Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

CFIUS: Executive Branch Actions on Evolving National Security Risks and Enforcement

Updated September 10, 2026

In 2022, the Biden Administration issued the "first-ever presidential directive" defining additional national security factors for the Committee on Foreign Investment in the United States (CFIUS) to consider in evaluating foreign investment transactions. Executive Order (EO) 14083 reaffirms a "commitment to open investment," while seeking to ensure CFIUS "remains responsive to an evolving national security landscape and the nature of the investments that pose related risks." The EO informs how CFIUS reviews strategic transactions—in general and with regard to key sectors and factors—and focuses on countries that have a strategic goal of acquiring critical technology or critical infrastructure that affects U.S. leadership in areas related to national security. It could enhance scrutiny of investments from countries that may meet such criteria, such as the People's Republic of China (PRC, or China). President Trump's America First Investment Policy, issued in 2025, echoes some of these themes with commitments to utilize CFIUS and to restrict certain PRC investments.

Also in 2022, the U.S. Department of the Treasury published CFIUS Enforcement and Penalty Guidelines (Guidelines) that describe how it approaches enforcement and penalty determinations for violations by parties subject to CFIUS action. Some viewed the Guidelines as a signal that CFIUS may more proactively seek enforcement actions and civil monetary penalties. In 2024, Treasury finalized regulatory updates intended to "sharpen [CFIUS] penalty and enforcement authorities."

CFIUS Background

CFIUS is an interagency body, chaired by the U.S. Treasury Secretary, that serves the President in overseeing the potential U.S. national security implications of certain foreign investment in the U.S. economy. It has associated authorities (50 U.S.C. §4565; 31 C.F.R. Chapter VIII) to review, clear, and, if required, impose terms of mitigation to address national security risks before allowing transactions to proceed. CFIUS also has authority to refer transactions to the President for action, including prohibiting or compelling divestiture of transactions that present risks that CFIUS determines it cannot sufficiently mitigate. See CRS In Focus IF10177, *Committee on Foreign Investment in the United States (CFIUS)*.

Executive Order 14083

CFIUS decisionmaking is not public, in part to protect the confidentiality of parties to a transaction. EO 14083 gives insight into issues CFIUS may be navigating since the implementation of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA; P.L. 115-232, Title XVII, Sub. A), which expanded CFIUS jurisdiction in key areas.

The EO requires CFIUS to adopt specified approaches and direction. While the EO does not name China, it targets behaviors common to PRC investments focused on U.S. capabilities in strategic areas prioritized and funded by China's industrial policies (see CRS In Focus IF10964, *Made in China 2025 and China's Industrial Policies*). The EO also addresses foreign investors' use of U.S. entities and persons to act as third parties and calls for scrutiny of third-party ties in transactions.

EO 14083 makes explicit certain national security factors that CFIUS is required to consider in reviewing investment transactions but does not otherwise change its authorities or jurisdiction. **The EO elaborates on two existing factors in the CFIUS statute:**

- **Critical U.S. supply chains resiliency**—both inside and outside the defense industrial base. Key sectors include microelectronics, artificial intelligence, biotechnology, quantum computing, advanced clean energy, climate technologies, critical materials, agriculture, and food security. The EO requires CFIUS to consider U.S. supply chains broadly, not only U.S. defense industrial base supply chains.
- **U.S. technological leadership—**with a focus on areas affecting national security. The EO directs the White House Office of Science and Technology Policy (OSTP) to publish "periodically" a list of sectors, in addition to those the EO identified, key to U.S. technological leadership. This provision may broaden the scope of technologies and risk areas CFIUS considers. CFIUS is also to consider "relevant third-party ties" of the foreign person, and whether a transaction could lead to future advancements and applications in such technologies for the foreign actor that could undermine U.S. national security. This framing directs CFIUS to not only consider how the transfer of a capability to a foreign acquirer could affect a *loss of certain U.S. national capabilities* (with respect to manufacturing capabilities, services, critical mineral resources, or technologies) but also how an acquisition could *enhance a foreign acquirer's gain in capabilities*. This provision may require CFIUS to more fully consider how a transaction advances the national capabilities of countries of concern. The PRC, for example, has used U.S. acquisitions to fill gaps in technologies such as semiconductors.

CFIUS is also to consider three additional factors:

- **Aggregate industry investment trends**—whether a transaction may affect U.S. national security with regard to the broader industry, and the effect of a series of investment transactions in which a foreign investor might gain control of a technology or sector over time.
- **Cybersecurity**—whether a transaction may provide foreign persons or third parties access to capabilities or information

databases and systems to conduct cyber intrusions or malicious cyber-enabled activity (e.g., designed to affect election outcomes or operation of critical infrastructure, such as smart grids). This provision looks at how transactions may create specific points of connection, access, and related touchpoints and risks in U.S. critical infrastructure.

- **U.S. persons' sensitive data**—whether a transaction involves a U.S. business with "access to [U.S.] persons' sensitive data," including "health, digital identity, or other biological data and any data that could be identifiable or de-anonymized," that could be exploited. The EO introduced a broader definition than current CFIUS regulations with respect to U.S. businesses that maintain or collect sensitive personal data. This factor also appears to promote greater scrutiny of claims that parties use only anonymized data by examining de-anonymizing capabilities.

Enforcement and Penalty Guidelines

CFIUS's Guidelines outline its approach to enforcement actions and penalty determinations. The Guidelines identify three categories of conduct that can constitute a violation of CFIUS's legal authorities or mitigation agreements: (1) failing to file a mandatory declaration or notice triggering CFIUS review; (2) failing to comply with a mitigation agreement; and (3) making material misstatements, omissions, or false certifications. The Guidelines explain that CFIUS relies on U.S.-government data, publicly available information, third-party service providers (e.g., auditors), tips, and information from parties to transactions to determine violations. CFIUS also has subpoena authority under 50 U.S.C. §4555(a). The Guidelines encourage cooperation by persons subject to CFIUS and "strongly encourage" self-disclosure of potential violations. Not all violations result in penalties; CFIUS has discretion to determine appropriate remedies. CFIUS considers several factors in determining penalties, such as

- harm to U.S. national security;
- the timing of any self-disclosure;
- whether the conduct was intentional, efforts to conceal or delay sharing information, and seniority of personnel involved;
- actions taken in response to the violation; and
- the subject's compliance record and internal policies.

CFIUS's Guidelines are nonbinding and do not change its statutory or regulatory authority to impose penalties. In 2024, Treasury revised applicable regulations to, among other changes, (1) extend penalties for material misstatements or omissions to include certain responses to CFIUS requests for information, (2) increase the maximum civil penalty to $5 million (from $250,000), and (3) allow 20 business days (extended from 15) for the petition and decision process.

In addition to CFIUS's authority to impose civil penalties, the Attorney General may seek judicial enforcement of presidential orders prohibiting transactions. In 2026, the Attorney General brought an enforcement action under this authority for the first time. See CRS Legal Sidebar LSB11435, *The Department of Justice's First Lawsuit Enforcing a Presidential Order Under Section 721 of the Defense Production Act*.

CFIUS Penalty Process

CFIUS first sends a notice that explains the conduct to be penalized, penalty amount, and legal basis for the action. The recipient has 20 days to submit a petition for reconsideration. CFIUS makes a final penalty determination within 20 days of receiving the petition or after the deadline to submit the petition expires; deadlines may be extended. If CFIUS concludes that an enforcement action is warranted, regulations (31 C.F.R. §§800.901, 902) authorize imposing penalties and damages, including civil penalties in certain cases.

Considerations for Congress

The 119th Congress is considering legislation to strengthen CFIUS by addressing perceived gaps in jurisdiction and PRC-related concerns, including PRC investments in U.S. strategic sectors, and "greenfield" investments in new U.S. facilities and land purchases. In 2025, Congress enacted P.L. 119-60 requiring notification of and restrictions on certain U.S. outbound investments to China.

The EO and Guidelines raise issues for possible legislation and oversight. Congress might update the risk factors and sectors that CFIUS must consider, drawing from the EO and factors Congress recommended in FIRRMA §1702(c). Congress last updated such factors in P.L. 110-49. Congress might also consider whether to adopt OSTP's critical and emerging technologies list when considering CFIUS's authority over non-passive and non-controlling foreign investments (e.g., minority stakes that afford a foreign person access to certain information, certain rights, or involvement in substantive decisionmaking) in U.S. businesses that develop, test, or produce such technologies. CFIUS's statute defines critical technologies in part by reference to a U.S. export-control regime for emerging technologies (50 U.S.C. §4817), which defines technologies according to their applications and use. OSTP identifies emerging technologies more broadly based on 14 areas.

Congress might engage Treasury and other CFIUS member agencies to obtain information about how CFIUS is acting on recent guidance and applying its authorities in practice. With the EO's focus on aggregate investments, Congress could require enhanced reporting on investments from foreign countries of concern over time by sector, critical supply chains, company, and country of investor. It could examine when instances of aggregation should trigger a new CFIUS review, or other agency responses to mergers and acquisitions (e.g., related to antitrust, securities, and telecom). On enforcement, Congress might scrutinize CFIUS mitigation terms and practices, define in legislation the enforcement mandates, expand penalties, or seek clarity on how disagreements among CFIUS agencies are resolved.

Peter J. Benson, Legislative Attorney
Cathleen D. Cimino-Isaacs, Specialist in International Trade and Finance
Karen M. Sutter, Specialist in Asian Trade and Finance

IF12415

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.