Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

National Security Review Bodies: Legal Context and Comparison

Updated November 9, 2022

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 Members of Congress, executive branch officials, and organizations 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. This Sidebar also 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
LSB10848

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 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.

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. As of October 2022, Commerce has designated the People's Republic of China (PRC), Cuba, Iran, North Korea, Russia, and the Nicolás Maduro regime in Venezuela as foreign adversaries. The Supply Chain 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 October 2022, 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 and China Unicom's international Section 214 authorizations in 2021 and 2022, respectively. All three of these denials or revocations were based on national security concerns related to PRC control and influence over these companies.

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 is gathering information on developing a long-term strategy to manage electric grid security risks and analyzing the need for a future prohibition order. (For more detail on U.S. policy on the electric grid, see this CRS Report.)

Legal Considerations for New National Security Review Systems

In recent years, some observers and Members of Congress have advocated for new or expanded national security review frameworks to examine transactions that may not be subject to existing procedures. Proposals in the 117th Congress include legislation that would authorize systems to review and potentially prohibit some U.S. companies' outbound investments in certain foreign countries, foreign companies' purchases of U.S. agricultural land, and foreign acquisition of U.S. genetic testing companies. In addition to policy debates about the merits of individual programs, creating or expanding national security systems can raise legal issues about the programs' structure and operations.

Procedural Due Process: The Due Process Clause of the Constitution's Fifth Amendment requires, among other things, that the government provide a person deprived of a property right with notice of the government action and a meaningful opportunity to contest it. This requirement—known as procedural due process—can be relevant in legal challenges to national security reviews. For example, the U.S. Court of Appeals for the District of Columbia Circuit held that, before the President can order a company to divest an acquisition under the CFIUS process, due process requires the government to provide the affected company with the unclassified information on which it based its decision and an opportunity to respond. In challenges to designations on OFAC lists, by contrast, courts have concluded that the government's interest in national security outweighed litigants' needs for a pre-deprivation hearing and access to classified information supporting the designation.

Judicial Review: An issue related to due process is the extent to which those affected by national security review bodies' actions can seek judicial review. Some review bodies' decisions, such as OFAC licensing decisions, are considered final agency actions subject to judicial review under the Administrative Procedure Act (APA). The APA requires courts to give deference to agencies' decisionmaking while allowing courts to overturn agency actions that are arbitrary, capricious, or outside an agency's legal authority. Other statutes seek to limit judicial review of certain national security review bodies' decisions by exempting some decisions from the APA, requiring litigation to be brought in a specified court, or prohibiting judicial review altogether. Even the most restrictive of these provisions, however, have not completely foreclosed judicial review. In cases involving restrictive statutes, courts have adjudicated certain issues, such as whether the national security review bodies exceeded statutory authority (called *ultra vires* review) and whether they complied with judicially enforceable constitutional requirements, including procedural due process standards.

Extraterritoriality: Another consideration tied to the Due Process Clause is the extraterritorial scope of the review system. Statutes underlying national security review frameworks generally require some nexus between the transaction under review and a U.S. person or property interest. IEEPA-based sanctions, for example, apply to transactions involving U.S. persons or property subject to U.S. jurisdiction, and export controls apply to U.S. origin goods, services, and technology or the direct product of those items. Apart from these statutory requirements, some courts have stated that the Due Process Clause imposes an overarching constitutional requirement for a link between the United States and the prohibited action. Not all courts, however, agree that this territorial constitutional constraint applies in every case.

Confidentiality: Government reviews of private commercial transactions can require a balance between the transacting parties' desire for confidentiality and the public interest in the process. Several national security review frameworks include confidentiality mandates, which differ depending on the legal paradigm. Some frameworks prohibit the government from disclosing parties' private information gathered during the review process unless an exception applies. CFIUS's legal authorities provide even stricter confidentiality by stating that materials submitted during its review process are exempt from the Freedom of Information Act absent an exception. To keep Congress informed, confidentiality requirements may allow disclosure to Congress and require periodic briefing and reports to relevant congressional committees.

Classified Information: The United States must often rely on classified information when making national-security-driven decisions, and some transaction review frameworks provide specialized processes for handling that information. For instance, 2018 amendments to CFIUS's statutory authorities added provisions governing the use of classified and other protected information deemed necessary to resolve the judicial proceedings.

Trade Agreements: Creating or expanding national security review programs potentially could implicate U.S. obligations under its trade agreements. Many bilateral and multilateral trade agreements state that they do not prevent parties from actions needed to protect "essential security interests," but the scope of this national security exception is the subject of significant debate, discussed in this CRS Legal Sidebar.

First Amendment: National security review systems can implicate the First Amendment's protections for freedom of speech and association—although the Supreme Court has frequently suggested that courts may give greater deference to the government in order to address national security issues. Some entities have made First Amendment claims under the theory that they were sanctioned for expressing a particular viewpoint or supporting certain causes. Most First Amendment challenges of this type have failed, but at least one federal appellate court held that an OFAC regulation that barred "coordinated advocacy" with an organization on an SDN List violated the First Amendment's guarantee of freedom speech. In 2021, the communications app WeChat obtained a preliminary injunction on First Amendment grounds that barred Commerce from implementing a Trump Administration executive order that would have largely prevented U.S. users from using WeChat. That executive order, which President Biden revoked, likely violated the First Amendment by closing a medium of public expression that was one of the only viable means for communication in some communities, according to the court.

IEEPA Exceptions: When national security systems rely on the NEA and IEEPA, statutory exceptions to the President's transaction-blocking authority may be a point of consideration. Under IEEPA's exceptions, the President does not have authority to regulate or prohibit personal communications, medicine and humanitarian assistance, informational materials, and travel-related transactions. During the Trump Administration, two federal district courts concluded that IEEPA did not provide authority to restrict access to the TikTok video-sharing app because TikTok's services could be considered personal communications or informational material. President Biden revoked the executive order on which those TikTok restrictions were based, but the Biden Administration is reportedly still evaluating restrictions on TikTok's operations under the CFIUS rubric as of October 2022.

Author Information

Stephen P. Mulligan
Legislative Attorney

Chris D. Linebaugh
Legislative Attorney

Disclaimer