Westlaw Today
powered by Reuters

The ICTS supply chain rules: towards a U.S.-China tech decoupling?

By Anthony Rapa, Esq., Blank Rome LLP

AUGUST 9, 2022

A July 2022 report relayed the news that the U.S. Department of Commerce (Commerce) is investigating the installation of Huawei equipment into cell towers situated near U.S. military bases and missile silos, based on concerns the equipment could hoover up sensitive data and transmit it to China.[1]

The report indicates that Commerce is carrying out the investigation pursuant to its rules implementing Executive Order (EO) 13873[2] on "Securing the Information and Communications Technology and Services Supply Chain" (the ICTS Rules).

What are the ICTS Rules, and how will they be enforced? The ICTS Rules empower Commerce to review — and as warranted, to mitigate, block, or unwind — dealings in information and communications technology and services (ICTS) that have a nexus with a designated "foreign adversary," including China and Russia.

As for enforcement, that has been a key question for industry since Commerce first issued the rules in January 2021, in the closing days of the Trump Administration. Since then, public reporting has shed light on Commerce's gradual efforts to wield its investigative powers and build out the administrative infrastructure needed to fully implement the rules.

As full maturation of the ICTS Rules seems to draw ever nearer, now is a good time to explore the rules in detail and assess their implications for cross-border tech development, which will be especially relevant for companies involved in telecommunications, connected applications, software development, and emerging technologies, or with a nexus to critical infrastructure.

Scope of ICTS rules

On January 19, 2021, the day before President Trump left office and President Biden was inaugurated, Commerce issued the ICTS Rules, scheduled to take effect March 22, 2021, setting up a framework for Commerce review of certain transactions subject to U.S. jurisdiction involving ICTS in which a non-U.S. national has an interest.[3] The rules implement EO 13873 of May 15, 2019.

After President Biden took office, observers wondered whether his administration would rescind the rules or extend their effective date as it had done with certain other Trump Administration executive actions, but to the surprise of some, the Biden Administration allowed the rules to take effect on March 22, 2021.

Under the ICTS Rules, an ICTS transaction is defined 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*."

As full maturation of the ICTS Rules seems to draw ever nearer, now is a good time to explore the rules in detail and assess their implications for cross-border tech development.

Specifically, the ICTS Rules authorize Commerce review of ICTS transactions:[4]

- conducted by any person subject to U.S. jurisdiction or involving any property subject to U.S. jurisdiction;
- involving any property in which a foreign country or foreign national has an interest;
- initiated, pending, or completed on or after January 19, 2021; ***and***
- Involving one of the following types of ICTS:
  - ICTS that will be used by a party to the transaction in a "critical infrastructure" sector, as designated in Presidential Policy Directive 21 — Critical Infrastructure Security and Resilience,[5] including chemicals, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare / public health, information technology, nuclear reactors / materials / waste, transportation systems, and water / wastewater systems;
  - ICTS integral to WLANs, mobile networks, satellite payloads, satellite operations and control, cable access points, wireline access points, core networking systems, or long- and short-haul networks;

- ICTS integral to data hosting or computing services that uses, process, or retains sensitive personal data for more than one million U.S. persons in a 12-month period preceding the transaction;
- Any of the following, if greater than one million units have been sold to U.S. persons in the 12-month period prior to the transaction:
  - Internet-enabled sensors, webcams, or any other endpoint surveillance or monitoring device;
  - Routers / modems / home networking; or
  - Drones / UAS;
- Software designed for connecting with and communicating via the internet that is in use by greater than one million U.S. persons in the 12-month period prior to the ICTS transaction, including desktop, mobile, web-based, and gaming applications; or
- ICTS integral to artificial intelligence, quantum key distribution, quantum computing, drones, UAS, or advanced robotics.

Commerce has since proposed amending the ICTS Regulations to apply to "connected software applications," implementing Executive Order 14034 on "Protecting Americans' Sensitive Data from Foreign Adversaries."[6]

Commerce review process

If an ICTS transaction meets the criteria described above, then Commerce is authorized to conduct a review to assess whether the transaction poses an undue or unacceptable risk to U.S. national security based on its nexus to a designated "foreign adversary," including China, Cuba, Iran, North Korea, Russia, and Venezuela. Where Commerce determines that there is such a risk, it is empowered to prohibit an ICTS transaction or order mitigation measures.

Specifically, upon receipt of information voluntarily submitted by parties to a transaction, obtained through compulsory production, or obtained through other sources (*i.e.*, open source, classified information, etc.), or upon request from certain U.S. government agencies (noted below), Commerce has discretion to consider a referral of an ICTS transaction for review.[7]

Specifically, Commerce will assess whether a 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."[8]

The ICTS Rules define such persons as:

> 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.[9]

In this regard, the focus is on ties to the designated "foreign adversary," *i.e.*, the nation that Commerce has designated as an adversary, *e.g.*, China. Therefore, as set out in the definition, an entity subject to the jurisdiction of or owned by a foreign adversary (*e.g.*, a Chinese-incorporated entity or an entity owned by the Chinese government) is in scope, along with ICTS supplied by such an entity (*e.g.*, Chinese-origin code or content).

Commerce's enforcement of the ICTS Rules has focused on the issuance of subpoenas to companies in support of national security reviews under the rules.

For entities not organized in "foreign adversary" countries, the focus is on whether such an entity acts at the direction or control of a foreign adversary (*e.g.*, China) or of a person controlled or majority financed by an adversary.

The process steps for Commerce specifically are as follows:[10]

- In considering a referral, Commerce can accept it, reject it, or request more information.
- If Commerce accepts the referral, it will conduct an initial review to assess whether the transaction poses an "undue or unacceptable risk."
- If Commerce assesses that a transaction meets these criteria, it will engage in interagency consultation with the "appropriate agency heads" — 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, and the Chairman of the Federal Communications Commission.
- Following interagency consultation, if Commerce assesses that a transaction poses an "undue or unacceptable risk," it will notify the parties to the transaction.
- Within 30 days of receiving such notification, a party to an ICTS transaction can submit a written request for Commerce to mitigate or rescind the initial determination.
- This submission triggers a second interagency review.
- Within 180 days (unless extended) of accepting a referral and commencing the initial review, Commerce will reach a final determination regarding the transaction, and will notify the parties that the transaction is prohibited, not prohibited, or permitted subject to mitigation measures. Commerce

will publish in the Federal Register decisions to prohibit a transaction.

Failure to comply with a final determination is punishable under the International Emergency Economic Powers Act[11] by civil penalties of up to $330,947 (annually adjusted for inflation) and criminal penalties of up to one million dollars and/or 20 years' imprisonment.[12]

Enforcement to date

In March 2021, Commerce issued an Advance Notice of Proposed Rulemaking requesting input from the public regarding how Commerce should implement a pre-clearing process for parties seeking to engage in ICTS transactions.[13] Commerce has not implemented any such framework to date.

Impacted companies should assess whether their ICTS supply chain includes exposure to "foreign adversary" countries and entities under their control.

Publicly available information indicates that, as of this writing, Commerce's enforcement of the ICTS Rules has focused on the issuance of subpoenas to companies in support of national security reviews under the rules.[14]

In its budget proposal for Fiscal Year 2023, Commerce has requested $36.2 million to implement the ICTS Rules, including through the hiring of 114 personnel to "*intake and adjudicate licenses, provide a credible enforcement and penalty capability, allow for dedicated legal support for transaction reviews, licenses, and enforcement actions, and correlate complex technical analysis and interpret all-source intelligence (to include cybersecurity threat concerns).*"[15]

Practice tips

Companies active in covered ICTS areas should consider their supply chain exposure to "foreign adversary" countries, particularly China and Russia.

As indicated above, this includes companies in the following sectors:

- Telecommunications / networking
- Personal data storage
- Surveillance devices
- Drone technology
- Communications software / connected applications
- Emerging technology (e.g., artificial intelligence, quantum technology, robotics)
- Critical infrastructure

Impacted companies should assess whether their ICTS supply chain includes exposure to "foreign adversary" countries and entities under their control. Notably, this includes not only entities domiciled in the specified "adversary" countries, but also entities organized elsewhere that could be subject to direction by an entity organized in an "adversary" country, *e.g.*, a company with substantial Chinese or Russian investment or financial backing.

ICTS supply chain risks can arise through the following:

- Sourcing of covered equipment from an adversary country or from an entity under its control
- Sourcing of equipment incorporating components provided by an adversary country or from an entity under its control
- Sourcing of software developed in whole or in part in an adversary country or by an entity under its control
- Storage / accessibility of U.S. personal data in an adversary country or by an entity under its control
- Active connections by covered ICTS to an adversary country or to an entity under its control

Companies that identify ICTS supply chain risks should consider a strategy to de-risk (such as by finding alternative sources for impacted items) or, as appropriate based on the nature and magnitude of the risk, to engage with Commerce proactively, notwithstanding the current lack of a "preclearance" process.

Notes

[1] Alexandra Alper, "U.S. Probes China's Huawei Over Equipment Near Missile Silos," Reuters, Jul. 21, 2022, https://reut.rs/3A5LKy0.

[2] Exec. Order No. 13873, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22,689 (May 15, 2019).

[3] Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909 (Jan. 19, 2021); 15 C.F.R. Part 7.

[4] 15 C.F.R. § 7.3.

[5] Presidential Policy Directive — Critical Infrastructure Security and Resilience, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[6] Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications, 86 Fed. Reg. 67379 (Nov. 26, 2021); Exec. Order No. 14034, Protecting Americans' Sensitive Data from Foreign Adversaries, 86 Fed. Reg. 31,423 (June 9, 2021).

[7] 15 C.F.R. § 7.100(a); 15 C.F.R. § 7.103(a).

[8] 15 C.F.R. § 7.100(c).

[9] 15 C.F.R. § 7.2.

[10] 15 C.F.R. § 7.103(b)-(c); 15 C.F.R. § 7.104; 15 C.F.R. § 7.105(b); 15 C.F.R. § 7.107; 15 C.F.R. § 7.108; 15 C.F.R. § 7.109.

[11] 50 U.S.C. § 1705.

[12] 15 C.F.R. § 7.200.

[13] Securing the Information and Communications Technology and Services Supply Chain: Licensing Procedures, 86 Fed. Reg. 16,312 (Mar. 29, 2021).

[14] *See* Press Release, U.S. Department of Commerce, U.S. Secretary of Commerce Gina Raimondo Statement on Actions Taken Under ICTS Supply Chain Executive Order (Mar. 17, 2021), https://bit.ly/3Q70t1p; Press Release, U.S. Department of Commerce, U.S. Department of Commerce Statement on Actions Taken Under ICTS Supply Chain Executive Order (Apr. 13, 2021), https://bit.ly/3Qra82y. Notably, the July 2022 *Reuters* report regarding Huawei indicates that Commerce issued Huawei a subpoena in April 2021, which would seem to sync up with the April 2021 press release noted herein.

[15] The Department of Commerce Budget in Brief, Fiscal Year 2023 at 70, https://bit.ly/3zCPcP7; *see also* Sara Friedman, "Commerce Dept. Plans to Develop Office for ICTS Supply Chain 'From Scratch,' Using Additional Resources," Inside Cybersecurity, May 17, 2022 https://bit.ly/3Qfkseo.

About the author

Anthony Rapa is a partner in the Washington, D.C., office of **Blank Rome LLP**, and leads the firm's national security team. A dual U.S./U.K.-qualified practitioner, he advises clients on international risk matters in the context of cross-border trade, operations and investments, including economic sanctions, export controls, supply chain security and foreign investment reviews. He can be reached at anthony.rapa@blankrome.com.

This article was first published on Westlaw Today on August 9, 2022.