CFIUS has circled its civil enforcement wagons — Trump 2.0 is likely to build upon activities begun by Biden administration

By Barbara Linney, Esq., Baker & Hostetler LLP, Randy Cook, Esq., Alvarez & Marsal, and Scott Jansen, Esq.

FEBRUARY 13, 2025

The Committee on Foreign Investment in the United States (CFIUS or the Committee), which is chaired by the U.S. Department of Treasury, dramatically increased its civil monetary enforcement posture in 2023-2024, including issuing six civil monetary penalties totaling over $70 million in penalties (*See* U.S. Department of the Treasury, CFIUS Enforcement, (Accessed Jan. 22, 2025) https://bit.ly/4aLoWEt.).

The Trump administration is unlikely to substantially change this trend, given its continued focus on geopolitical and industrial competition with China and other nations. Increased enforcement through presidential blocks of CFIUS-eligible transactions and continued high usage of CFIUS mitigation agreements are likely. Accordingly, investors, companies, counsel and professionals engaged in CFIUS-related activities need to account for a risky CFIUS enforcement environment going forward.

The Trump administration's planned federal agency staffing and program expenditure reductions are unlikely to impact CFIUS activities because CFIUS has a national security focus, and it pays for itself through CFIUS filing fees and civil monetary penalties.

CFIUS civil enforcement 101

CFIUS reviews certain foreign investments to determine the effect of the transaction on the national security of the United States. Foreign investments and acquisitions of U.S. companies that develop or build critical technology, have sensitive data or large amounts of data, or are involved in critical infrastructure are key focus areas for CFIUS. CFIUS does not exclusively focus on Chinese investments, but Chinese investments do receive heightened scrutiny.

Most CFIUS filings are voluntarily submitted (i.e., without a legal requirement to do so), as there are significant statutory incentives to do so. Foreign investment activity into U.S. companies with critical technology have mandatory regulatory filing requirements (with civil financial penalties for violations). Investors and U.S. businesses may (or must) file a joint voluntary notice (long-form filing) or Declaration (short-form filing).

Upon receipt of the filing, CFIUS will review the transaction and make one of three decisions:

(1) Conclude the transaction presents no national security risk and issue a "safe harbor" letter, permitting the subject transaction to go forward and prohibiting future review by CFIUS (31 C.F.R. § 800.508(d).);

(2) Determine the transaction presents unmitigable national security risk(s) and request the president "block" the financial transaction (and require divestment if the transaction has previously closed) (31 C.F.R. § 800.508(c); 50 U.S.C. § 4565(d).); or

(3) Conclude the transaction presents mitigable national security risk(s) and negotiate a national security agreement (NSA) requiring parties to the transaction to do or not do certain enumerated activities (e.g., governance restrictions, limits on network or data access or storage, and limits on business activities).

Investors, companies, counsel and professionals engaged in CFIUS-related activities need to account for a risky CFIUS enforcement environment going forward.

At the end of calendar year 2023 (the Committee's last public reporting), there were 246 active CFIUS mitigation agreements under monitorship, and the use of verification measures such as site visits and third-party oversight is becoming more prevalent and impactful for transactions (U.S. Department of the Treasury, Committee on Foreign Investment in the United States Calendar Year 2023 Annual Report to Congress, (Accessed Jan. 22, 2025) https://bit.ly/4e6VwAZ).

Under the CFIUS statute (50 U.S.C. § 4565) and its implementing regulations (31 C.F.R. § 800.901), there are three types of violations, which may result in civil monetary penalties:

- Failure to file a required CFIUS filing under 31 C.F.R. § 800.401;
- Violations of material provisions of CFIUS mitigation agreements, conditions, or orders (strict liability standard); and
- Material misstatement, omission, or false certification provided to CFIUS in a Declaration or Joint Voluntary Notice. (The December 2024 CFIUS regulatory changes expanded civil monetary penalties to all material statements or omissions made to the Committee) (31 C.F.R. § 800.901(b), 31 C.F.R. § 800.901(c), 31 C.F.R. § 800.901(a).).

Given the growing CFIUS civil monetary penalties posture of CFIUS, parties subject to CFIUS legal jurisdiction and their advisors should increase attention to CFIUS compliance requirements and enforcement risks.

If CFIUS determines that a violation occurred, the Committee currently has discretionary authority to:

1. Issue civil monetary penalties, up to $5 million per violation (until December 2024, the previous authorized amount was $250,000 per violation) or the value of the transaction, whichever is greater, for:
    - Failing to file a required CFIUS filing under 31 C.F.R. § 800.401;
    - Material violation of a CFIUS agreement term or condition; and
    - Material misstatements, omissions, or false certification in CFIUS filings.
2. Revoke regulatory "safe harbor" previously granted, and unilaterally initiate a new review of the transaction;
3. Negotiate a mandatory violation remediation plan;
4. Require a party to mandatorily file with CFIUS all future transactions subject to CFIUS jurisdiction for five years; and/or
5. Seek injunctive relief (31 C.F.R. § 800.901(a)(b),(c); 50 U.S.C. § 4565(b)(1)(D)(ii, iii); 50 U.S.C. § 4565 (l)(3)(A)(i, iii); 31 C.F.R. § 800.902(a), (b), (c).).

Each of these authorities has the potential for major legal and reputational consequences to the violator. To date, CFIUS has used only civil monetary penalties for enforcement, but CFIUS may use multiple civil enforcement authorities in the future.

Recent CFIUS civil monetary penalties

As noted earlier, CFIUS issued six civil monetary penalties in 2024 and 2023, as stated earlier. The significance of each civil monetary penalty is discussed below.

2024: As widely reported, telecommunications company T-Mobile paid a $60 million civil penalty for multiple violations in 2020 and 2021 of its 2018 NSA with CFIUS. T-Mobile reportedly failed to prevent unauthorized access to NSA-sensitive data and failed in certain instances to inform CFIUS promptly, delaying CFIUS's ability to investigate and mitigate potential national security harm to U.S. government agencies.

- The Committee rarely identifies companies with CFIUS agreements because of CFIUS statutory confidentiality provided to all CFIUS filers, but CFIUS did so in this instance because T-Mobile had already publicly reported the existence of its NSA (50 U.S.C. § 4565(c).).
- Data and cybersecurity is an increasing focus of the Committee (and the U.S. government writ large, especially in light of recent revelations regarding Chinese exploitation of U.S. telecommunications infrastructure). As a result, most CFIUS NSA agreements signed today have detailed data and/or cybersecurity requirements (e.g., data storage and access requirements and compliance with industry cybersecurity standards).

2024: A $1.25 million civil penalty against a transaction party that submitted five material misstatements to CFIUS (including forged documents and signatures) in its filing with CFIUS and during transaction review. The Committee ultimately rejected the filing, and the transaction was abandoned.

- CFIUS routinely conducts its own due diligence on statements made to the Committee, including using U.S. intelligence community resources. False statements to CFIUS and/or omitting relevant information in communication with the Committee is viewed extremely negatively by CFIUS.

2024: An $8.5 million civil penalty against a company with an NSA for the company's majority shareholders removing all of the company's NSA-required independent directors (causing the NSA security director position to be vacant and NSA government security committee to become defunct).

- NSA requirements related to independent (often U.S. person) board management are typically reserved for foreign investments with the most significant U.S. national security risks. Removing independent directors without CFIUS approval is a significant NSA violation, as evidenced by the $8.5 million penalty.

2023: A $990,000 civil penalty against a company with an LOA (Letter of Assurance) for twice failing to maintain an LOA-required statement on its corporate website concerning its foreign ownership. CFIUS determined that these violations potentially

limited the company's customers' (actual and potential) knowledge of the foreign ownership, which may have placed at risk these customers' data and technology.

- Given that the violation was of an LOA and not an NSA, the LOA was likely signed before CFIUS's 2018 statutory changes, after which NSA became used more often. This penalty highlights that CFIUS monitors companies for compliance for many years after the LOA/NSA is signed.

2023: A $200,000 civil penalty against a company with an NSA for failing to divest its foreign acquirer's interest in the company before the NSA-required date.

- The Committee is often willing to work with companies facing divestment requirements. However, it will not accept the lack of diligent efforts to divest.

2023: A $100,000 civil penalty against a company with an NSA for failing to divest its

foreign acquirer's interest in the company before the NSA-required date.

Final comments

Given the growing CFIUS civil monetary penalties posture of CFIUS, parties subject to CFIUS legal jurisdiction and their advisors should increase attention to CFIUS compliance requirements and enforcement risks.

- Investors and companies operating in CFIUS-sensitive sectors, such as advanced technology, sensitive data and critical infrastructure, should seek out expert counsel and professional advisory services to understand the CFIUS regulatory environment and enforcement risk environment.
- Notifications, declarations and statements to CFIUS must be carefully scrutinized by persons with appropriate expertise, knowledge and authority for completeness and accuracy.
- If a CFIUS NSA is negotiated, parties must ensure that all mitigation provisions are understood, executable, resourced and accountably implemented.
- Finally, if a transaction is targeted for compliance investigation and possible enforcement action, parties must ensure that appropriate expertise and capabilities are engaged to respond timely, transparently and accountably.

Without a doubt, implementing these recommendations implicates real investment of scarce time, attention and financial resources by transaction parties. But failure to appropriately account for and invest in capabilities to address CFIUS compliance requirements may expose investors, companies and related parties to significant enforcement penalties and the potential for additional legal, transaction and other reputational consequences.

About the authors



Barbara Linney (L) is a partner in the Washington, D.C., office of **Baker & Hostetler LLP**. She has more than 30 years' experience representing U.S. and foreign-based clients in CFIUS and other international trade, export controls, sanctions and defense security matters. **Randy Cook** (C) is a managing director at consulting firm **Alvarez & Marsal** and is based in New York. He serves as a third-party monitor and auditor for companies subject to CFIUS national security compliance agreements. He also advises companies on U.S. export controls and sanctions matters and his experience includes serving as a federal prosecutor, law firm and in-house attorney, and U.S. Army officer. **Scott Jansen** (R), an international trade attorney in Washington, D.C., was most recently with Baker & Hostetler LLP, where he represented clients in CFIUS, export control and sanctions matters. A retired Air Force JAG, he previously served at the Department of Defense CFIUS office, where he primarily focused on CFIUS compliance matters, to include CFIUS penalties.

This article was first published on Reuters Legal News and Westlaw Today on February 13, 2025.