Cooley

As CFIUS Announces Significant Penalties, Companies and Investors Confront a Shift in CFIUS Filing Cost-Benefit Dynamics

September 24, 2024

On the heels of releasing its 2023 Annual Report to Congress, the Committee on Foreign Investment in the United States (CFIUS) publicly announced six new penalties on parties that failed to comply with CFIUS requirements in connection with cross-border transactions. The penalties range from $100,000 to a staggering $60 million fine for T-Mobile's alleged violation of the terms of a National Security Agreement (NSA), imposed as a condition of CFIUS's approval of T-Mobile's merger with Sprint.

These penalties mark a significant shift in the government's enforcement posture and its signaling to the market regarding compliance. Indeed, in its nearly 50-year history, CFIUS previously issued only two penalties. Going forward, parties to cross-border transactions may fairly conclude that this shift portends a significant change in the cost-benefit dynamics of voluntary CFIUS filing decisions.

Specifically, with CFIUS increasingly using NSAs to manage perceived national security risks, increasingly relying on standardized NSA templates as a basis for negotiations, and closely monitoring NSAs for post-closing noncompliance, parties may find the costs of voluntarily submitting to a CFIUS review rising relative to the potential benefits of receiving CFIUS clearance.

1. Shifts in CFIUS enforcement tools and posture

Since the passage of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) to strengthen and modernize CFIUS, CFIUS has marshalled and directed substantial resources (including hiring large numbers of new staff) to monitoring and enforcement efforts. These efforts include establishing an enforcement office within the Department of the Treasury to identify and address potential NSA violations and issue penalties for noncompliance.

With respect to penalties for NSA violations, FIRRMA authorizes CFIUS to fine parties up to $250,000 or the value of the underlying transaction – whichever is greater – **per violation**. As reflected in the penalties described below, where CFIUS identifies multiple violations of an NSA, it can aggregate several fines in a single enforcement action. Seeking even greater deterrence powers, in April 2024, CFIUS issued a proposed rulemaking to increase penalties per violation up to $5 million or the value of the underlying transaction – whichever is greater – per violation. In parallel with this increase in penalties, the legal threshold for imposing penalties has been sharply lowered. Prior to FIRRMA, the relevant legal standard was whether a party "intentionally or through gross negligence" violated a material provision of an NSA (see 31 CFR § 800.801 (2017)). Post-FIRRMA, the CFIUS regulations now impose a strict liability standard such that CFIUS can impose penalties on "[a]ny person who violates a material provision" of an NSA without reference to intentionality or negligence (see 31 CFR § 800.901 (2024)). Thus, NSA parties can now face penalties for any violation, regardless of cause or intent.

This dual dynamic – a dramatic increase in potential fines accompanied by a strict liability culpability standard – is already changing the cost-benefit calculus for making voluntary CFIUS filings, particularly with respect to the venture capital financings that FIRRMA was in large part designed to address. This changing calculus may account, in part, for the material decline in the number of CFIUS filings from 2022 to 2023.

2. National Security Agreements – negotiation and enforcement

When CFIUS identifies national security concerns arising from a transaction, it can effectively compel the parties to enter into an NSA to mitigate the perceived risks by conditioning CFIUS's approval on the transacting parties' agreement to NSA terms. Historically, NSA terms varied considerably to reflect the specific circumstances of the transaction under review – including the nature of the perceived national security vulnerabilities presented by the US business and threats presented by the foreign party. Recently, however, and partly in an effort to improve efficiency, CFIUS has pivoted to the use of "standardized" NSA templates and shown reluctancy to negotiate modifications to its standard NSA terms and definitions.

While standard NSA templates may work reasonably well for late-stage companies and large institutional investors, unintended consequences of this efficiency drive are emerging. One such consequence is that smaller US companies (e.g., startups raising venture funding) are increasingly faced with the choice of abandoning their transactions or agreeing to NSAs with the same burdensome terms, conditions and compliance obligations that are imposed on large Fortune 100 or public companies that have greater resources to comply with NSA requirements. For example, in cases where an NSA requires a third-party monitor and/or auditor, NSA compliance can cost $1 million or more annually – a challenging, if not impossible, burden for an early-stage company.

The 2023 Annual Report states that CFIUS adopted mitigation measures and conditions in 43 instances last year, representing "approximately 18 percent" of the total number of 2023 CFIUS notices. Another way of interpreting those data is to say that mitigation was required for nearly a quarter (i.e., 23%) of **distinct** notices submitted to CFIUS for review (i.e., counting a transaction only once if the parties withdrew and resubmitted a filing to address the expiration of the regulatory deadline for completing CFIUS reviews and investigations). As of the end of 2023, CFIUS reported that it had 246 active mitigation agreements in place – about 20% of which were entered into in 2023 alone.

CFIUS also is strengthening its monitoring and enforcement efforts with respect to ensuring compliance with NSAs after they are accepted. CFIUS reports that the CFIUS Monitoring Agencies (CMAs) that monitor compliance with NSA terms conducted 43 site visits in 2023. During these site visits, CMA personnel conduct compliance-focused interviews with senior executives and line-level personnel, review compliance records and assess physical security controls, among other things. Where CMAs identify instances of noncompliance, they pursue remediation efforts and determine whether a civil monetary penalty is appropriate, consistent with the CFIUS Penalty and Enforcement Guidelines.

Regardless of whether enforcement manifests in an NSA negotiated before closing or in connection with a CFIUS-initiated post-closing inquiry, the government's more aggressive enforcement posture has the potential to significantly impact transaction costs.

3. CFIUS penalties – nature and magnitude

From a policy perspective, the number and size of the newly announced penalties are consonant with the proliferation of NSAs. Based on the brief description of each penalty published by CFIUS, it is clear that the range of penalizable offenses is comprehensive – to include misrepresentations to CFIUS during the review process, failures to comply with substantive national security commitments and lack of diligent compliance with procedural NSA requirements.

- In 2024, CFIUS issued a **$60 million penalty** against T-Mobile for violation of an NSA arising from T-Mobile's 2018 merger with Sprint. Citing T-Mobile's failures to prevent and report instances of unauthorized access to certain sensitive data implicating US national security, CFIUS issued the largest penalty in its history.
- In 2024, CFIUS fined an unnamed party a **$1.25 million penalty** for including material misstatements in a CFIUS filing that included forged documents and signatures, and in which the foreign acquirer misrepresented the source of funding for the transaction and other matters. CFIUS ultimately rejected the defective filing, spurring the parties to abandon the transaction. While the $1.25 million penalty represented the maximum authorized fine under the current CFIUS regulations, CFIUS seeks in a rulemaking to increase that cap to $5 million per violation.
- In 2024, CFIUS issued an **$8.5 million penalty** for failure to comply with an NSA. CFIUS determined that the penalized company's majority shareholders orchestrated an effort to remove all independent directors, thereby causing the security director position to be vacant and the board's government security committee to be defunct in violation of an NSA. Although not named in the CFIUS announcement, the penalized company appears to be TuSimple, an autonomous driving technology company, which announced a settlement with CFIUS in May 2024 for events that occurred in 2022.

- In 2023, CFIUS issued a **$990,000 penalty** for two violations of an NSA. CFIUS determined that on two occasions the US business failed to maintain a statement on its website regarding its foreign ownership, as the NSA required. Aggravating factors contributing to the penalty included the duration of the violations, managerial involvement in the violations, failure to self-disclose the violations and the US business's lack of compliance procedures and training.
- In 2023, CFIUS issued a **$200,000 penalty** for failure to consummate the divestiture of a foreign acquirer's interest in a US business by the deadline specified in the governing NSA. While acknowledging the particularly difficult market conditions that prevailed during the COVID pandemic, CFIUS nonetheless issued the penalty, citing repeated violations of other NSA provisions, prolonged failure to make serious efforts to divest and the transaction party's failure to timely inform CFIUS of its failure to meet the divestment deadline.
- In 2023, CFIUS issued a **$100,000 penalty** for failure to divest a foreign acquirer's interest in a US business by the NSA deadline. While again acknowledging difficult market conditions during the COVID pandemic, and the penalized party's small size and lack of sophistication, CFIUS issued the penalty, again finding repeated violations of other NSA provisions, prolonged failure to make serious efforts to divest and failure to timely notify CFIUS that it would be unable to meet the divestment deadline.

Clearly discernable from the range of violations resulting in penalties is the importance for NSA parties to:

- Carefully negotiate NSA terms that are consistent with business operations and realities – and therefore easier to comply with.
- Ensure that the parties and the government have a meeting of the minds regarding the meaning of NSA requirements.
- Strictly comply with NSA terms after closing.

CFIUS is demonstrating its willingness and ability to penalize parties even when there are mitigating factors behind the penalized noncompliance – such as unfavorable market conditions, limited party sophistication and resources, and co-party culpability. With CFIUS insisting on complex NSA terms and aggressively pursuing penalties for any violation, parties are forced to confront a difficult question: Is submitting a voluntary filing that could result in an NSA worth the benefit of receiving safe harbor approval? It's a cost-benefit analysis that transaction parties must consider in today's marketplace.

4. Enforcement is up, CFIUS filings are down

Perhaps in part as a consequence of emerging NSA negotiation and enforcement dynamics, and the evolving cost-benefit assessments concerning voluntary CFIUS filings, the total number of CFIUS filings in 2023 was down nearly 23% from the previous year. In 2023, CFIUS reviewed 109 declarations of "covered transactions" (i.e., transactions subject to CFIUS jurisdiction) and 233 notices of covered transactions. Compare those figures to 2022, where CFIUS reviewed 154 declarations of covered transactions and 286 notices of covered transactions. 2023 saw the lowest number of notices reviewed since 2020.

This decrease in filings makes it difficult to assess CFIUS's claims of improved efficiency in the review and disposition of transactions submitted for review. While the 2023 Annual Report notes that more transactions are clearing in shorter time frames, and that fewer cases are requiring a withdrawal and refile to "restart" the CFIUS clock, these trends might be attributable not only to improved processes within CFIUS, but also to the reduced number of filings submitted and the additional resources (i.e., funding and personnel) CFIUS has to manage its workload. The "efficiencies" might even obscure more negative trends impacting transacting parties' cost-benefit assessments concerning the CFIUS process.

Indeed, one interpretation of the dynamics behind a more "efficient" CFIUS process is that there is an increasing reluctance among transacting parties to submit voluntary filings in the first place. From a cost-benefit perspective, obtaining CFIUS clearance for a transaction will always constitute a valuable – if often not necessary – benefit to certain parties. Anecdotally speaking, however, the cost of pursuing that benefit appears to be increasing and uncertain. From the perspective of the transacting parties, CFIUS "costs" manifest not only in the expense of undergoing a formal CFIUS review and potential investigation, but also in the operational and financial burdens of negotiating and complying with NSA terms. As CFIUS appears to be increasingly turning to NSAs to manage perceived national security risks, and relying increasingly on standard NSA templates as a basis for negotiations, the costs of submitting a voluntary CFIUS filing become correspondingly high and uncertain.

This trend – combined with FIRRMA's strict liability standard and CFIUS's pivot to a more aggressive enforcement posture – can create significant disincentives for transaction parties to submit voluntary CFIUS filings, ample uncertainty to justify foregoing filings in the first place, and a decision to assume the risk of a post-closing CFIUS inquiry.

While only CFIUS has insight into all CFIUS filings and outcomes, in our experience, the current enforcement environment is influencing many transacting parties to structure transactions to limit CFIUS exposure and avoid making voluntary filings. For smaller companies and transactions, in particular, the dilemma is clear: With CFIUS effectively forcing complex and costly NSA terms on an increasing number of transactions, running NSA negotiations on accelerated timelines that do not take commercial realities into account, adhering to templatized NSAs containing ambiguous and ill-fitting terms, and then assessing substantial penalties for noncompliance, fewer transaction parties are willing to subject themselves to a voluntary review by CFIUS and the uncertainties that come with it. Simply put, the value proposition has shifted away from submitting voluntary filings as parties become more reluctant to undergo a CFIUS review unless a filing is legally required.

5. Non-notified transactions/post-closing CFIUS inquiries

Since 2020, when CFIUS began reporting its "non-notified" figures reflecting instances of CFIUS-initiated inquiries concerning transactions that were not affirmatively notified to CFIUS before closing, CFIUS has initiated inquiries into 396 non-notified transactions. These inquiries resulted in 60 post-closing CFIUS filings – an approximately 15% "hit" rate.

Although the number of non-notified inquiries has declined since 2020, the percentage of such inquiries resulting in formal requests for filings has increased, perhaps reflecting a more targeted and sophisticated approach by CFIUS. Nearly 27% of non-notified inquiries in 2023 resulted in a filing, compared with 23% in 2022 and only 6% in 2021.

CFIUS uses various methods to identify non-notified transactions – including referrals from other government agencies that become aware of a transaction, tips from the public, classified reporting, media reports, voluntary self-disclosures, congressional notifications, and multiple commercial and proprietary databases, including the Refinitiv database. CFIUS continues to hire staff to identify and evaluate potential non-notified transactions. With additional resources and dedicated staff, transaction parties should expect to see increased post-closing scrutiny of transactions that present perceived national security risks. In light of the enforcement dynamics and costs discussed above, parties must consider the risk, likelihood and cost of a post-closing CFIUS inquiry as part of their deal risk calculus.

These risks and costs include the specter of penalties for failing to make mandatory filings when required. While CFIUS has not yet issued penalties for failure to make a mandatory filing, in 2023, it began issuing formal letters to parties notifying them that they had missed a mandatory filing and were in noncompliance. Now that the market has been put on notice, we expect CFIUS to begin issuing penalties for failure to comply with mandatory filing provisions in the near term.

Conclusion

Given the fact that nearly a fourth of all notices result in NSAs, the difficulty and expense of complying with complex NSA terms, and the significantly increased monitoring and enforcement posture from CFIUS reflected in these newly announced penalties, transaction parties need to carefully consider the impact of an NSA within their overall cost-benefit analysis and account for that risk in the commercial deal terms. CFIUS is certainly flexing its regulatory muscle, demonstrating that it has the resources, capability and resolve to heavily enforce its authorities. With the backing of the president and Congress, CFIUS is emboldened to impose its will on transaction parties. Transaction parties will continue to face increased CFIUS scrutiny, so it is more important than ever for them to be aware of CFIUS developments and factor CFIUS risks into their transactions so they are not caught off guard by the regulatory watchdog.

Key Contacts

Christopher Kimball Washington, DC	ckimball@cooley.com +1 202 842 7892
Dillon Martinson Washington, DC	dmartinson@cooley.com +1 202 728 7092