Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

May 26, 2023

CFIUS Executive Order on Evolving National Security Risks and CFIUS Enforcement Guidelines

On September 15, 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 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 E.O. informs how CFIUS reviews strategic transactions—in general and with regard to key sectors and factors—and could potentially enhance scrutiny of investments from countries of concern, such as the People's Republic of China (PRC or China). Also, in October 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 see the Guidelines as a signal that CFIUS may more proactively seek enforcement actions and civil monetary penalties.

CFIUS Background

CFIUS is an interagency body, chaired by the U.S. Treasury Secretary, which serves the President in overseeing the potential national security implications of certain foreign investment in the U.S. economy. It has associated legal authorities (50 U.S.C. §4565; 31 C.F.R. Chapter VIII), for example, to review, clear, and, if required, impose terms of mitigation to address U.S. 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 CFIUS determines it cannot sufficiently mitigate. See CRS In Focus IF10177, *The Committee on Foreign Investment in the United States*.

Executive Order 14083

CFIUS decisionmaking is not public, in part to protect the confidentiality of parties to a transaction. E.O. 14083 gives insight into issues CFIUS may be navigating. The use of an E.O. requires CFIUS to adopt specified approaches and direction. While the E.O. does not name China, it targets behaviors common to PRC investments that seek U.S. capabilities in strategic areas prioritized and funded by China's industrial policies (see CRS In Focus IF10964, *"Made in China 2025" Industrial Policies: Issues for Congress*). The E.O. focuses on countries that have a strategic goal of acquiring critical technology/infrastructure that affects U.S. leadership in areas related to national security. It also addresses foreign investors' use of U.S. entities and persons to act as third parties. This focus may signal U.S. government concerns that China among others may be using U.S. workarounds to evade scrutiny.

> With respect to investments directly or indirectly involving foreign adversaries or other countries of special concern, what may otherwise appear to be an economic transaction undertaken for commercial purposes may actually present an unacceptable risk to U.S. national security due to the legal environment, intentions, or capabilities of the foreign person, including foreign governments, involved in the transaction. —E.O. 14083

E.O. 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 E.O. 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 E.O. requires CFIUS to consider U.S. supply chains broadly, not only U.S. Department of Defense supply chains.
- **U.S. technological leadership—**with a focus on areas affecting national security. The E.O. directs the Office of Science and Technology Policy (OSTP) to publish "periodically" a list of sectors, in addition to those the E.O. identified, fundamental to U.S. technological leadership. This provision may broaden the scope of technologies CFIUS considers and place emphasis on certain areas of risk in reviewing transactions. 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. In particular, with China's use of U.S. acquisitions to fill technology gaps, this provision may require CFIUS to more fully consider how a transaction advances PRC national capabilities.

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 E.O. introduces 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' first-ever Guidelines outline its approach to enforcement actions and penalty determinations. The Guidelines are non-binding and do not change CFIUS' statutory or regulatory authority to impose penalties. The Guidelines outline three categories of conduct that can constitute a violation of CFIUS' legal authorities or mitigation agreements: 1) failing to file a mandatory notice or declaration triggering CFIUS review; 2) failing to comply with a mitigation agreement; and 3) making material misstatements, omissions or false certifications.

CFIUS Penalty Process

In imposing penalties, CFIUS first sends a notice that explains the conduct to be penalized, the penalty amount, and the legal basis for the action. The recipient has 15 days to submit a petition for reconsideration. CFIUS makes a final penalty determination within 15 days of receiving the petition or after the deadline to submit the petition expires. Deadlines may be extended upon agreement. If CFIUS concludes that an enforcement action is warranted, federal regulations (31 C.F.R. §§800.901, 902) authorize imposing penalties and damages, including a civil penalty of up to $250,000 or, in some cases, the value of the transaction. To date, CFIUS has announced two civil penalties: a $1 million penalty in 2018 for a party's failure to establish security policies and report as required in a mitigation agreement, and a $750,000 penalty in 2019 for a party violating a CFIUS interim order while a transaction was under review.

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 and "strongly encourage" self-disclosure of potential violations. Not all violations result in penalties; CFIUS has discretion to determine what remedies are appropriate. CFIUS considers the timing of self-disclosure when determining how to respond to a violation. CFIUS also considers several factors in determining penalties, such as

- Harm to U.S. national security;
- Whether the conduct was intentional or the result of negligence, efforts to conceal or delay sharing information, and seniority of personnel involved;
- Actions taken in response to the violation, including voluntary self-disclosure and cooperation; and
- The subject's history, familiarity, and record of compliance with CFIUS and the extent to which its internal policies were adequate.

Considerations for Congress

The 118th Congress is considering various legislation to strengthen CFIUS by addressing perceived gaps in jurisdiction and China-related concerns, including U.S. outbound investment and technology transfer and licensing to China in strategic industries; PRC investments in U.S. strategic sectors; PRC ties to U.S. research; "greenfield" investments in new U.S. facilities and land purchases.

The E.O. and Guidelines raise issues for possible legislation and oversight of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA, P.L. 115-232, Title XVII, Subtitle A), which expanded CFIUS jurisdiction in key areas. Congress might update in statute the risk factors and sectors that CFIUS must consider, drawing from the E.O. and the factors Congress recommended in FIRRMA §1702(c). Congress last updated such factors in the Foreign Investment and National Security Act of 2007 (P.L. 110-49). Similarly, Congress might consider whether to adopt the OSTP-defined technologies as the operative list that establishes CFIUS jurisdiction over investments in which foreign parties have sensitive access to or influence over a U.S. business, but not formal control (i.e., non-passive and non-controlling investments). The technologies on OSTP's list are more broadly defined than current CFIUS statute and regulations, which set jurisdiction by export-controlled technologies.

Congress might engage Treasury and other CFIUS member agencies to ascertain the extent to which CFIUS is acting on the new guidance in practice. With the E.O.'s focus on aggregate investments, Congress could require enhanced reporting on PRC investments 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, including related to antitrust, securities, and telecom, for example. Given the E.O.'s specific mention of agriculture and food security, Congress might consider making the U.S. Department of Agriculture a full CFIUS member agency. On enforcement, Congress might scrutinize CFIUS mitigation terms and practices, define in legislation the enforcement mandates, expand penalties (e.g., criminal), or seek clarity on how any disagreements among CFIUS agencies are resolved.

Cathleen D. Cimino-Isaacs, Specialist in International Trade and Finance
Stephen P. Mulligan, Legislative Attorney
Karen M. Sutter, Specialist in Asian Trade and Finance

Disclaimer