, the Secretary must then make a formal initial determination in writing that (i) explains why the Covered ICTS Transaction presents such risks; and (ii) sets forth whether the Secretary has initially determined to prohibit the Covered ICTS Transaction or to propose mitigation measures under which the transaction may be permitted. The Secretary then must notify the parties to the Covered ICTS Transaction either by direct service (*e.g.*, mail, email, personal delivery) or publication in the *Federal Register*.

Under the Rule, a party to a Covered ICTS Transaction then has 30 days from the date of service to (i) provide a response; (ii) submit arguments or evidence that the party believes may establish that an insufficient basis exists for the initial determination; and/or (iii) propose remedial steps which the party believes would negate the basis for the initial determination. Such responses must be in writing and the

Secretary may, but is not required to, engage in meetings with the parties to discuss the responses. The Rule provides confidentiality protection for the responses and any business confidential information or documents submitted to Commerce.

After receipt of a party's response, the Secretary must consider how or whether any such information provided affects the initial determination and then Commerce must engage with the relevant other agencies prior to issuing a final determination. If the agencies and Commerce cannot reach a consensus on the final determination with respect to the Covered ICTS Transaction, the Secretary can notify the President, who will then provide direction with respect to the final determination.

As noted above, within 180 days of accepting a referral, the Secretary must issue a final determination as to whether the Covered ICTS Transaction is (i) prohibited, (ii) not prohibited, or (iii) permitted subject to mitigation measures. However, the Secretary has discretion to determine that additional time for review is necessary. Final determinations are required to be sent to the transaction parties and relevant other U.S. government agencies consulted, before being published in the *Federal Register* (subject to a requirement to redact or omit any confidential business information regarding the parties).

Licensing Process

The Rule states that within 60 days of its publication in the *Federal Register* (*i.e.*, by March 22, 2021), Commerce will publish a related rule that will create procedures under which parties to Covered ICTS Transactions can apply to Commerce for a license to engage in the transaction. However, as this licensing rule has not yet been published or sent to the Office of the Federal Register, it is captured by the Biden Administration's regulatory "freeze" order and would have to be reviewed by Biden appointees or designees at Commerce, who would then decide whether it will be published and, if so, its contents. As a result, it is unlikely that this licensing rule will be issued by March 22, 2021 and, as with the Rule more generally, it is unclear whether or how the Biden Administration will ultimately implement any such licensing framework related to the Rule.

Penalties

The Rule empowers Commerce to impose IEEPA civil penalties (currently approximately $308,000 per violation) on parties to Covered ICTS Transactions (or other persons) who violate any final determination, mitigation agreement, or other order imposed under the Rule. The U.S. Department of Justice may also seek criminal prosecution for willful violations.

Implications

The Rule, if ultimately implemented, would provide Commerce with significant new powers to review a broad array of ICTS transactions by Chinese and Russian ICTS companies that currently offer or sell or plan to offer or sell relevant ICTS products or services in the United States, whether directly or indirectly.

Unlike some of Commerce's other actions targeting China in the Trump Administration (such as, for example, the addition of dozens of Chinese companies to the Entity List), the Rule does not aim to prohibit U.S. items and technology from flowing to China or Chinese companies. Rather, the Rule instead aims to prevent Chinese companies from selling or making available certain ICTS products in the United States or to U.S. persons. In doing so, the Rule creates a review process and prohibition and mitigation powers that are not unlike the powers CFIUS has in the context of corporate transactions involving non-U.S. investors or non-U.S. persons' real estate investments in the United States. The concern animating the Rule is that such products can allegedly be used to introduce security vulnerabilities into U.S. systems and used to exfiltrate U.S. person data to China (or other "foreign adversary" jurisdictions) for malign purposes.

The Rule was published in the *Federal Register* the day before President Biden's inauguration and, as a result, it is unclear whether or how the Biden Administration will ultimately implement or enforce the Rule. The Biden Administration's Commerce Department could, for example, withdraw and revise the Rule, extend the Rule's comment period, or entirely abandon the Rule. In this way, at the start of the Biden Administration, the Rule is similarly situated to a number of Trump Administration initiatives aimed at China that had been proposed, but not yet implemented, at the time of President Biden's inauguration, including: the Executive Order targeting non-U.S. persons' use and offering of U.S. "information as a service" products, the Executive Orders attempting to ban WeChat and TikTok from the United States, the Executive Order attempting to ban another eight Chinese software applications from the United States, and the State Department's "Clean Network Initiative."

Additionally, a prior proposed version of the Rule issued in late 2019 received numerous comments from U.S. industry groups that raised a number of concerns about the draft Rule, including, among others, that the Rule was unnecessarily broad in scope, did not sufficiently address due process concerns with respect to parties engaging in ICTS transactions, was unlimited in terms of review timing, did not provide sufficient transparency, and did not provide "safe harbor" protections for ICTS transactions reviewed by Commerce under the Rule.

While Commerce's announcement of the Rule in January 2021 stated that Commerce had revised the Rule in response to many of these comments, the Rule as currently drafted may nonetheless continue to face opposition from a number of U.S. industry groups, particularly in light of the recent change in Administration. Commerce has also requested, in its *Federal Register* announcement of the Rule, that interested parties submit comments and proposed edits to the Rule as currently drafted and Commerce has committed to reviewing and considering such comments (although without committing to a specific

timeframe for such review). Although the Rule has been meaningfully revised compared to the late 2019 draft, including with respect to increased transparency requirements, more detail with respect to the specific categories of ICTS covered by the Rule, and specific timeframes for Commerce's review under the Rule, we expect that U.S. industry will likely again express concerns to Commerce regarding the Rule's new substance and implementation process.

Both U.S. companies (including U.S. subsidiaries of Chinese or Russian companies) and non-U.S. companies (including, in particular, Chinese or Russian technology companies) engaged in ICTS Transactions that involve products or services designed, developed, manufactured, or supplied by Chinese or Russian companies should carefully review the Rule and monitor its status in the coming months. More broadly, both U.S. and non-U.S. companies (and, in particular, Chinese or Russian technology companies) should evaluate any current (as the Rule is retroactive to transactions pending or initiated as of January 19, 2021) or planned transactions in the United States or with U.S. persons relating to ICTS designed, developed, manufactured, or supplied by Chinese or Russian companies to determine whether any such transactions may be likely to be reviewed under the criteria included in the Rule (if implemented) and, if so, consider potential mitigation options in case notified of a review by Commerce.

We will continue to monitor developments with respect to the Rule and provide further updates as appropriate.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Jessica S. Carey
+1-212-373-3566
jcarey@paulweiss.com

Christopher D. Frey
+81-3-3597-6309
cfrey@paulweiss.com

Michael E. Gertzman
+1-212-373-3281
mgertzman@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Brad S. Karp
+1-212-373-3316
bkarp@paulweiss.com

Xiaoyu Greg Liu
+86-10-5828-6302
gliu@paulweiss.com

Richard S. Elliott
+1-202-223-7324
relliott@paulweiss.com

Rachel M. Fiorill
+1-202-223-7346
rfiorill@paulweiss.com

Karen R. King
+1-212-373-3784
kking@paulweiss.com

Associate Joshua R. Thompson contributed to this client alert.

---

1 Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," 84 Fed. Reg. 22689 (May 17, 2019), available here.

2 *Id*.

3 "Securing the Information and Communications Technology and Services Supply Chain," 86 Fed. Reg. 4909 (Jan. 19, 2021), available here (the "Rule"); *see* The White House, "Regulatory Freeze Pending Review," (Jan. 20, 2021), available here.

4 John D. McKinnon, "Commerce Nominee Pledges Tough China Stance, but Mum on Huawei Blacklist" THE WALL STREET JOURNAL (Jan. 26, 2021), available here.

5 *Id*.

6 The White House, "Presidential Policy Directive – Critical Infrastructure Security and Resilience," (Feb. 12, 2013), available here.

7 The Rule defines "sensitive personal data" as meaning: "(1) Personally-identifiable information, including: (i) Financial data that could be used to analyze or determine an individual's financial distress or hardship; (ii) The set of data in a consumer report, as defined under 15 U.S.C. § 1681a, unless such data is obtained from a consumer reporting agency for one or more purposes identified in 15 U.S.C. § 1681b(a); (iii) The set of data in an application for health insurance, long-term care insurance, professional liability insurance, mortgage insurance, or life insurance; (iv) Data relating to the physical, mental, or psychological health condition of an individual; (v) Non-public electronic communications, including email, messaging, or chat

communications, between or among users of a U.S. business's products or services if a primary purpose of such product or service is to facilitate third-party user communications; (vi) Geolocation data collected using positioning systems, cell phone towers, or WiFi access points such as via a mobile application, vehicle GPS, other onboard mapping tool, or wearable electronic device; (vii) Biometric enrollment data including facial, voice, retina/iris, and palm/fingerprint templates; (viii) Data stored and processed for generating a Federal, State, Tribal, Territorial, or other government identification card; (ix) Data concerning U.S. Government personnel security clearance status; or (x) The set of data in an application for a U.S. Government personnel security clearance or an application for employment in a position of public trust; or (2) Genetic information, which includes the results of an individual's genetic tests, including any related genetic sequencing data, whenever such results, in isolation or in combination with previously released or publicly available data, constitute identifiable data. Such results shall not include data derived from databases maintained by the U.S. Government and routinely provided to private parties for purposes of research. For purposes of this paragraph, "genetic test" shall have the meaning provided in 42 U.S.C. 300gg-91(d)(17)."

[8] The Rule defines "U.S. person" as meaning "any United States citizen; any permanent resident alien; or any entity organized under the laws of the United States or any jurisdiction within the Unites States (including such entity's foreign branches)."

[9] The Rule refers to the definition of "undue" and "unacceptable" risks as defined in Executive Order 13873, which are: "(i) 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) an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or (iii) an [otherwise] unacceptable risk to the national security of the United States or the security and safety of United States persons."

[10] *See* the Rule at 4909-4910.