



National Security Review Bodies (Part I): Legal Context and Comparison

Updated September 6, 2023

Federal law creates several frameworks that allow the United States to review the national security risks posed by some private commercial transactions. These legal frameworks give the United States authority to review, prohibit, and, in some cases, unwind a wide range of commercial dealings, but they do not capture all commercial transactions that might present national security risks. Some [organizations](#) and [Members of Congress](#) have proposed new or modified processes to address transactions not captured under current legal structures. This Sidebar examines and draws contrasts among several key legal frameworks that allow the United States to review and prohibit some private commercial transactions due to national security risks. A [companion Sidebar](#) introduces legal issues that could arise from proposals to expand or create new review mechanisms.

Departments of Commerce and State Export Controls

Discussed in this [CRS Report](#), the export control system is one of the primary frameworks for evaluating commercial transactions' possible national security risks. The export control system [governs](#) U.S.-origin exports to a foreign country or national, transfers from one foreign country to another (called [reexports](#)), or transfers within a foreign country. These export restrictions apply to, among other things, [defense articles](#) and services (e.g., items and technology for military use), [nuclear equipment](#) and material, and [dual-use items](#) (e.g., items with both civilian and military uses). Among these categories, export controls of dual-use items cover the broadest range of transactions. The [Export Control Reform Act of 2018](#), which is implemented through the Export Administration Regulations (EAR), provides legal authority for dual-use and certain other export controls. Other statutory schemes, such as those governing [nuclear-related items](#) and [foreign military sales](#), create authority for non-dual-use controls programs. [Several agencies](#) administer and enforce export controls, with the Bureau of Industry and Security (BIS) in the Department of Commerce (Commerce) playing a leading role in dual-use exports.

The EAR create several interagency bodies responsible for establishing what exports and which end users are permissible and for reviewing and issuing [license](#) applications for certain controlled exports. For example, an [End-User Review Committee](#) with representatives from the Departments of Commerce, State, Defense, Energy, and (in some cases) the Treasury decides what parties should be on the [Entity List](#). Exports to parties on the Entity List are either prohibited or subject to additional license

Congressional Research Service

<https://crsreports.congress.gov>

LSB11034

requirements because those parties threaten U.S. [national security or foreign policy](#) or raise certain terrorism and nonproliferation concerns. BIS and several [other agencies](#) have authority to review applications for licenses, and the EAR create [processes and timelines](#) for reviewing such applications, [resolving inter-agency disagreements](#) on whether to grant applications, and [appealing](#) denials. The EAR also create a [process](#) for administrative enforcement of export controls through an [administrative law judge](#).

The EAR address [a large portion](#) of U.S. outbound trade flow, but the export control system does not regulate all transactions among U.S. and foreign actors. For instance, export controls do not apply to purely monetary transactions, such as U.S. banks' conversion of payments in foreign currencies into U.S. dollars (*dollar-clearing*). The export control system also does not govern U.S. companies' capital investment in foreign entities when the investment does not involve the transfer of goods, services, or technology.

Office of Foreign Assets Control Economic Sanctions

The Office of Foreign Assets Control (OFAC) in the Department of the Treasury (Treasury) plays a key role in national security reviews of commercial transactions as one of the primary agencies that [administers and enforces](#) economic sanctions. OFAC administers a varied set of individual, country-based, and issue-specific sanctions programs, discussed in this [CRS In Focus](#). The legal authority for many of the sanctions programs administered by OFAC derives from the President's power to block transactions under the International Emergency Economic Powers Act ([IEEPA](#)) after declaring an emergency under the National Emergencies Act ([NEA](#))—although other statutory schemes [authorize](#) or [require](#) the President to impose sanctions in particularized settings, such as the [counterterrorism](#) context.

For economic sanctions enforcement, OFAC maintains a public list of “persons” (a term that includes individuals and companies) subject to sanctions on its Specially Designated Nationals and Blocked Persons List, known as the [SDN List](#). The list includes “individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries,” as well as “individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific.” OFAC's [Non-SDN Lists](#) identify persons whose assets are partially blocked or with whom some transactions are permitted. (Economic sanctions can also result in placement on the Entity List administered by BIS.)

Although OFAC publishes the SDN and Non-SDN Lists, the agency responsible for designating the persons for those lists varies depending on the sanctions program. Regardless of the program and designating authority, [federal regulations](#) generally allow a sanctioned person to file an administrative petition with OFAC to be removed from an OFAC list through a process called [delisting](#). Federal regulations also allow OFAC to issue [licenses](#) permitting transactions that would otherwise be blocked.

Being placed on the SDN List can deny the designated person access to nearly all aspects of the U.S. financial system, including dollar-clearing transactions. It can also deny access to any assets the designee has that are under U.S. jurisdiction, and U.S. persons are usually prohibited from transacting with the designee. At the same time, OFAC's list-based sanctions derived from IEEPA/NEA authorities have certain limits. These sanctions programs generally focus on the national risk posed by the parties involved in transactions rather than examining whether broader classes of transactions by their nature raise national security risks and should be reviewed regardless of the parties involved.

Committee on Foreign Investment in the United States (CFIUS) Reviews

CFIUS is an interagency committee that serves the President in reviewing for potential national security risks that may arise from foreign investments in the United States. CFIUS reviews certain foreign investment transactions, including some real estate investments, to determine whether they threaten to

impair U.S. national security. In contrast to OFAC sanctions, CFIUS is not a list-based program, and the committee can review any foreign investment transaction that falls within its statutory ambit (detailed in this [CRS Report](#)). When CFIUS determines that a transaction presents a sufficient national security risk, it can impose [mitigation measures](#) and make recommendations to the President on whether to prohibit or suspend the transaction. The President has the [ultimate authority](#) to prohibit or suspend a covered transaction if he or she finds there is credible evidence that the transaction would threaten to impair national security and that other laws do not provide adequate and appropriate authority to protect the United States. Presidents have used this authority to [prohibit](#) planned transactions and to require parties to [divest](#) or “unwind” completed transactions.

CFIUS’s statutory authority derives from Section 721 of the [Defense Production Act](#), as amended and codified in [50 U.S.C. § 4565](#). CFIUS is chaired by the Secretary of the Treasury and is made up of [11 regular members](#), two of whom are ex officio.

CFIUS traditionally reviews mergers, acquisitions, and takeovers that could result in a foreign entity taking control of a U.S. business. [Amendments](#) to CFIUS’s statutory authorities enacted in 2018 allow the committee’s review of some [non-controlling investments](#) in U.S. businesses involving critical technologies, critical infrastructure, or U.S. citizens’ sensitive personal data. The 2018 amendments also authorized CFIUS to review transactions involving U.S. [real estate](#) near military installations, airports, and military ports. Overall, the President has prohibited seven transactions since CFIUS’s formation. The seven transactions involved foreign acquisitions of [MAMCO Manufacturing](#) (1990), four U.S. [wind farm project companies](#) (2012), [Aixtron SE](#) (2016), [Lattice Semiconductor Corporation](#) (2017), [Qualcomm Incorporated](#) (2018), [StayNTouch](#) (2020), and [Musical.ly](#) (2020). CFIUS generally does not review outgoing U.S. investments (e.g., a U.S. company’s investment in a foreign corporation), nor does it review purchases or sales of individual commercial items or services.

Sector-Specific Review Processes

In some areas, the executive branch has used existing legal authorities to create national security review structures that are specific to certain sectors.

Outbound Investment in Sensitive Technologies

In August 2023, President Biden issued [Executive Order \(E.O.\) 14105](#), which addresses national security risks arising from outbound capital investment from the United States to foreign companies involved in certain sensitive technologies. The order cites concerns that outbound capital flows can be exploited to accelerate development of technologies used to support foreign countries’ military, intelligence, surveillance, and cyber capabilities. Invoking the NEA and IEEPA, President Biden declared that foreign development of these capabilities constitutes an unusual and extraordinary threat to the United States. While the order cites a threat from *countries of concern*, an annex to the order identifies only the People’s Republic of China (PRC), including Hong Kong and Macau, as a country of concern.

E.O. 14105 directs the Secretary of the Treasury, in consultation with Commerce and other executive branch agencies, to issue implementing regulations. On August 14, 2023, Treasury solicited public comment on its implementation plans in an [advance notice of proposed rulemaking](#).

E.O. 14105 addresses investment in three categories of *covered national security technologies and products*: semiconductors and microelectronics, [quantum information technologies](#), and [artificial intelligence \(AI\) systems](#). The order creates a two-tiered system for addressing national security risk from investment in these technologies:

- **Prohibited transactions:** Outbound investments in covered national security technologies and products that pose a particularly acute threat to national security are

prohibited. Treasury is considering prohibiting certain investments in technologies that enable advanced integrated circuits and supercomputers; advanced quantum information technologies; and AI systems incorporated into software designed to be exclusively for military, intelligence, or mass-surveillance uses.

- **Notifiable transactions:** Some outbound investments in covered national security technologies and products that may contribute to national security threats are permitted, but the U.S. investor must notify Treasury and provide information about the transaction. Treasury is considering a notification requirement for design, fabrication, and packaging of integrated circuits that are not otherwise prohibited transactions. Treasury is also considering mandatory notification for investments involving AI systems designed for cybersecurity, digital forensics, penetration testing, robotics, surreptitious listening devices, non-cooperative location-tracking, and facial recognition.

In the advance notice of proposed rulemaking, Treasury [noted](#) that covered transactions would likely include acquisitions of equity interests (*e.g.*, mergers and acquisitions, private equity, and venture capital), greenfield investments, joint ventures, and certain debt financing transactions. Treasury [expects to exempt](#) certain transactions from the prohibition and notification requirements, such as investments by a limited partner into funds that are solely passive and below a de minimis threshold. In contrast to the CFIUS process, Treasury [does not anticipate](#) that its outbound investment review regulations will require the executive branch to evaluate transactions' national security risks on a case-by-case basis. Instead, Treasury expects that the parties to transactions covered by E.O. 14105 will independently assess whether their planned investments are prohibited, notifiable, or permissible.

Information and Telecommunications Technology and Services

Under a January 2021 [rule](#) discussed in this [CRS In Focus](#), Commerce created a process to review whether transactions involving the supply chain of information and telecommunications technology and services (ICTS) present certain national security and economic risks. When a transaction in ICTS involves designated [foreign adversaries](#) and presents undue or unacceptable risks as outlined in the 2019 [Executive Order 13873](#), the January 2021 rule (Supply Chain Rule) allows Commerce to either prohibit the transaction or negotiate risk-mitigation measures. Upon issuing the Supply Chain Rule, Commerce [designated](#) the PRC, Cuba, Iran, North Korea, Russia, and the Nicolás Maduro regime in Venezuela as foreign adversaries. The rule regulates individual ICTS transactions—broadly [defined](#) as “any acquisition, importation, transfer, installation, dealing in, or use of any [ICTS].” The rule’s legal authority stems from IEEPA, which former President Trump invoked in 2019 after [declaring](#) a national emergency arising from foreign adversaries’ ability to create and exploit vulnerabilities in ICTS systems.

The Supply Chain Rule’s framework could allow Commerce to prohibit imports of items from entities upon which it imposes export and procurement restrictions and to regulate a broad range of commercial transactions that fall outside existing legal regimes. Despite its potential breadth, Commerce has not prohibited a transaction under the Supply Chain Rule’s review process as of August 2023, but it has used the rule to issue subpoenas to multiple [PRC-based companies](#) that provide ICTS in the United States.

Telecommunications Licenses

The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Telecom Committee) is an interagency body that reviews certain applications by foreign parties for U.S. telecommunications licenses and makes recommendations to the Federal Communications Commission (FCC) on whether to approve the licenses. The Attorney General chairs the Telecom Committee, and the Secretaries of Defense and Homeland Security serve as members, along with any other agency heads or assistants to the President that the President may appoint. Several other executive

branch officials act as [advisors](#) to the committee. The Telecom Committee operated for many years informally as “Team Telecom” until President Trump issued a 2020 [executive order](#) formalizing the committee. The FCC has also adopted its own [rules](#) on the process by which it seeks the Telecom Committee’s input.

The FCC refers three types of licenses or authorizations to the Telecom Committee: (1) [international Section 214 authorizations](#) allowing telecommunications carriers to provide telephone service between the United States and foreign points; (2) [submarine cable licenses](#) allowing persons to operate submarine cables that connect the United States with a foreign country or with another portion of the United States; and (3) [common carrier, broadcast, or aeronautical radio station licenses](#) when the applicant is a corporation with foreign ownership over certain thresholds.

The Telecom Committee reviews these applications to determine whether there is “[credible evidence](#)” that the license would pose a risk to the national security or law enforcement interests of the United States. If it determines that there is a credible risk, then it must [recommend](#) that the application either be denied or granted contingent on the applicant’s compliance with [mitigation measures](#). Once the FCC grants a license, the Telecom Committee [continues to monitor](#) the licensee’s compliance with any mitigation measures and may recommend that the FCC modify or revoke the license.

In recent years, the FCC has revoked or denied several international Section 214 authorizations for PRC-based companies on the advice of the Telecom Committee or Team Telecom. For instance, the FCC denied [China Mobile’s](#) application for an international Section 214 authorization in 2019 and revoked [China Telecom’s](#), [China Unicom’s](#), [Pacific Networks’](#), and [ComNet’s](#) international Section 214 authorizations in 2021 and 2022. All of these denials or revocations were based on national security concerns related to PRC control and influence over these companies. Appeals have resulted in [affirmations](#) of the FCC determinations in this category of actions because in each instance, the court [upheld](#) the challenged FCC order.

FCC Equipment Authorizations

As discussed in this [CRS Legal Sidebar](#), the FCC has adopted [new rules](#) restricting certain equipment that poses national security risks from being imported or sold in the United States. Under the [FCC’s regulations](#) all electronic equipment capable of emitting radio frequency energy must be authorized by the FCC before being imported or marketed in the United States. Additionally, under the new rules, the FCC [will not issue](#) any new authorizations for telecommunications equipment produced by Huawei Technologies company and ZTE Corporation, the two largest PRC telecommunications equipment manufacturers. It [will also not issue](#) new authorizations for equipment produced by three PRC-based surveillance camera manufacturers—Hytera Communications, Hangzhou Hikvision Digital Technology, and Dahua Technology—until the FCC approves these entities’ plans to ensure that their equipment is not marketed or sold for public safety purposes, government facilities, critical infrastructure, or other national security purposes.

Bulk Power System

In 2020, President Trump issued the [Bulk Power Executive Order](#), which invoked the NEA and IEEPA and directed the Secretary of Energy to prohibit certain transactions involving electric equipment in the U.S. bulk power system that presented undue and unacceptable risks due to foreign adversaries’ involvement. The Department of Energy implemented the executive order by issuing a [2020 Prohibition Order](#) that barred certain utilities from acquiring or installing some bulk power system electrical equipment that serviced critical defense facilities and was sourced from companies owned, controlled by, or subject to the jurisdiction or direction of the PRC. As rationale for the restriction, the 2020 Prohibition Order cited PRC plans and technological capability to undermine the United States’ electric grid.

The Biden Administration has sought to reformulate U.S. policy toward protecting the supply chain for the bulk power system. In 2021, the Biden Administration [revoked](#) the Department of Energy’s 2020 Prohibition Order and [allowed](#) the national emergency declared in the Bulk Power Executive Order to expire. (National emergency declarations [automatically terminate](#) after one year unless renewed by the President.) The Department of Energy under the Biden Administration still [describes](#) essential electric system equipment sourced from the PRC as a national security risk, but it has not renewed the Bulk Power Executive Order. (For more detail on U.S. policy on the electric grid, see this [CRS Report](#).)

Author Information

Stephen P. Mulligan
Legislative Attorney

Chris D. Linebaugh
Legislative Attorney

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS’s institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.