Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated October 26, 2022

The Information and Communications Technology and Services (ICTS) Rule and Review Process

In January 2021, the Department of Commerce (Commerce) created a new process for the executive branch to review transactions involving information and communications technology and services (ICTS) and to determine whether those transactions present national security and economic risks. Commerce established the process under an interim final rule (86 FR 4909), which implements Executive Order 13873 (May 15, 2019). When a transaction in ICTS involves "foreign adversaries" and presents certain "undue or unacceptable risks" to the United States, the new rule (Supply Chain Rule) allows Commerce to either block the transaction or negotiate risk-mitigation measures. The ICTS review process regulates individual *ICTS transactions*—broadly defined as "any acquisition, importation, transfer, installation, dealing in, or use of any [ICTS]." As such, it could subject a wide range of commercial interactions to a new federal approval process.

What Is ICTS?

ICTS is defined as any "hardware, software, or other product or service … primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means." The term includes a broad array of technologies and services, such as internet systems, wireless networks, cellular phones, computers, satellite systems, artificial intelligence, quantum computing, and cloud computing services.

Executive Order 13873

The Supply Chain Rule implements Executive Order 13873, titled *Securing the Information and Communications Technology and Services Supply Chain*. Invoking National Emergencies Act (50 U.S.C. § 1601) and citing the International Emergency Economic Powers Act (50 U.S.C. §1701), then-President Trump declared a national emergency because of the threat of foreign adversaries exploiting vulnerabilities in ICTS. In response to this threat, Executive Order 13873 prohibits transactions involving foreign-owned ICTS that present (1) an undue risk of sabotage or subversion to ICTS in the United States, (2) an undue risk of catastrophic effects on the security or resiliency of critical infrastructure or the digital economy in the United States, or (3) an unacceptable risk to U.S. national security or the security and safety of U.S. persons. The order delegates implementation to Commerce.

What Is a Foreign Adversary?

Executive Order 13873 references risks posed by *foreign adversaries*, which the order defines as any foreign government or foreign person "engaged in a long-term pattern or serious instances of conduct significantly adverse" to U.S. security or the safety of U.S. persons. The executive order does not identify entities that meet the definition, but Commerce elaborated on the term in the Supply Chain Rule. Commerce identified China (including Hong Kong), Cuba, Iran, North Korea, Russia, and the Nicolás Maduro regime in Venezuela as foreign adversaries. Commerce based its determination on several sources, including the U.S. National Security Strategy, the U.S. Intelligence Community's Worldwide Threat Assessment, the 2018 U.S. Cyber Strategy, and other reports and assessments from U.S. agencies. Commerce is to periodically review the list of foreign adversaries.

Determining Foreign Adversary Involvement

To be subject to the ICTS review process, a transaction must involve ICTS designed, developed, manufactured, or supplied by persons or entities owned by, controlled by, or subject to the jurisdiction of a foreign adversary. In determining whether the foreign adversary element is met, Commerce may consider (1) whether the party to the transaction or its suppliers have headquarters or other facilities in a foreign country controlled by a foreign adversary, (2) personal and professional ties between the party and a foreign adversary, (3) laws and regulations of the foreign adversary in which a party is headquartered or conducts operations, and (4) other factors that the Secretary of Commerce deems appropriate.

What Transactions Will Be Reviewed?

In addition to the foreign adversary requirement, a transaction must meet several criteria to be subject to the ICTS review process. First, the transaction must involve property subject to U.S. jurisdiction or activity conducted by an individual or entity subject to U.S. jurisdiction. Second, the transaction must involve property in which a foreign country or foreign national has an interest. Third, the transaction must be initiated, pending, or completed after January 19, 2021. Finally, the transaction must involve one of six categories of technology:

1. **Critical infrastructure**: ICTS that will be used in one of 16 critical infrastructure sectors designated in Presidential Policy Directive 21;
2. **Network infrastructure and satellites**: ICTS 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;
3. **Sensitive personal data processing**: ICTS integral to data hosting or computing services that process (or are expected to process)

sensitive personal data on more than 1 million U.S. persons;

4. **Monitoring, home networking, and drones**: Monitoring devices (e.g., webcams), home networking devices (e.g., routers and modems), and drones or other unmanned aerial systems when more than 1 million units have been sold to U.S. persons;
5. **Communication software**: Software designed primarily for internet connections and communications in use by more than 1 million U.S. persons; or
6. **Emerging technology**: ICTS integral to artificial intelligence and machine learning, quantum key distribution, quantum computing, drones, autonomous systems, or advanced robotics.

Connected Software Applications

In June 2021, President Biden issued Executive Order 14034, which directed the Secretary of Commerce to evaluate the risks posed by *connected software applications*, commonly called "apps." The order identified additional criteria for Commerce to consider when evaluating transactions involving apps under the Supply Chain Rule. Factors include the app's capacity to enable espionage and the sensitivity of data collected. In November 2021, Commerce published a proposed rule (86 FR 67379) that would expressly include apps in the definition of ICTS and add app-specific risk factors to the Supply Chain Rule.

Exclusions

The Supply Chain Rule excludes from review a U.S. person's acquisition of ICTS as part of a U.S. government-industrial security program, because those acquisitions are subject to other forms of oversight. It also excludes transactions that the Committee on Foreign Investment in the United States (CFIUS) is reviewing or has reviewed.

The ICTS Review Process

Referral: ICTS review begins with referral of a transaction to Commerce. Referral can take place in three ways: (1) Commerce's receipt of certain information that indicates review is warranted; (2) the head of a federal agency's request; or (3) at the Secretary of Commerce's discretion (i.e., self-referral). The Supply Chain Rule does not require parties to proactively notify Commerce of an ICTS transaction, but Commerce may require parties to furnish information and documents. At the referral stage, Commerce assesses whether a transaction meets the foreign adversary, technology, and other requirements to fall within the scope of the review process. After this assessment, Commerce can accept the referral, seek more information from parties, or reject the referral.

Initial review: If Commerce accepts a referral, it next conducts an initial review to determine whether the transaction poses an undue or unacceptable risk as described in Executive Order 13787. The Supply Chain Rule lists 10 criteria Commerce may use in evaluating these risks. Criteria include the type of the technology or service at issue, nature of the threat, and severity of potential harm. If Commerce determines that the transaction presents an undue or unacceptable risk, it must conduct an interagency consultation.

Initial determination: After the first interagency consultation, Commerce is to make an initial determination on whether to permit a transaction, prohibit it, or propose measures to mitigate risks. Unless it permits the transaction in full, Commerce must provide a written determination to the parties to the transaction. Next, the parties have 30 days to respond to the initial determination and propose their own remedial measures. If the parties respond, Commerce must engage in a second interagency consultation. If the parties do not respond, Commerce can make a final determination without a second consultation.

Final determination: After the initial determination process, Commerce may issue a final, written determination on whether to permit the transaction, prohibit it in full, or permit it subject to an agreement on risk-mitigation measures. Commerce must complete the total process within 180 days unless it determines in writing that more time is necessary. Violation of a final determination can result in civil and criminal penalties.

Comparisons to CFIUS

Some observers have likened the ICTS review process to CFIUS, which assists the President in overseeing the national security implications of foreign investment in the U.S. economy. Both CFIUS and the ICTS review involve interagency processes to review and block certain commercial transactions with foreign entities that present national security concerns. However, while CFIUS traditionally reviews major corporate restructurings and acquisitions, the Supply Chain Rule authorizes Commerce to review individual commercial sales. For example, whereas CFIUS might prevent a foreign entity from acquiring a stake in a U.S. semiconductor company, under the Supply Chain Rule, Commerce could block a U.S. company from buying individual semiconductors from a foreign company in a foreign adversary's jurisdiction.

Licensing and Pre-Approval

During the notice and comment period on a proposed version of the Supply Chain Rule (84 FR 65316), many commentators requested that Commerce allow parties to obtain pre-approval for planned ICTS transactions. In response, Commerce stated in the Supply Chain Rule that it plans to create a licensing process.

Congressional Interest

Members of Congress may have an interest in the Supply Chain Rule's impact on U.S. national security and economic interests. Because the ICTS sector is integrated into many aspects of the economy, the Supply Chain Rule could have a wide-ranging effect on U.S. industry. Some business and trade groups contend the rule is overbroad, lacks transparency, and results in costly compliance. Others view the rule as essential to protect U.S. national security and supply chains.

Stephen P. Mulligan, Legislative Attorney

IF11760

Disclaimer