ALERT MEMORANDUM

Commerce Initiates National Security Reviews of Information and Communications Technology and Services Transactions Linked to China

June 1, 2021

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

WASHINGTON

Paul Marquardt
+1 202 974 1648
pmarquardt@cgsh.com

Chase Kaniecki
+1 202 974 1792
ckaniecki@cgsh.com

William Dawley
+1 202 974 1771
wdawley@cgsh.com

The U.S. Department of Commerce (**Commerce**) recently announced[1] that it had issued multiple subpoenas to Chinese companies pursuant to Executive Order 13873 (**E.O. 13873**),[2] Securing the Information and Communications Technology and Services (**ICTS**) Supply Chain. According to Commerce, the subpoenas will help collect information necessary to determine whether transactions involving those companies satisfy the criteria set forth in E.O. 13873 and potentially could result in action with respect to those transactions to protect U.S. national security.

The first set of subpoenas came shortly after an interim final rule containing regulations to implement E.O. 13873 (the **Regulations**)[3] went into effect on March 22, 2021. As discussed in further detail below, under the Regulations, Commerce has the authority to review and prohibit or restrict transactions (including transactions it learns about from other private parties) conducted by any person, or involving any property, subject to U.S. jurisdiction, if they involve certain categories of ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a "foreign adversary"[4] and pose an "undue or unacceptable risk" to U.S. national security. E.O. 13873 and the Regulations contemplate a pre-transaction licensing process, but that process has not yet been established.

[1] U.S. Dep't of Commerce, *U.S. Department of Commerce Statement on Actions Taken Under ICTS Supply Chain Executive Order* (Apr. 13, 2021), available at: https://www.commerce.gov/news/press-releases/2021/04/us-department-commerce-statement-actions-taken-under-icts-supply-chain; U.S. Dep't of Commerce, *U.S. Secretary of Commerce Gina Raimondo Statement on Actions Taken Under ICTS Supply Chain Executive Order* (Mar. 17, 2021), available at: https://www.commerce.gov/news/press-releases/2021/03/us-secretary-commerce-gina-raimondo-statement-actions-taken-under-icts.

[2] Exec. Order No. 13873, *Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 22869 (May 15, 2019).

[3] 15 C.F.R. Part 7. Additional background on the related rulemaking process is available in the initial commentary in the related interim final rule. *See* 86 Fed. Reg. 4909 (Jan. 19, 2021).

[4] To date, Commerce has determined that China, Cuba, Iran, North Korea, Russia, and the Maduro regime in Venezuela are "foreign adversaries" for purposes of the Regulations. *See* 15 C.F.R. §7.4.

© Cleary Gottlieb Steen & Hamilton LLP, 2021. All rights reserved.
This memorandum was prepared as a service to clients and other friends of Cleary Gottlieb to report on recent developments that may be of interest to them. The information in it is therefore general, and should not be considered or relied on as legal advice. Throughout this memorandum, "Cleary Gottlieb" and the "firm" refer to Cleary Gottlieb Steen & Hamilton LLP and its affiliated entities in certain jurisdictions, and the term "offices" includes offices of those affiliated entities.

The review regime created by E.O. 13873 and the Regulations is in many respects similar to the national security foreign investment review regime overseen by the Committee on Foreign Investment in the United States (**CFIUS**). The ICTS regime empowers Commerce to review, and ultimately prohibit, certain transactions presenting national security risks. Like the CFIUS review regime, under the ICTS review regime Commerce may require the unwinding of ICTS transactions already completed (for example, by requiring equipment already installed in a U.S. network be removed) as well as prohibiting future transactions.

E.O. 13873 and the Regulations further the U.S. government's focus on U.S. network integrity, continuing a recent trend toward controlling U.S. persons' and companies' acquisition of foreign hardware and software. For example, in 2020 the U.S. government imposed restrictions on the ability of federal contractors to use telecommunications equipment and services from specified Chinese entities pursuant to Section 889 of the 2019 National Defense Authorization Act. Other actions include the State Department's "Clean Network" policy initiative, which includes the "Clean Store" effort to "remove untrusted applications from U.S. mobile app stores,"[5] former President Trump's 2020 and 2021 executive orders prohibiting transactions with certain Chinese software companies,[6] and President Biden's 2021 executive order directing federal agencies to conduct 100-day supply chain reviews for semiconductors, high-capacity batteries (including electric-vehicle batteries), critical and other strategic minerals, and pharmaceuticals and active pharmaceutical ingredients, and year-long supply chain reviews in the defense, public health, information and communications technology, transportation, energy, and agricultural commodities and food products sectors.[7] Together with the Regulations, these recent actions impose a new type of restriction on which foreign counterparties U.S. persons and companies may deal with that fills the gap between blunt tools like blocking sanctions (which would bar all dealings with such entities within U.S. jurisdiction) and U.S. import controls.

This memorandum provides an overview of transactions potentially subject to review under the Regulations, as well as the current ICTS Transaction review process and a potential proactive licensing procedure called for by the Regulations.

I. Covered ICTS Transactions

As noted above, under E.O. 13873 and the Regulations, Commerce has broad authority to review and prohibit or impose conditions—on a case-by-case, fact-specific basis in consultation with other federal agencies—on any:

"ICTS Transaction" that is …

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

[5] U.S. Dep't. of State, *Announcing the Expansion of the Clean Network to Safeguard America's Assets* (Aug. 5, 2020), available at https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/.
[6] Exec. Order No. 13942, *Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain*, 85 Fed. Reg. 48637 (Aug. 6, 2020); Exec. Order No. 13943, *Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain*, 85 Fed. Reg. 48641 (Aug. 6, 2020); Exec. Order No. 13971, *Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies*, 86 Fed. Reg. 1249 (Jan. 5, 2021). Executive Orders 13942 and 13943, which targeted TikTok and WeChat, respectively, were blocked by federal courts in December 2020.
[7] Exec. Order No. 14017, *America's Supply Chains*, 86 Fed. Reg. 11849 (Feb. 24, 2021).

communication by electronic means (including electromagnetic, magnetic, and photonic), including through transmission, storage, or display."[8]

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." [9]

conducted within U.S. jurisdiction,

This includes transactions conducted by any person subject to the jurisdiction of the United States or involving property subject to the jurisdiction of the United States.[10]

involving property in which any foreign party has an interest,

Including through an interest in a contract for the provision of the relevant technology or service.[11]

initiated, pending, completed or involving acts or services occurring on or after January 19, 2021, and

Regardless of the date of the relevant contract. Covers acts and services (*e.g.*, executing part of a managed services contract, installing software updates, or making repairs) on or after January 19, 2021, even if the related contract predates that date.[12]

involving one of six broad categories of ICTS set out in the Regulations.

The six categories[13] are:

i. *Critical Infrastructure*. ICTS that will be used by a party to a transaction in a sector or subsector designated (or later designated) as critical infrastructure by Presidential Policy Directive 21—Critical Infrastructure Security and Resilience.[14]

ii. *Network Infrastructure and Satellites*. Software, hardware, or any other product or service integral to wireless local area networks, mobile networks, satellite payloads, satellite operations and control, cable access points, wireline access points, core networking systems, or long- and short-haul systems.

iii. *Sensitive Personal Data*. Software, hardware, or any other product or service integral to data hosting or computing services that uses, processes, or retains, or is expected to use, process, or

[8] 15 C.F.R. §7.2. (definition of ICTS).
[9] *1*5 C.F.R. §7.2. (definition of ICTS Transaction).
[10] 15 C.F.R. §7.2 (definition of U.S. person).
[11] 15 C.F.R. §7.3.
[12] *Id.*
[13] 15 C.F.R. §7.3(a)(4).
[14] Presidential Policy Directive/PPD-21 (Feb. 12, 2013), available at: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

retain, sensitive personal data on greater than one million U.S. persons at any point over the twelve months preceding an ICTS Transaction.[15]

iv. *Surveillance/Monitoring, Home Networking, and Drones/UAVs*. If greater than one million units have been sold to U.S. persons at any point over the twelve months prior to an ICTS Transaction, any of: (i) internet-enabled sensors, webcams, and any other end-point surveillance or monitoring device; (ii) routers, modems, and any other home networking device; or (iii) drones or any other unmanned aerial system.

v. *Internet Connection and Communication Software*. 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 twelve months preceding an ICTS Transaction.

vi. *Emerging Technologies*. ICTS that is integral to artificial intelligence and machine learning, quantum key distribution, quantum computing, drones, autonomous systems, or advanced robotics.

II. Exempted ICTS Transactions

The Regulations exempt ICTS Transactions involving acquisitions of ICTS items authorized under a U.S. government-industrial security program or that CFIUS is actively reviewing, or has reviewed, from the scope of "Covered ICTS Transactions." However, ICTS Transactions conducted by parties to transactions reviewed by CFIUS that were not part of the transaction reviewed by CFIUS (e.g., equipment purchased from a supplier acquired by a foreign person in a CFIUS-reviewed transaction) are not exempted. Also, although not completely exempted from the Regulations, Commerce noted in its commentary in the related interim final rule that "ICTS Transactions solely involving personal ICTS hardware devices, such as handsets, do not warrant particular scrutiny."[16]

III. Review of Covered ICTS Transactions

The Secretary of Commerce may review any covered ICTS Transaction to determine if it involves both (i) ICTS designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a "foreign adversary" identified in the Regulations and (ii) any "undue or unacceptable risk" to U.S. national security as set out in E.O. 13873, and ultimately to conclude whether the ICTS Transaction should be permitted, permitted with negotiated mitigation measures, or prohibited. The Regulations set out the following steps for review.

Step 1: Referral. The Secretary of Commerce has broad discretion to initiate reviews of ICTS Transactions and can consider referrals from and information provided by any other government agency, a private party, or publicly available sources. Heads of other federal government agencies also can request that the Secretary of Commerce review an ICTS Transaction. When the Secretary of Commerce decides to conduct a review, Commerce will initially determine whether an ICTS Transaction is both within the scope of the Regulations (*i.e.*, satisfies the criteria set forth above) and involves ICTS designed, developed, manufactured or supplied by persons **owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary**. The Secretary will then start

[15] The Regulations use a substantively identical definition of "sensitive personal data" to the definition included in the regulations administered by the Committee on Foreign Investment in the United States (CFIUS). *See* 31 C.F.R. §800.241.
[16] *See* 86 Fed. Reg. 4909, 4913 (Jan. 19, 2021).

an initial review, request further information from the parties, or reject the referral. Once it accepts a referral, Commerce has 180 days[17] to complete the following steps in the review.

The Regulations identify six **foreign adversaries**, although Commerce can add additional regimes (and must periodically review the list in consultation with other federal agencies): [18]

- The People's Republic of China (including Hong Kong)
- The Republic of Cuba
- The Islamic Republic of Iran
- The Democratic People's Republic of Korea
- The Russian Federation
- The regime of Venezuelan politician Nicolás Maduro

As a practical matter, given existing U.S. sanctions, only Russian and Chinese companies are likely to be affected. Under the Regulations, the following persons are considered to be **owned by, controlled by, or subject to the jurisdiction or direction of 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; and
- any corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary.

Commerce considers the following non-exhaustive factors in determining whether an 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:[19]

- Whether the person or its suppliers have headquarters, research, development, manufacturing, test, distribution, or service facilities, or other operations in a foreign country, including one controlled by, or subject to the jurisdiction of, a foreign adversary.
- Ties between the person— including its officers, directors or similar officials, employees, consultants, or contractors—and a foreign adversary.
- Laws and regulations of any foreign adversary in which the person is headquartered or conducts operations, including research and development, manufacturing, packaging, and distribution.

Step 2: Initial Review. Commerce will assess whether the covered ICTS Transaction poses an **undue or unacceptable risk** to U.S. national security.

An **undue and unacceptable risk** is any of the following risks identified in E.O. 13873:[20]

[17] Unless the Secretary of Commerce determines in writing that additional time is necessary. *See* 15 C.F.R. §7.109(b).
[18] 15 C.F.R. §7.4.
[19] 15 C.F.R. §7.100(c).
[20] 15 C.F.R. §7.2.

- a 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;
- a risk of catastrophic effects on the security or resiliency of 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.

Under the Regulations, Commerce considers the following non-exhaustive factors to determine whether an ICTS Transaction poses an undue and unacceptable risk: [21]

- The nature and characteristics of the related ICTS, including technical capabilities, applications, and market share considerations.
- The nature and degree of ownership, control, direction, or jurisdiction exercised by the foreign adversary over the design, development, manufacture, or supply at issue.
- The statements and actions of the foreign adversary, the persons involved in the design, development, manufacture, or supply, and the parties to the transaction.
- Whether the transaction poses a discrete or persistent threat.
- The nature of the vulnerability implicated by the transaction.
- Whether there is an ability to otherwise mitigate the risks posed by the transaction.
- The severity of the harm posed by the transaction on health, safety, and security, critical infrastructure, sensitive data, the economy, foreign policy, the natural environment, and National Essential Functions (as defined by Federal Continuity Directive2 (FCD–2)).
- The likelihood that the transaction will in fact cause threatened harm.

The Regulations allow Commerce to consider almost any source of information, including public information, classified information available to the federal government, information requested from parties to a transactions, and information from third parties or other federal agencies in analyzing covered ICTS Transactions.[22]

Step 3: First Interagency Consultation. If Commerce finds that the covered ICTS Transaction likely poses an undue or unacceptable risk to U.S. national security, Commerce will notify and consult with appropriate agency heads to determine whether such a risk exists.[23]

Step 4: Initial Determination. After interagency consultation, Commerce will either determine that no such risk exists (and end its review without precluding future review) or find a undue or unacceptable risk. If the latter,

[21] 15 C.F.R. §7.103(c).
[22] *See* 15 C.F.R. §7.100.
[23] Defined to include the Secretary of the Treasury, the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the United States Trade Representative, the Director of National Intelligence, the Administrator of General Services, the Chairman of the Federal Communications Commission, and the heads of any other executive departments and agencies the Secretary determines is appropriate. *See* 15 C.F.R. §7.2.

Commerce will make an initial written determination on the specific risk and whether the transaction will be prohibited or subject to mitigation measures.

Step 5: Notification. If Commerce makes an initial determination, it will notify the parties to the ICTS Transaction by either publication in the Federal Register or service of a copy.

Step 6: Potential Party Response. Parties have 30 days to respond in writing to Commerce's initial determination.[24] Parties can argue against the initial determination or propose remediation.

Step 7: Second Interagency Consultation. If the parties respond, Commerce will consider the submission and seek consensus from appropriate agency heads on a final determination. Without consensus, the Secretary of Commerce will notify the President of its proposed final determination and any objections (and cannot issue a final determination without receiving direction from the President).

Step 8: Final Determination. Either after completing the second consultation or if the parties to the ICTS Transaction do not respond within 30 days of service of the initial determination, Commerce will issue its final determination on whether the ICTS Transaction is:

- Prohibited;
- Not prohibited; or
- Permitted subject to adoption of negotiated mitigation measures.

The Regulations provide that if a ICTS Transaction is prohibited, "the Secretary shall have the discretion to direct the least restrictive means necessary to tailor the prohibition to address the undue or unacceptable risk posed by the ICTS Transaction."[25] However, these "least restrictive means" could potentially include prohibiting a transaction that has not yet occurred or requiring the unwinding of a transaction that has already been completed.

Step 9: Publication. Final determinations to prohibit an ICTS Transactions will be served on the parties and published in the Federal Register (with confidential business information omitted).

IV. Licensing ICTS Transactions

Although the interim final rule outlines a 120-day process that parties can use to apply for licenses for ICTS Transactions and provided for Commerce to publish the procedures by March 22, Commerce has yet to publish any procedures. Instead, at this point, Commerce is seeking additional public input on the scope of a potential licensing or other pre-clearance process through an advance notice of proposed rulemaking (the **ANPR**) published March 29, 2021.[26] Although many expect the licensing process to be similar to national security reviews undertaken by CFIUS, Commerce's questions in the ANPR indicate that the form of the future procedures remains uncertain and that the various categories of ICTS Transactions may not be subject to the same procedures.[27] Given that the ANPR comment period remains open until April 28, 2021, and the lack of a timeline

[24] The Regulations explicitly state that parties have no right to obtain access to information considered in making the initial determination (including both classified and sensitive but unclassified information).
[25] 15 C.F.R. §7.109(c).
[26] 86 Fed. Reg. 16312 (Mar. 29, 2021).
[27] 86 Fed. Reg. 16312, 16313 (Mar. 29, 2021). Commerce is seeking input on such preliminary considerations as what approach Commerce should take to licensing and whether certain ICTS Transaction categories should or should not be considered for a license or pre-clearance.

for when Commerce expects to issue a notice of proposed rulemaking, it appears unlikely that any licensing or other pre-clearance process will be available in 2021.

In the meantime, although parties can refer their ICTS Transaction to Commerce under the Regulations, as noted above, the Secretary of Commerce has discretion regarding whether to accept referrals and review ICTS Transactions. Also, even if Commerce determines that the ICTS Transaction does not present any undue or unacceptable risks under E.O. 13873, that initial determination does not preclude Commerce from reviewing the same transaction in the future "where additional information becomes available."[28]

V. Enforcement

Violations of any final determination or direction issued under the Regulations, including of any mitigation measures or other conditions imposed by Commerce, are subject to potentially significant penalties under the International Emergency Economic Powers Act (IEEPA):

- A maximum civil penalty of $250,000, or an amount that is twice the amount of the ICTS Transaction that is the basis of the violation with respect to which the penalty is imposed.
- A maximum criminal penalty of $1,000,000 and imprisonment of 20 years.

…

CLEARY GOTTLIEB

[28] *See* 15 C.F.R. §7.105(a)(2).