TAKE THE MONEY AND RUN: THE DISINCENTIVE MATRIX OF VOLUNTARY CFIUS FILINGS FOR AMERICAN COMPANIES IN THE AGE OF NATIONAL SECURITY PROTECTIONISM

MATTHEW FLOYD*

* J.D. Candidate, American University Washington College of Law (2026); B.A. concentration in International Law, Georgetown University (2021). I am first and foremost grateful to my wife, Emma Floyd, for her unwavering support and endless cheerleading throughout law school. Thank you to the incredible staff of the *Administrative Law Review*, particularly Ainnir O'Regan and Isabelle Stringer, whose edits brought this piece to life. And finally, to my father, Price Floyd, whose stories serving our country's foreign policy establishment inspired me to be an engaged American, voracious reader, and learned of all things national security.

INTRODUCTION

The United States is the world's top destination for Foreign Direct Investment (FDI).[1] There is a bipartisan consensus that FDI is good for the American economy—it supports job growth, allows industry expansion, and facilitates nearly a quarter of all exports.[2] As FDI has grown, so too has the national security interest in the critical technologies, critical infrastructure, and data that drive the U.S. economy.[3] The Department of the Treasury's (Treasury's) Committee on Foreign Investment in the United States (CFIUS or the Committee)[4] is charged with preventing foreign persons from

1. CATHLEEN D. CIMINO-ISAACS & KAREN M. SUTTER, CONG. RSCH. SERV., IF10177, COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS) 1 (2025); *see also* SHAYERAH I. AKHTAR & CATHLEEN D. CIMINO-ISAACS, CONG. RSCH. SERV., IF10636, FOREIGN DIRECT INVESTMENT: BACKGROUND AND ISSUES 1 (2025) (defining FDI in part as "cross-border investment that occurs when a resident of one country obtains a lasting interest in and degree of influence over the management of a business in another country").

2. U.S. DEP'T OF COM., OFF. OF THE UNDER SEC'Y FOR ECON. AFFS., FOREIGN DIRECT INVESTMENT IN THE UNITED STATES 1 (2024), https://www.commerce.gov/sites/default/files/2024-10/FDI-Report-Final.pdf [https://perma.cc/SQ8Q-LM6G] ("For decades and across administrations, the United States has provided foreign companies with a stable and welcoming market in which to invest.").

3. *See generally The Committee on Foreign Investment in the United States (CFIUS)*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius [https://perma.cc/3HBY-3TMV] (last visited Oct. 25, 2025).

4. Committee on Foreign Investment in the United States (CFIUS) is an interagency body chaired by the Department of the Treasury and made up of members including, but not limited to, the Department of Justice, Department of Homeland Security, Department of Commerce, Department of Defense, Department of State, Department of Energy, Office of the U.S. Trade Representative, and the Office of Science & Technology Policy. *See CFIUS Overview*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-overview [https://perma.cc/5VCG-NRSW] (last visited Oct. 25, 2025) [hereinafter *CFIUS Overview*,

purchasing and gaining access to U.S. businesses that work in these areas of critical technology, critical infrastructure, and sensitive personal data (TID U.S. businesses).[5] Treasury has always articulated that its review of foreign investment is specifically tailored to those critical industries that could impact national security.[6] Recently, the Biden Administration labeled this long-standing U.S. policy, "small yard, high fence."[7] The "small yard, high fence" doctrine holds that while the number of critical industries reviewed by Treasury, "yards," would be small, the investment restrictions, "fences," placed on those industries would be high.[8] The yard, however, has proven to be bigger than originally thought.

The U.S. government's understanding of what presents a national security threat has expanded as global economic competition becomes an increasing priority.[9] Specifically, national security has expanded to encompass a wide variety of industries including food security and water, healthcare, artificial intelligence, telecommunications and media, and critical infrastructure.[10] Because of the ever-expanding nature of what constitutes a national security threat, U.S.

TREASURY]. CFIUS conducts an interagency "review" of a filing made by the parties to determine if there is a potential national security threat that could arise because of the transaction. *Id.*

5. 45 U.S.C. § 4565(a)–(b); 31 C.F.R. § 800.248 (2025) ("*TID U.S. business* means any U.S. business that: (a) [p]roduces, designs, tests, manufactures, fabricates, or develops one or more critical technologies; (b) [p]erforms the functions . . . with respect to covered investment critical infrastructure; or (c) [m]aintains or collects, directly or indirectly, sensitive personal data of U.S. citizens.").

6. *See The Committee on Foreign Investment in the United States (CFIUS)*, *supra* note 3.

7. Geoffrey Gertz, Opinion, *Goodbye to Small Yard, High Fence*, N.Y. TIMES (Dec. 31, 2024), https://www.nytimes.com/2024/12/31/opinion/china-semiconductor-biden-xi.html [https://perma.cc/MXB8-ZNNN].

8. *Id.*

9. *See* CIMINO-ISAACS & SUTTER, *supra* note 1, at 1 ("In 2018, Congress passed the Foreign Investment Risk Review Modernization Act (FIRRMA[)] . . . which expanded CFIUS's jurisdiction and review process in key ways. FIRRMA was intended to 'strengthen and modernize' CFIUS and enhance its ability to address concerns involving nonpassive, noncontrolling investments (e.g., minority stake) in TID business and real estate transactions . . . ."); *see also* Christopher M. Tipler, Comment, *Defining 'National Security': Resolving Ambiguity in the CFIUS Regulations*, 35 U. PA. J. INT'L L. 1223, 1249 (2014) ("[T]he Committee's reach seems to be expanding, adding further murkiness to the national security standard.").

10. Dimitri Slobodenjuk, Jennifer Storey, Mark Currell & Renée Latour, *The Evolving Concept of National Security Around the World*, GLOB. COMPETITION REV. (Nov. 25, 2024), https://globalcompetitionreview.com/hub/fdi-regulation-hub/fourth-edition/article/the-evolving-concept-of-national-security-around-the-world [https://perma.cc/3WR6-269D].

companies are playing a guessing game as to whether their business meets CFIUS's conception of a TID U.S. business that CFIUS would regulate.[11]

U.S. businesses that have cause to believe they are a TID U.S. business may voluntarily file their transaction with CFIUS either prior to a foreign person acquiring their assets or after the transaction is completed.[12] If the transaction is approved, the business is granted "safe harbor" status and will not be subjected to a future CFIUS investigation.[13] If the transaction is not approved after interagency review,[14] the U.S. business must either withdraw from the deal, engage in a national security agreement (NSA or mitigation agreement), or have the deal referred to the President for ultimate review.[15] Alternatively, U.S. businesses that determine their transaction does not require a mandatory filing can choose not to file with CFIUS at all.[16] This can

---

11. *See* Ezra Borut, Rick Sofield, Jordan Corrente Beck & John M. Satira, *To File, or Not to File: The Changing Calculus for Voluntary CFIUS Filings*, 24 PRIV. EQUITY REP., Fall 2024, at 8.

12. 31 C.F.R. § 800.501 (2025).

13. *CFIUS Overview*, TREASURY, *supra* note 4 ("Where CFIUS has completed all action with respect to a covered transaction or the President has announced a decision not to exercise his authority under section 721 with respect to the covered transaction, then the parties receive a 'safe harbor' with respect to that transaction . . . ."); *see also* 31 C.F.R. § 800.508(d) (2025).

14. The CFIUS interagency process operates by consensus such that each agency member of CFIUS must approve of a proposed transaction before Treasury can grant final approval. *See generally* LATHAM & WATKINS LLP, COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES KEY QUESTIONS ANSWERED 1–2 (2025), https://www.lw.com/admin/upload/SiteAttachments/CFIUS-Booklet-Key-Questions-Answered-2025.pdf [https://perma.cc/8P9L-PJ6P].

15. CFIUS may impose a national security agreement (NSA) with the parties to the transaction as a condition for approval. *See CFIUS Mitigation*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-mitigation [https://perma.cc/MY7B-FLK2] (last visited Oct. 25, 2025). This agreement might require the U.S. seller to prevent foreign persons from working on projects subject to export controls, selling off assets CFIUS deems sensitive to another U.S. company, or subjecting the parties to monitoring and compliance requirements, where CFIUS conducts audits and site visits. U.S. GOV'T ACCOUNTABILITY OFF., GAO-24-107358, FOREIGN INVESTMENT IN THE U.S.: EFFORTS TO MITIGATE NATIONAL SECURITY RISKS CAN BE STRENGTHENED 11–13, 16 (2024). "Since 2000, the number of mitigation agreements has grown steadily, rising roughly fourfold in the last decade." *Id.* at ii. In 2024, there were 242 active CFIUS mitigation agreements. CFIUS, ANNUAL REPORT TO CONGRESS 39 (2024) [hereinafter "CFIUS, ANNUAL REPORT TO CONGRESS"]; *see also CFIUS Overview*, TREASURY, *supra* note 4.

16. 31 C.F.R. § 800.401 (2025). Parties to a transaction "shall submit to the Committee a declaration with information regarding" that transaction where the transaction is "a covered transaction that results in the acquisition of a substantial interest in a TID U.S. business by a

leave the foreign buyer vulnerable to Treasury's penalty and enforcement scheme if a national security threat is found and all the U.S. business's assets were sold to the foreign buyer.[17] If a U.S. business is selling all of its assets to the foreign buyer, the voluntary filing regime incentivizes U.S. companies not to file because the possibility of CFIUS identifying a national security risk and halting the deal is both unclear and "onerous."[18] The U.S. government's expansive conception of national security, coupled with an absent enforcement posture against U.S. companies that "take the money and run,"[19] creates the very threat CFIUS was charged with eliminating.[20]

Part I of this Comment discusses the statutory development of CFIUS and provides an outline of the Committee's regulatory scope.[21] Part II discusses the ever-expanding concept of national security from both the government and private sector perspective as it pertains to CFIUS filings.[22] Part III evaluates the definitions of TID in TID U.S. business.[23] Part IV identifies the gap in the penalty and enforcement regulations that encourages U.S. businesses not to voluntarily file in certain instances and analyzes a hypothetical transaction.[24] Part V recommends CFIUS, via the Treasury Chair, publish annual guidance regarding the types of transactions that would merit a TID U.S. business to voluntarily file a notice.[25] In addition, Part V recommends amending the penalties and damages provision at § 800.901 to include a penalty and clawback provision that disgorges earnings from U.S. businesses that

---

foreign person in which the national or subnational governments of a single foreign state . . . have a substantial interest," or "a covered transaction involving a TID U.S. business that produces, designs, tests, manufactures, fabricates, or develops one or more critical technologies for which a U.S. regulatory authorization would be required." *Id.*; *see* description of mandatory filings *infra* Section I.B.2.

17. *See* 31 C.F.R. § 800.901 (2025).

18. Borut et al., *supra* note 11, at 9.

19. *Take the Money and Run* is a song by the Steve Miller Band from their 1976 album *Fly Like an Eagle*. STEVE MILLER BAND, *Take the Money and Run*, *on* FLY LIKE AN EAGLE (Capitol Records 1976). The song is about two young lovers (Billy Joe and Bobbie Sue) who robbed an establishment in El Paso, Texas during which Billy Joe shot someone. Steve Miller Band, *Take the Money and Run*, GENIUS, https://genius.com/Steve-miller-band-take-the-money-and-run-lyrics [https://perma.cc/3HZ9-5QAA] (last visited Oct. 25, 2025). Bobbie Sue ran off with the money and was pursued by detective Billy Mack who "makes his living off of the people's taxes." *Id.* The song reached number 11 on Billboard's Hot 100 in 1976. *Id.*

20. *See CFIUS Overview*, TREASURY, *supra* note 4.

21. *See* discussion *infra* Part I.

22. *See* discussion *infra* Part II.

23. *See* discussion *infra* Part III.

24. *See* discussion *infra* Part IV.

25. *See* discussion *infra* Part V.A.

sell all of their assets where the transaction is found to pose a national security threat post-closing.[26]

I. HISTORY, PURPOSE, AND REGULATORY POWER OF THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES

On May 7, 1975, President Ford created CFIUS via executive order to "review investments in the United States which . . . might have major implications for United States national interests."[27] After its inception, the Committee was slow to start and purportedly only met ten times between 1975 and 1980, reflecting a far more languid version of the Committee than what it is today.[28] In that period, CFIUS had neither bark nor bite and was unable to take any action beyond simple review and reporting of foreign investment activity.[29] However, in 1988, CFIUS sharpened its teeth with the passage of the Exon-Florio amendment to the Defense Production Act of 1950 (DPA).[30] With Exon-Florio in place, CFIUS could review foreign investment transactions and subsequently recommend them to the President, who was empowered "to investigate, suspend, or prohibit any foreign mergers, acquisitions, or takeovers that could harm U.S. national security interests."[31]

The next major statutory development for CFIUS came with the passage of the Foreign Investment & National Security Act of 2007 (FINSA),[32] which brought, among other changes, a requirement that "[a]t no lower than the Assistant Secretary level, Treasury and the lead agency must certify to Congress that CFIUS had 'no unresolved national security concerns' in any review it conclude[d]."[33] The certification requirement elevated the nature of

26. *See* discussion *infra* Part V.B.

27. Exec. Order No. 11,858, 40 Fed. Reg. 20,263 (May 7, 1975); *see also* JAMES K. JACKSON, CONG. RSCH. SERV., RL33388, THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS) 4 (2020) ("According to a Treasury Department memorandum, the Committee was established in order to 'dissuade Congress from enacting new restrictions' on foreign investment, as a result of growing concerns over the rapid increase in investments by Organization of the Petroleum Exporting Countries (OPEC) countries in American portfolio assets (Treasury securities, corporate stocks and bonds) . . . ." (citation omitted)).

28. *See* Heath P. Tarbert, *Modernizing CFIUS*, 88 GEO. WASH. L. REV. 1477, 1484 (2020).

29. *See id.* at 1486.

30. *Id.*; Defense Production Act, 50 U.S.C. § 4565 (creating § 721 of the Defense Production Act (DPA)); *see also* Tarbert, *supra* note 28, at 1485 (stating that Exon-Florio's passage was allegedly in partial response to Japanese owned Fujitsu's attempted 1987 acquisition of the Fairchild Semiconductor Corporation, a U.S. computer chip manufacturer and military contractor).

31. Tarbert, *supra* note 28, at 1486.

32. Pub. L. No. 110-49, sec. 2, § 721,121 Stat. 246.

33. U.S. DEP'T OF THE TREASURY, CFIUS REFORM: THE FOREIGN INVESTMENT &

Committee accountability to Congress such that any approved transaction that was later found to present national security risks could be used as ammunition against a sitting President for being soft on national security.[34] The most recent and significant CFIUS legislation passed by Congress is the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which expanded the scope of what constitutes a covered transaction, extended CFIUS's timeline for review, and strengthened the use of NSAs.[35]

A. CFIUS Jurisdiction and Covered Transactions

Pursuant to § 721 of Title VII of the DPA, CFIUS has jurisdiction "to review any covered transaction, as defined in § 800.213 . . . to mitigate any risk to the national security of the United States that arises as a result of such transactions."[36] Section 800.213 defines a covered transaction as any of the following:

(a) A covered control transaction [which "means any transaction . . . by or with any foreign person that could result in foreign control of any U.S. business"[37]];

(b) A covered investment [which "means an investment, direct or indirect, by a foreign person . . . in an unaffiliated TID U.S. business"[38]];

(c) A change in the rights that a foreign person has with respect to a U.S. business in which the foreign person has an investment, if that change could result in a covered control transaction or a covered investment; or

(d) Any other transaction, transfer, agreement, or arrangement, the structure of which is designed or intended to evade or circumvent the application of section 721.[39]

NATIONAL SECURITY ACT OF 2007 (FINSA) (2008), https://home.treasury.gov/system/files/206/Summary-FINSA.pdf [https://perma.cc/UZG8-ZYQ8]; *see also* FINSA § 721, 121 Stat. at 250.

34. *See generally Oversight of the Committee on Foreign Investment in the United States (CFIUS) and Other Efforts to Strengthen National Security in the United States: Hearing Before the H. Comm. on Fin. Servs.*, 118th Cong. 8–9 (2023) (statement of Hon. Paul Rosen, Assistant Secretary, Investment Security, U.S. Department of the Treasury) (revealing Congress's power to oversee CFIUS as well as its ability to scrutinize the national security posture of the President's appointees).

35. U.S. DEP'T OF THE TREASURY, SUMMARY OF FIRRMA'S KEY PROVISIONS (n.d.), https://home.treasury.gov/system/files/206/Summary-of-FIRRMA.pdf [https://perma.cc/FCC5-WBF3]; *see also* H.R. No. 5515, 115th Cong. § 1701 (2018), *reprinted in* 50 U.S.C. § 4565.

36. 31 C.F.R. § 800.101 (2025).

37. *Id.* § 800.210.

38. *Id.* § 800.211.

39. *Id.* § 800.213.

In sum, CFIUS has broad jurisdiction to review any foreign person's acquisition or attempted acquisition of a U.S. business.[40] Businesses that work in critical technology, critical infrastructure, or sensitive personal data—categories whose definitions have arguable degrees of clarity and confusion—have higher cause to worry about being caught in CFIUS's net because of the possible filing requirements.[41]

B. CFIUS Filing Regimes Explained: Voluntary Notice or Declaration v. Mandatory Declarations

1. Voluntary Notice or Declaration

The CFIUS regulations state that "a party or parties to a proposed or completed transaction *may* file a voluntary notice [or declaration] of the transaction with the Committee" where that transaction is a covered transaction.[42] While a voluntary notice and a declaration follow different procedures, both are filings that inform CFIUS of a proposed merger and acquisition (M&A) deal between a U.S. business and a foreign person.[43] A voluntary notice provides CFIUS with specific details and a comprehensive understanding of the transaction, review of which can last anywhere from 45 to 105 days, if not longer.[44] A voluntary declaration however, is a brief summary document requiring less detail-intensive information and an expedited 30-day assessment period.[45] "Declarations require far less (and far less detailed) information than Notices and do not require the parties to pay a filing fee to the Treasury."[46] If CFIUS is unable to conclude whether there are "national security issues arising from the underlying transaction" from a voluntary declaration, CFIUS might request the parties to file a voluntary notice.[47] However, it is arguable whether the word "request" is appropriate in the instance where a government agency, with the power to investigate and ultimately prevent your transaction, is *suggesting* you do something. Rather, the request appears compulsory. Law firms with CFIUS practice groups are constantly advising parties to cross-border M&A deals on "whether to submit a voluntary CFIUS

40. *Id.* § 800.211.

41. *Id.*; *see also id.* § 800.401.

42. *Id.* § 800.501(a) (emphasis added).

43. *Id.*

44. *See CFIUS Overview*, COOLEY, https://www.cooley.com/services/practice/cfius/cfius-overview [https://perma.cc/HDV4-M7MN] (last visited Sept. 7, 2025) [hereinafter *CFIUS Overview*, COOLEY].

45. *Id.*

46. *Id.*

47. *Id.*

filing, . . . whether the potential national security risks will be of interest to CFIUS, [and] whether CFIUS might wish to mitigate those risks."[48]

2. Mandatory Declarations

As for mandatory declarations, the CFIUS regulations state that parties to a transaction "*shall* submit to the Committee a declaration"[49] regarding transactions where (1) a foreign state holds a substantial interest in the foreign person participating in the covered transaction;[50] or (2) a foreign person could directly control or acquire an interest in "a TID U.S. business that produces, designs, tests, manufactures, fabricates, or develops one or more critical technologies for which a U.S. regulatory authorization would be required."[51]

In essence, mandatory declarations are a more robust filing that act as a tool to prevent foreign governments from using U.S. companies for nefarious purposes and to prevent private foreign persons from gaining control or knowledge of critical technologies that would otherwise require an export control license.[52]

II. WHAT IS NATIONAL SECURITY?

A. The Defense Production Act, Key Terms Defined

Under the DPA, national security issues are defined as those "relating to 'homeland security[,'] including its application to critical infrastructure."[53] Further, "homeland security" is defined by § 4552 of the DPA as "efforts" to prevent, reduce, minimize, and recover from acts of terrorism against the United States.[54] Considering that CFIUS gained prominence after 9/11, as an additional national security tool in the U.S. government's arsenal, such an interpretation of national security and homeland security makes sense.[55] The issue with the statutory definitions and their association with terrorism, however, is that they do not reflect how CFIUS perceives and reviews the threat of foreign investment in the United States today.[56] CFIUS is not

48. *Id.*
49. 31 C.F.R § 800.401(a) (2025) (emphasis added).
50. *Id.* § 800.401(b)(1).
51. *Id.* § 800.401(c)(1).
52. *See id.*
53. Defense Production Act, 50 U.S.C. § 4565(a)(1).
54. *Id.* § 4552(11).
55. *See* JACKSON, *supra* note 27, at 17.
56. *See* Memorandum on America First Investment Policy, 2025 DAILY COMP. PRES. DOC. 292 (Feb. 21, 2025) (labeling corporate entities, China, and other State actors as the dominant threat within foreign investment).

spending its time monitoring illicit equity purchases by the Taliban, Al-Qaeda, or ISIS—groups associated with terrorism.[57] Instead, CFIUS is reviewing everyday transactions like the German telecommunications company Deutsche Telekom's (T-Mobile's) acquisition of Sprint, a U.S. telecommunications company.[58] In that instance, CFIUS penalized the U.S. subsidiary, T-Mobile US, $60 million for failing to prevent unauthorized access to sensitive data (likely U.S. personal data) and other instances of unauthorized access (potentially access to critical telecom infrastructure).[59] The national security threat there was not terrorism, nor was the foreign person from a country with national security interests adversarial to the United States.[60]

One way of discerning a statutory understanding of national security is by turning to what the DPA defines as critical infrastructure.[61] Critical infrastructure "means any systems and assets, whether physical or cyber-based, so vital to the United States that the degradation or destruction of such systems and assets would have a debilitating impact on national security, including, but not limited to, national economic security and national public health or safety."[62] A plain language statutory interpretation of national security, then, is the protection of any system or asset that is "vital" to the United States and its economic welfare, public health, or safety. [63] What is

57. *See id.*

58. *CFIUS Enforcement*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-enforcement [https://perma.cc/7GTA-A2M8] (last visited Oct. 25, 2025).

59. *Id.*

60. Germany has been a NATO ally of the United States since its accession to the organization in 1955. *See NATO Member Countries*, N. ATL. TREATY ORG., https://www.nato.int/cps/en/natohq/topics_52044.htm [https://perma.cc/W8SQ-NBQU] (Mar. 11, 2024, 3:11 PM).

61. Defense Production Act, 50 U.S.C. § 4552(2).

62. *Id.* In fact, CFIUS legislation, at the time the Foreign Investment and National Security Act of 2007 (FINSA), adopted the definition of "critical infrastructure" from the Patriot Act of 2001 and the Homeland Security Act of 2002. *See* JACKSON, *supra* note 27, at 17; *see also* USA PATRIOT ACT of 2001, 42 U.S.C. § 5195c(e) (defining critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"); Homeland Security Act of 2002, 6 U.S.C. § 101(4) (same); FINSA, Pub. L. 110-49, sec. 2, §§ 5–6, 121 Stat. 246, 247 (clarifying "[t]he term 'national security' . . . to include those issues relating to 'homeland security', including its application to critical infrastructure" and defining critical infrastructure to mean "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security").

63. 50 U.S.C. § 4552(2).

considered "vital" is determined by the political prerogatives of the sitting President as well as his or her cabinet who make up CFIUS and choose which foreign investment transactions to review.[64] Therefore, any investment into an industry, business, health, or economic issue considered vital to the United States can be investigated by CFIUS.[65] Consequently, any issue can be a national security issue.[66]

The national security factors CFIUS employs when reviewing a transaction can also help elucidate CFIUS's conception of national security:[67]

> [T]he President or [CFIUS] may, taking into account the requirements of national security, consider—
>
> (1) domestic production needed for . . . national defense requirements,
>
> (2) the capability and capacity of domestic industries to meet national defense requirements, including the availability of human resources, products, technology, materials, and other supplies and services,
>
> (3) the control of domestic industries and commercial activity by foreign citizens . . . ,
>
> (4) the potential effects of the . . . transaction on sales of military goods, equipment, or technology to any country [regulated by export controls] . . . ;
>
> (5) the potential effects of the . . . transaction on United States international technological leadership . . . ;
>
> (6) the potential national security-related effects on United States critical infrastructure, including major energy assets;
>
> (7) the potential national security-related effects on United States critical technologies;
>
> (8) whether the covered transaction is a foreign government-controlled transaction . . . ;
>
> (9) as appropriate, . . . a review of [whether the country follows nonproliferation guidelines, the country's cooperation with the United States on counter-terrorism, and the risk of military technology being illegally transferred or diverted] . . . ;

64. *Id.* § 4565(l); *see also* Memorandum on America First Investment Policy, *supra* note 56 ("Economic security is national security.").

65. *See* 50 U.S.C. § 4565(k); *see also* Memorandum on America First Investment Policy, *supra* note 56.

66. *See* Stephen Heifetz, Opinion, *When 'National Security' Becomes a Political Excuse, We All Lose*, THE HILL (Oct. 26, 2024, 8:00 AM), https://thehill.com/opinion/national-security/4953322-us-steel-nippon-acquisition-criticism/ [https://perma.cc/7RVW-TMYS] ("The parameters of this [national security] exception . . . are not policed by courts or any other independent body, so 'national security' means whatever the governing administration says it means.").

67. *See* 50 U.S.C. § 4565(f).

(10) the long-term projection of United States requirements for sources of energy and other critical resources and material; and

(11) such other factors as the President or the Committee may determine to be appropriate . . . .[68]

These factors provide minimal clarity to U.S. businesses because any response to one factor—and its interplay with another—is entirely subjective. For instance, how could a concrete company (possibly critical infrastructure)[69] know how much concrete is needed for national defense requirements (factors 1 and 2)? Moreover, how could it possibly know the national security effects of allowing itself to be purchased by, for example, a Chilean or Portuguese company (factor 3)?[70] Such an endeavor is entirely speculative and lacks any sort of certainty required for business planning.

B. National Security or Protectionism? U.S. Steel

The most recent and controversial instance of CFIUS identifying a questionable national security threat is Japanese company Nippon Steel's acquisition of U.S. Steel.[71] Nippon Steel initially announced its intent to purchase U.S. Steel in December 2023 for $14.9 billion in cash and debt.[72] President Biden decidedly blocked the deal after CFIUS could not decide whether the deal presented a national security threat.[73] President Biden stated "US Steel has been an iconic American steel company for more than a century, and it is vital for it to remain an American steel company that is domestically owned and operated."[74] Because CFIUS and the President keep their national security analyses confidential, critics reasonably speculated that President

68. *Id.*

69. *See* 31 C.F.R. § 800.214 (2025).

70. *See* U.S. GOV'T ACCOUNTABILITY OFF., *China's Foreign Investments Significantly Outpace the United States. What Does that Mean?*, WATCHBLOG: FOLLOWING THE FED. DOLLAR (Oct. 16, 2024), https://www.gao.gov/blog/chinas-foreign-investments-significantly-outpace-united-states.-what-does-mean [https://perma.cc/PX4P-PSWH].

71. *See* George F. Will, Opinion, *Biden's 'Security' Concern About TikTok and U.S. Steel is Doubly Specious*, WASH. POST, (Jan. 8, 2025), https://www.washingtonpost.com/opinions/2025/01/08/biden-tiktok-us-steel-security/ [https://perma.cc/YBB4-PW93].

72. *See* Fatima Hussein, Josh Boak & Marc Levy, *Biden Blocks $14 Billion Acquisition of US Steel by Japan's Nippon Steel*, ASSOCIATED PRESS, (Jan. 3, 2025, 5:15 PM), https://apnews.com/article/nippon-steel-japan-cfius-economy-biden-099564a3cddca587af0d7340e0c15ed6 [https://perma.cc/E93P-URV6].

73. *See id.*

74. Matt Egan, *Biden Says It's 'Vital' US Steel Remain American Owned and Operated*, CNN (Mar. 14, 2024, 7:52 PM), https://www.cnn.com/2024/03/14/economy/biden-says-us-steel-should-remain-american/index.html [https://perma.cc/U6YB-885M].

Biden's decision to block the deal was a political calculation to drum up electoral support in Pennsylvania.[75] In a stunning reversal of policy, President Trump ordered CFIUS to review the transaction again and permitted the sale of U.S. Steel to Nippon Steel with the contingency that there be a "golden share" provision which allows the U.S. government to hold a board seat in the merged entity and thus control key business decisions.[76] There is a strong national security counterargument: America must retain total control of a reliable supply chain of American steel in the event of global conflict.[77] However, Japan is an ally of the United States, and a Japanese-owned steel company based in the United States would be expected to support the country in industrial production of armaments in the instance of global conflict.[78] Stephen Heifetz, a partner at Wilson Sonsini Goodrich and Rosait, who previously served on CFIUS, stated "[c]oncern about steel production seems like a loincloth for a naked political aim."[79] The national security exception, he said, is "now infinitely malleable."[80]

III. THE "CRITICAL" IN CRITICAL TECH, CRITICAL INFRASTRUCTURE, AND SENSITIVE PERSONAL DATA

Treasury is concerned with preventing the foreign acquisition of U.S. businesses that deal in critical technology, critical infrastructure, and sensitive data, where that acquisition would pose a national security threat.[81] Beyond the ambiguity and elasticity of how the U.S. government perceives national security is the lack of clarity in what types of critical technology, critical infrastructure, and sensitive data will raise CFIUS eyebrows.[82] The

75. *See* Heifetz, *supra* note 66.

76. Marc Levy, *Nippon Steel Finalizes $15B Takeover of US Steel After Sealing National Security Agreement*, ASSOCIATED PRESS (June 18, 2025, 6:42 PM), https://apnews.com/article/trump-us-steel-nippon-steel-golden-share-0bda2cf3c6de313206b481be0baf78cb [https://perma.cc/7CHZ-SL3J] ("Clearly the definition of what is national security has expanded to included national economic security . . . ." (quoting Anil Khurana, Executive Director of the Baratta Center for Global Business at Georgetown University)).

77. Presidential Statement on the President's Order Regarding the Proposed Acquisition of United States Steel Corporation by Nippon Steel Corporation, 2025 DAILY COMP. PRES. DOC. 9 (Jan. 3, 2025) ("Without domestic steel production and domestic steel workers, our nation is less strong and less secure.").

78. *Id.*

79. Heifetz, *supra* note 66.

80. *Id.*

81. *See* 31 C.F.R. § 800.101 (2025) (providing the scope of regulatory coverage for the CFIUS regulations); *see also* 31 C.F.R. § 800.211 (2025) (defining covered investment).

82. Pillsbury assessed Grindr's decision not to voluntarily file and stated that "it would

categories of critical technology, critical infrastructure, and sensitive personal data (TID) present varying levels of confusion to U.S. businesses depending on the level of communication, examples, and past enforcement actions conducted and provided by the Executive Branch.[83]

A. Critical Technology

Critical technology is defined generally as:

(a) Defense articles or defense services included on the United States Munitions List (USML) . . . ;

(b) Items included on the Commerce Control List (CCL) . . . controlled [in part] for reasons relating to national security, chemical and biological weapons proliferation . . . or . . . regional stability . . . ;

(c) [Anything related to] nuclear equipment, parts and components . . . ;

(d) Nuclear facilities, equipment, and material. . . ;

(e) Select agents and toxins . . . ;

(f) [And finally,] [e]merging and foundational technologies controlled under section 1758 of the Export Control Reform Act of 2018 [which are identified by the Emerging Technology and Research Advisory Committee].[84]

A fundamental dilemma for U.S. businesses attempting to discern whether they should file a voluntary notice or mandatory disclosure, or file at all, is the difficulty in understanding the export control system (by way of the USML and CCL) to determine if the technology they produce is "critical" or "emerging."[85] For example, in response to a 2018 advance notice of

---

have been clear that the [Personally Identifiable Information] held by Grindr was potentially a source of concern" but that a "risk assessment will inform the parties' decision as to whether to make a voluntary filing." Pillsbury, *CFIUS Grounds Grindr IPO*, JDSUPRA (Apr. 1, 2019), https://www.jdsupra.com/legalnews/cfius-grounds-grindr-ipo-50846/ [https://perma.cc/7V6U-22HA]. However, even after a "careful risk assessment" the parties chose not to file, which was against the Chinese buyer's interest. *Id.* This leads one to the rational conclusion that the parties did not believe that the Personally Identifiable Information would raise national security concerns and require a forced divesture. *Id.*

83. *See* 31 C.F.R. § 800.248 (2025).

84. 31 C.F.R. § 800.215(a)–(f); *see also* Export Control Reform Act of 2018, 50 U.S.C. § 4817.

85. Kirsten S. Lowell, *The New "Arms" Race: How the U.S. and China Are Using Government Authorities in the Race to Control 5G Wearable Technology*, 12 GEO. MASON INT'L L.J., no. 2, 2021, at 1, 25 ("Even if companies are not purposefully trying to work around CFIUS review, companies often do not realize they are involved with critical technology."); *see also* 31 C.F.R. § 800.215(f).

proposed rulemaking (ANPRM)[86] by the Department of Commerce to include the undefined and broadly unarticulated term "emerging technology"[87] as part of the definition of "critical technologies"[88] (which would apply to CFIUS regulations under FIRRMA and the export controls system), almost 250 U.S. and foreign corporations, industry associations, and advocacy groups submitted comments.[89] A "consensus" emerged among ANPRM commentators that "urged [Department of Commerce] to reject a broad brush approach to defining 'emerging technologies.'"[90] U.S. businesses who do not know if the technology they produce is "critical" for national security purposes certainly can't be expected to know if the technology they produce is "emerging"—especially when the U.S. government cannot or will not formulate a precise definition themselves.[91] In the promulgation of Treasury's version of this final rule, rather than clarifying the definition of critical technologies and its relation to emerging technologies, Treasury stated "what constitutes a 'critical technology' shall be assessed as of the earliest date of any of the conditions set forth in § 800.104(b)(1)–(4)"—a list of events that can occur in the lifecycle of a transaction.[92] In other words, Treasury and the Department of Commerce have largely ignored U.S. business pleas for clarification on critical technologies.

The U.S. government, however, has a vested interest in retaining an amorphous outline for what constitutes critical technology because it allows for wiggle room when identifying critical or emerging technology in transactions seen as problematic. Moreover, while the engineers and technical staff (who inform export controls) at the Department of Commerce are considered subject matter experts across critical technology fields,[93] the government's

86. Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201 (proposed Nov. 19, 2018) (to be codified at 15 C.F.R. pt. 744).

87. *See* 31 C.F.R. § 800.215(f); Defense Production Act, 50 U.S.C. § 4817.

88. *See* 31 C.F.R. § 800.215.

89. JEFFERY P. CUNARD, ANNA R. GRESSEL, MICHAEL DIZ, JONATHAN E. LEVITSKY, JIM PASTORE & MICHAEL SCHAPER, WHAT IS ON THE HORIZON FOR EXPORT CONTROLS ON "EMERGING TECHNOLOGIES"? INDUSTRY COMMENTS MAY HOLD A CLUE 2 (DEBEVOISE & PLIMPTON 2019), https://www.debevoise.com/-/media/files/insights/publications/2019/09/20190923-tmt-insights-what-is-on-the-horizon.pdf [https://perma.cc/Y8Z2-WZ6N].

90. *Id.*

91. *Id.* at 1–2.

92. Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 85 Fed. Reg. 57,124, 57,126 (Sept. 15, 2020) (codified at 31 C.F.R. pt. 800).

93. *See, e.g.*, *Office of National Security Controls (ONSC)*, BUREAU OF INDUS. & SEC., DEP'T. OF COMMERCE, https://www.bis.gov/ONSC#office-leadership [https://perma.cc/5J9A-9ZX3] (last visited Oct. 25, 2025) ("ONSC engineers and analysts review and process export license

awareness of state-of-the-art technology has lagged in comparison to the private sector's pace of development.[94]

B. Critical Infrastructure

The definition of critical infrastructure in the CFIUS regulations departs slightly from the definition in CFIUS's founding legislation, the DPA.[95] The CFIUS regulations define critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security."[96] The notable distinction in the Code of Federal Regulations is the absence of "economic security and national public health or safety," which is language contained in the DPA definition.[97] This regulatory disappearing act, however, is short lived considering that CFIUS investigates transactions that are tangentially related to national security but certainly related to economic security,[98] public health,[99] and safety.[100] In David

---

applications for items controlled for [National Security] reasons. . . . ONSC is at the forefront of shaping and enforcing policies crucial for safeguarding national security interests related to export controls.").

94. CUNARD ET AL., *supra* note 89, at 2 (reporting that technologies mentioned in the ANPRM, including emerging technologies under the definition of critical technologies, were "already . . . in widespread, commercial use for years").

95. *Compare* 31 C.F.R. § 800.214 (2025), *with* 50 U.S.C. § 4552(2).

96. 31 C.F.R. § 800.214.

97. 50 U.S.C. § 4552(2).

98. *See* Memorandum on America First Investment Policy, *supra* note 56 ("Economic security is national security."); *see also* Aimen Mir, Christine Laciak, Colin Costello & Timothy Swartz, *New CFIUS Executive Order Reflects Evolved CFIUS National Security Risk Analysis*, FRESHFIELDS (Sept. 23, 2022, 4:33 PM), https://blog.freshfields.us/post/102hxrv/new-cfius-executive-order-reflects-evolved-cfius-national-security-risk-analysis [https://perma.cc/LS8Q-UGLS] ("As CFIUS expands its consideration of economic security factors, it will capture an increasing number of transactions where the national security implications may not be obvious or may be more attenuated.").

99. *See* Antonia I. Tzinova, Robert A. Friedman & Marina Veljanovska O'Brien, *New Executive Order Creates Roadmap of Heightened CFIUS Scrutiny for Cross-Border M&A*, HOLLAND & KNIGHT (Sept. 20, 2022), https://www.hklaw.com/en/insights/publications/2022/09/publnew-executive-order-creates-roadmap-of-heightened-cfius-scrutiny [https://perma.cc/7RNE-DZ2F] ("Supply chain shortages over the last three years [including] public health (e.g., COVID-19 prevention and response materials) . . . have widened the national security aperture.").

100. *See* TikTok Inc. v. Garland, 122 F.4th 930, 943 (D.C. Cir. 2024) ("[A]s part of the [NSA] process, 'Executive Branch negotiators engaged in extensive, in-depth discussions with

Copperfield-like fashion,[101] the expansive notion of national security re-appears even when it does not appear in the CFIUS regulations themselves.

However, the DPA and CFIUS regulation's broad definition of critical infrastructure is supplemented by more specific examples of critical infrastructure in Appendix A to Part 800 of the CFIUS regulations.[102] For example, in the appendix, critical infrastructure could be defined as a public water system, a water treatment plant, or an interstate oil pipeline.[103] CFIUS, then, is able to retain its large net of jurisdictional capture with the statutory definition of critical infrastructure in the DPA,[104] while also communicating somewhat clearly to the U.S. business community what specific infrastructure with which CFIUS is concerned[105]

C. Sensitive Personal Data

Data collection is a simple reality of living in the modern world.[106] Providing personal identifiable information (PII) is often a barrier to entry for websites, setting up social media accounts, online shopping, and even ordering food to-go.[107] The CFIUS regulations define sensitive personal data generally to mean:

Oracle, the proposed Trusted Technology Provider, whose responsibility under the proposed mitigation structure included storing data in the United States, performing source code review, and ensuring safety of the operation of the TikTok platform in the United States.'"), *aff'd*, 145 S. Ct. 57 (2025) (per curiam).

101. David Copperfield is a world-renowned magician who is famous for his tricks of illusion including making the Statue of Liberty disappear. *See Biography*, DAVID COPPERFIELD, https://www.davidcopperfield.com/html/biography.html [https://perma.cc/4M77-RX8U] (last visited Oct. 26, 2025).

102. 31 C.F.R. pt. 800, app. A (2025).

103. *Id.*

104. *See* 50 U.S.C. § 4552(2).

105. *See* 31 C.F.R. pt. 800, app. A.

106. *See generally* BROOKE AUXIER, LEE RAINIE, MONICA ANDERSON, ANDREW PERRIN, MADHU KAMAR & ERICA TURNER, PEW RSCH. CTR., AMERICANS AND PRIVACY: CONCERNED, CONFUSED, AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION (2019), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf [https://perma.cc/7Y4P-Z2LY]; *id.* at 2 ("[Data collection] is such a common condition of modern life that roughly six-in-ten U.S. adults say they do not think it is possible to go through daily life *without having data collected about them* by companies or the government.").

107. *See id.* at 2, 37.

(1) Identifiable data that is:

(i) Maintained or collected by a U.S. business that:

(A) Targets or tailors products or services to any U.S. executive branch agency or military department with intelligence, national security, or homeland security responsibilities, or to personnel and contractors thereof;

(B) Has maintained or collected any identifiable data . . . on greater than one million individuals [within the span of a year].[108]

This definition applies to information in the categories of financial data, health insurance, health conditions, electronic communications, geolocation data, biometrics, and data used to generate a state or federal government ID or security clearance.[109]

But what about the information you put into a dating application? In 2019, CFIUS required Kunlun Tech, the Chinese owner of Grindr, a dating application, to resell the application after only owning it for two years.[110] While private digital communications related to romance is not what normally sounds the national security alarm, Grindr held personal data "on its customers, including U.S. officials and government contractors who could be blackmailed or compromised. Moreover, since Grindr use[d] geolocation, it c[ould] track its users' movements."[111] This type of data, and who the data identifies, falls squarely into CFIUS's definition of sensitive personal data that they are concerned with foreign persons obtaining.

IV. THE GAP IN THE CFIUS PENALTY PROVISIONS

CFIUS has the power to impose penalties on parties to a transaction in three instances: (1) where the party submits a filing to CFIUS that contains a material misstatement, contains an omission, or makes a false certification; (2) where a party is required to submit a mandatory declaration and does not; and (3) where a party violates a provision of an NSA made with CFIUS.[112]

The glaring issue here is that the current penalty regulations contain no provisions for situations where the U.S. business sells all their assets *and* the transaction falls under the voluntary filing scheme *but* CFIUS still finds a

108. 31 C.F.R. § 800.241(a)(1) (2025).

109. *Id.* § 800.241(a)(1)(ii).

110. *See* Sarah Bauerle Danzman & Geoffrey Gertz, *Why is the U.S. Forcing a Chinese Company to Sell the Gay Dating App Grindr?*, WASH. POST (Apr. 3, 2019), https://www.washingtonpost.com/politics/2019/04/03/why-is-us-is-forcing-chinese-company-sell-gay-dating-app-grindr/ [https://perma.cc/F4VZ-JQDA].

111. *Id.*

112. 31 C.F.R. § 800.901 (noting that NSA and mitigation agreements are one and the same).

national security threat post-closing.[113] The U.S. business that sells all of its assets unhooks itself from the penalty provisions because (1) there is no penalty provision that covers this scenario, and (2) when CFIUS finds a national security threat post-closing, the former owner of the U.S. business is no longer there (i.e., they are not actively contributing to the national security threat by sharing ownership with a foreign person that would trigger § 800.901(b)).[114] If, however, the U.S. seller retains *any* level of ownership in the business such as an equity stake or maintaining an asset, then CFIUS would be able to penalize the U.S. seller if CFIUS finds that a mandatory filing is required under § 800.901(b) (even if it is an after-the-fact analysis).[115]

In sum, the current penalty regulations lack a provision to cover U.S. businesses that sell all their assets *and* their transaction falls under the voluntary filing scheme. This exact fact pattern has occurred with no consequences for the U.S. seller and drastic consequences (divestment) for the foreign buyer.[116] Not only does this gap in the penalty provisions incentivize U.S. sellers not to file in the instance where a mandatory declaration is not required, it presents a legitimate national security threat during the interim period where the foreign acquirer has ownership of the TID U.S. business and when CFIUS eventually requires they divest their ownership.

---

113. *See, e.g.*, *infra* Part IV.B. Note, there has been only one instance where parties to a CFIUS transaction have contested a CFIUS decision and Presidential Order in an Article III Court. *See* Ralls Corp. v. Comm. on Foreign Inv. in U.S., 758 F.3d 296, 325 (D.C. Cir. 2014) (holding that CFIUS and the President are required to provide parties with the unclassified evidence that informed their decision pursuant to the Due Process Clause of the Fifth Amendment).

114. 31 C.F.R. § 800.901(b).

115. *Id.*

116. Ralls Corp., a company owned by Chinese nationals and incorporated in Delaware with its principal place of business in Georgia, purchased four American-owned, limited liability companies: Pine City Windfarm, LLC; Mule Hollow Windfarm, LLC; High Plateau Windfarm, LLC; and Lower Ridge Windfarm, LLC. *Ralls Corp.*, 758 F.3d at 304. Included in the purchases were all the companies' assets "necessary for windfarm development." *Id.* Ralls Corp. did not file with CFIUS despite the transaction falling under CFIUS jurisdiction. CFIUS identified a national security risk after closing and ultimately the President of the United States ordered Ralls Corp. to divest its interest. *Id.* at 306. There was no punitive action against the four U.S. businesses that sold their assets and land to Ralls Corp. despite it being "located in and around the eastern region of a restricted airspace and bombing zone maintained by the United States Navy." *Id.* at 304.

A. Why U.S. Businesses Are Not Incentivized to File When They Sell All of Their Assets

CFIUS is tasked with the tall order of safeguarding national security using limited resources.[117] The creation of the voluntary filing scheme is a direct result of the impossibility that would come with requiring all cross-border M&A deals, investments, and real estate purchases to be filed with the U.S. government. The volume of activity is simply too high for CFIUS to process.[118] However, CFIUS compounds the difficulty of eliminating national security threats by not clearly articulating what a national security threat is.[119]

In December 2008, Treasury published "Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States" in a one-time instance because a statutory provision in the DPA required it.[120] In that guidance, Treasury described, in a general way, "Types of Transactions That CFIUS Has Reviewed and That Have Presented National Security Considerations."[121] The descriptions start broad and, unfortunately for U.S. businesses trying to glean clarity, stay that way.[122] For example the guidance states:

---

117. *See generally* U.S. GOV'T ACCOUNTABILITY OFF., GAO-24-107358, FOREIGN INVESTMENT IN THE U.S.: EFFORTS TO MITIGATE NATIONAL SECURITY RISKS CAN BE STRENGTHENED 1–2 (2024) ("[I]n 2018 . . . trends in the volume and complexity of foreign investment transactions filed with CFIUS, together with staffing constraints, may have limited CFIUS members' ability to monitor compliance with mitigation agreements. In its most recent public report, CFIUS acknowledged that the transactions it reviews are increasingly complex." (footnote omitted)).

118. *See* Borut et al., *supra* note 11, at 9 ("CFIUS requests filings for such a small fraction of non-notified transactions because doing so is resource intensive and can only be initiated if senior executive branch officials approve the request.").

119. There is no formal definition of a national security threat. Instead, CFIUS has national security "factors" that it considers when it reviews a transaction for approval. CIMINO-ISAACS & SUTTER, *supra* note 1, at 1; *see also* Defense Production Act, 50 U.S.C. § 4565(f)(1)–(10) (listing the statutory factors for national security risk assessment). In September of 2022, President Biden instructed CFIUS to expand their considerations to include supply chain resiliency threats, "within and outside of the defense industrial base," as well as food security threats, climate adaptation technologies, cybersecurity, aggregate investment trends by foreign persons, and more. Exec. Order No. 14,083, 87 Fed. Reg. 57,369, 57,370–72 (Sept. 20, 2022).

120. 73 Fed. Reg. 74,567, 74,568 (Dec. 8, 2008); 50 U.S.C. § 4565(b)(2)(E).

121. 73 Fed. Reg. at 74,570.

122. *Id.* ("CFIUS does not focus on any one U.S. business sector or group of sectors. Since its inception, CFIUS has received and reviewed voluntary notices regarding transactions across a broad spectrum of the U.S. economy. The following description of covered transactions that CFIUS has reviewed and that have presented national security considerations is illustrative only.").

> Some covered transactions that CFIUS has reviewed have presented national security considerations because they involve infrastructure that may constitute United States critical infrastructure, including major energy assets, which section 721 identifies as presenting national security considerations. As defined in section 721 and further explained in the regulations, CFIUS determines whether a transaction involves critical infrastructure on a case-by-basis, depending on the importance of the particular assets involved in the transaction.[123]

A U.S. business that *might* be involved with critical infrastructure, but does not deal in the energy sector, is provided no substantive guidance on whether they should file a voluntary notice.[124] They are only told their transaction will be assessed on the facts presented. Guidance in this instance is a misnomer. Rather, it is a rearticulation of the ambiguity strewn through the CFIUS statutory definitions—all of which are inherently ambiguous and open to executive interpretation.[125] Without any real guiding compass, it is no small wonder why U.S. businesses would rather not file and execute their deals than gamble on CFIUS finding an issue with their transaction. Moreover, the "non-notified team," a group within CFIUS dedicated to finding M&A deals that were not filed with CFIUS and potentially pose a national security threat, only opens inquiries into a very small fraction of deals that are identified.[126] Specifically, of the "thousands of transactions not filed with CFIUS (known as 'non-notified transactions'), . . . formal inquiries were only opened into 60 of them" in 2023.[127] Therefore, not only are U.S. businesses confused on whether their sale presents a national security threat, but also the chances that their deal is ever identified by CFIUS is unlikely because of resource constraints.[128] It is only logical that many U.S. businesses decide not to file at all.

The disincentive to file compounds when a U.S. business seeks to sell all its assets in their entirety to a foreign person and the transaction does not fall under mandatory filing rules. Again, this is because the current penalty regulations contain no provisions for situations where a U.S. business sells all

123. *Id.*

124. *See id.*

125. *See id.* at 74,569 ("Section 721 requires CFIUS to review covered transactions notified to it 'to determine the effects of the transaction[s] on the national security of the United States,' but does not define 'national security,' other than to note that the term includes issues relating to homeland security. Instead, section 721 provides an illustrative list of factors, . . . for CFIUS and the President to consider in assessing whether the transaction poses national security risks." (first alteration in original)); *see also* 31 C.F.R. § 800.214 (2025); 50 U.S.C. § 4552(2).

126. *See* Borut et al., *supra* note 11, at 9.

127. *Id.*

128. *See id.*

their assets *and* the transaction falls under the voluntary filing scheme.[129] The U.S. business that wants to sell all of its property interests faces a decision matrix where filing a voluntary notice means risking CFIUS finding a national security threat in the transaction and either (a) imposing an NSA that could reduce the profitability of the sale[130] or (b) referring the transaction to the President who has the power to block it.[131]

Not filing a voluntary notice means, at maximum risk, exposing the transaction to the possibility of it being discovered by the non-notified team and being asked to submit a voluntary notice.[132] If the transaction is not discovered prior to its conclusion, the U.S. business walks away with money in hand and no fear of penalization—even though there may very well be a legitimate national security threat present. Statistics on voluntary notices and their subsequent investigations released by the Committee in their annual report to Congress reveal that it is not uncommon for transactions that fall under the voluntary filing scheme to present a national security threat that merits a subsequent investigation.[133] Not filing a voluntary notice presents zero profit loss potential for the U.S. seller because, in this instance, they have sold their assets, have avoided the high costs that are inherent to the CFIUS filing and counsel process,[134] and have faced no threat of a financial penalty.

---

129. *See* 31 C.F.R. § 800.901 (2025).

130. *See CFIUS Mitigation*, *supra* note 15; *As CFIUS Announces Significant Penalties, Companies and Investors Confront a Shift in CFIUS Filing Cost-Benefit Dynamics*, COOLEY (Sept. 24, 2024), https://www.cooley.com/news/insight/2024/2024-09-24-as-cfius-announces-significant-penalties-companies-and-investors-confront-a-shift-in-cfius-filing-cost-benefit-dynamics [https://perma.cc/2RQ2-QRHP] ("[S]maller 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.").

131. *See* 50 U.S.C. § 4565(d)(1).

132. *See CFIUS Non-Notified Transactions*, DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-non-notified-transactions [https://perma.cc/V2QB-6JSH] (last visited Oct. 26, 2025).

133. *See* CFIUS, ANNUAL REPORT TO CONGRESS, *supra* note 15, at 14 (reporting that CFIUS conducted a subsequent investigation of 116 of the 209 notices filed in 2024).

134. While the actual filing fees for a voluntary notice are not jaw-dropping, the cost to hire the experienced counsel who predominately reside in white-shoe law firms can bring the transaction cost into the millions of dollars at current billing rates. *See* Farhad Jalinous, *United States*, WHITE & CASE (Oct. 30, 2020), https://www.whitecase.com/insight-our-

The incentive–disincentive matrix is shown below where:

U.S. business submits Voluntary Filing	**U.S. business does not submit Voluntary Filing**
Outcome 1 Unknown probability that CFIUS identifies a national security threat and imposes an NSA or recommends the transaction to the President.[135]	**Outcome 2** Unknown probability that the non-notified team identifies the transaction and requests a voluntary notice or initiates a unilateral review.[136]
Outcome 3 Unknown probability that CFIUS grants the transaction Safe Harbor status—which has sole benefit to the foreign buyer.[137]	**Outcome 4** 100% probability that the U.S. business can sell all its assets with no penalty.[138]

In this simplified decisionmaking matrix, the ambiguities behind what constitutes a national security threat, as well as the inability for U.S. businesses to reliably predict what CFIUS will do with a voluntary notice comes to the fore. The optimal choice that provides the most certainty to the U.S. business lies

thinking/united-states-0 [https://perma.cc/DTS2-6KG9] ("[Voluntary filing fees] are assessed based on a tiered approach, providing for a proportional cost equal to or less than 0.15 percent of the transaction value. The lowest fee is US$750 for transactions valued between US$500,000 and US$5 million (transactions under US$500,000 are not subject to fees), and the highest-tier fee is US$300,000 for transactions valued at US$750 million or more."); *see also* Staci Zaretsky, *The Biglaw Firms With the Highest Hourly Rates (2024)*, ABOVE THE LAW (Nov. 14, 2024, 1:07 PM), https://abovethelaw.com/2024/11/the-biglaw-firms-with-the-highest-hourly-rates-2024/ [https://perma.cc/3REN-SZXW] (reporting that partner hourly billing rate ranged from $800 to $2,620 an hour).

135. *See CFIUS Mitigation*, *supra* note 15; *see also, e.g.*, Ralls Corp. v. Comm. on Foreign Inv. in U.S., 758 F.3d 296, 325 (D.C. Cir. 2014) (example of a transaction being referred to the President and contested on due process grounds).

136. *See CFIUS Non-Notified Transactions*, *supra* note 132; *see also, e.g.*, *President Trump Orders Divestiture of StayNTouch, Inc. by Shiji Group of China*, COVINGTON (Mar. 9, 2020), https://www.cov.com/en/news-and-insights/insights/2020/03/president-trump-orders-divestiture-of-stayntouch-inc-by-shiji-group-of-china [https://perma.cc/B98T-5X3Z] (example of non-notified transaction being identified post-closing).

137. *See CFIUS Overview*, TREASURY, *supra* note 4.

138. *See Overview and Key Takeaways from CFIUS 2024 Annual Report*, COVINGTON (Aug. 18, 2025), https://www.cov.com/en/news-and-insights/insights/2025/08/overview-and-key-takeaways-from-cfius-2024-annual-report (discussing a reduction in voluntary filings by businesses seeking foreign investment, in an effort to avoid CFIUS mitigation and oversight).

in Outcome 4—take the money and run. CFIUS has created an asymmetric information environment[139] between regulator and regulated that incentivizes U.S. businesses not to participate in the voluntary filing regime.

B. Hypothetical Transaction

Corporation A, LogisticsWatch, is incorporated in Delaware, headquartered in Jakarta, and owned and controlled by an Indonesian shipping conglomerate. Corporation B, IntraCoastal Data, incorporated and headquartered in Delaware, is an open-source geolocation data company that collects geolocation and identifiable information on the commercial ships that traverse the Intracoastal Waterway which is maintained by the U.S. Army Corps of Engineers.[140] IntraCoastal Data does not collect geolocation information on more than one million individuals at any given time within a twelve-month period and does not specifically target products to any military department with intelligence, national security, or homeland security responsibilities. The geolocation data on the ships includes those commercial ships that depart from Norfolk, Virginia, which is also the location of Naval Station Norfolk, which "supports the operational readiness of the US Atlantic Fleet."[141] Corporation A, LogisticsWatch, wishes to purchase in whole the assets and title to Corporation B, IntraCoastal Data. The total acquisition is valued at $10 million.

Here, we have a corporation (LogisticsWatch) owned and controlled by an Indonesian shipping conglomerate—where Indonesia received close to $7.5 billion in Chinese investment in 2023 alone[142]—attempting to buy a U.S. business that collects geolocation data on the commercial ships that

---

139. *See generally* OFF. OF INV. SEC., U.S. DEP'T OF TREASURY, CFIUS CONFIDENTIALITY 1 (n.d.), https://home.treasury.gov/system/files/206/CFIUS-Confidentiality.pdf [https://perma.cc/4J4A-3WN4] (stating that CFIUS cannot reveal filings or other information collected during the filing process publicly).

140. *See Water Highway*, NAT'L GEOGRAPHIC, https://education.nationalgeographic.org/resource/water-highway/ [https://perma.cc/T6W4-R8YH] (last visited Aug. 29, 2025) ("Stretching from Norfolk, Virginia, to Miami, Florida, the Atlantic Intracoastal Waterway is an inland channel for recreational boaters and commercial shipping. The waterway is maintained by the U.S. Army Corps of Engineers (USACE). The mission of USACE is to 'provide vital public engineering services in peace and war to strengthen our nation's security, energize the economy, and reduce risks from disasters.'").

141. *Naval Station Norfolk*, U.S. DEP'T OF THE NAVY, https://cnrma.cnic.navy.mil/Installations/NAVSTA-Norfolk/ [https://perma.cc/PT85-SASZ] (last visited Aug. 29, 2025).

142. *See* Joan Aurelia, *Could China Provide the Renewable Energy Investment Indonesia Needs?*, DIALOGUE EARTH (Jan. 29, 2025), https://dialogue.earth/en/business/china-renewable-energy-investment-indonesia/ [https://perma.cc/X6Z4-85P3] ("In 2023, Chinese investment reached USD 7.4 billion, the highest in the ASEAN region.").

traverse our nation's intracoastal waterway system. The primary asset in this acquisition is the data itself. The primary danger, however, is that the data collection's scope might capture incidental activity occurring at Naval Station Norfolk or sensitive activity conducted by the U.S. Army Corps of Engineers.[143] While Indonesia is not a foreign adversary, the People's Republic of China is, and it is commonly known that China uses deceptive corporate structures and arrangements to get access to U.S. businesses.[144]

IntraCoastal Data uses open-source methods to collect the geolocation data of ships, including combing through satellite imagery (that they did not take themselves). It is up for debate whether or not IntraCoastal Data even constitutes a TID U.S. business because they are not collecting sensitive personal data on more than one million individuals at any given time and they are not developing critical technology.[145] Yet they are still within CFIUS jurisdiction that could merit a voluntary filing because it is a covered control transaction under the regulations because a foreign person (LogisticsWatch) is purchasing a U.S. business (IntraCoastal Data) in its entirety, such that it can exert full control over the U.S. business.[146]

IntraCoastal Data can choose not to file with CFIUS and receive the $10 million valuation of the transaction because this transaction does not trigger the mandatory filing requirement. CFIUS, through their non-notified team or through intelligence collection from the Director of National Intelligence (DNI),[147] might discover this transaction has occurred after-the-fact and impose mitigation measures on LogisticsWatch and make them sell their new acquisition at auction to a U.S. buyer. Meanwhile, IntraCoastal Data faces no financial repercussions for the national security threat that was present in the interim period and is financially rewarded for not filing.

---

143. *See generally Naval Station Norfolk*, *supra* note 141 (providing background on the strategic location of the Norfolk Naval Station and the commitment to safety).

144. *See* Memorandum on America First Investment Policy, *supra* note 56; *see also* Eli Clemens, *How Some Chinese Companies Obscure Ties to China and What Policymakers Should Do About It*, INFO. TECH. & INNOVATION FOUND. (Nov. 3, 2025), https://www2.itif.org/2025-china-ties.pdf [https://perma.cc/X8WL-G4L9].

145. *See* 31 C.F.R. §§ 800.241, 800.248 (2025).

146. *See id.* § 800.210.

147. *See CFIUS Non-Notified Transactions*, *supra* note 132; *see also* Defense Production Act, 50 U.S.C. § 4565(b)(4)(A)(i) ("[T]he Director of National Intelligence shall expeditiously carry out a thorough analysis of any threat to the national security of the United States posed by any covered transaction, which shall include the identification of any recognized gaps in the collection of intelligence relevant to the analysis.").

V. RECOMMENDATION TO CLARIFY AND CLAW BACK

The problem with the current CFIUS regulations is two-pronged. One, the U.S. business community is confused as to what types of transactions merit a voluntary filing and in what instances.[148] To remedy this confusion, CFIUS should issue annual guidance in the form of a non-binding policy statement that communicates to those they regulate what TID U.S. businesses they are concerned with and where they might encourage a voluntary filing. Two, the current penalty regulations fail to incentivize U.S. businesses to voluntarily file where the U.S. business is selling all its assets, and a national security threat could be present.[149] The regulations must be amended to close the "take the money and run" loophole by imposing a pain of a penalty and a profit clawback provision. Clear communication in the form of policy statements joined with palpable consequences in the form of penalties are the solutions to the United States' foreign investment risk.

A. Recommendation to Publish Annual Guidance (Policy Statement)

The Emerging Technology and Research Advisory Committee, housed in the Department of Commerce, informs CFIUS on the specific types of technology that the United States is interested in protecting from foreign ownership every 180 days.[150] The recommended next step is for CFIUS to publish an annual policy statement that includes these findings along with examples of transactions that would merit a voluntary filing.

The Administrative Procedure Act (APA) describes two types of guidance documents an agency can publish: interpretive rules or general statements of policy (policy statements).[151] Treasury should use the latter in publishing their descriptions of transactions that merit a voluntary filing. There are concrete benefits to using a policy statement as the vehicle for the recommendation. One, policy statements are "not binding on members of the public."[152] Consequently, the non-binding nature of the policy statement will not interfere with the voluntary nature of the filing scheme. Two, policy statements are "issued . . . to advise the public *prospectively* of the manner in

148. *See generally* Aimen Mir et al., *supra* note 98 (conducting an in-depth review of new CFIUS orders and explaining when CFIUS may flag transactions for voluntary filing).

149. *See supra* text accompanying notes 135–139.

150. *See* 50 U.S.C. § 4817(d).

151. 5 U.S.C. § 553(b)(A); *see also* KATE R. BOWERS, CONG. RSCH. SERV., LSB10591, AGENCY USE OF GUIDANCE DOCUMENTS 1 (2021).

152. Admin. Conf. of the U.S., Recommendation 2017–5, *Agency Guidance Through Policy Statements*, 82 Fed. Reg. 61,728, 61,736 (Dec. 29, 2017).

which the agency proposes to exercise a discretionary power."[153] In this respect, CFIUS is not binding itself to the black letter of the policy statement and therefore retains its autonomy during national security review to decide matters differently than they may have espoused in a policy statement. Three, policy statements are particularly helpful for regulatory environments with greater uncertainty because they can be disseminated quickly and thus are more easily accessible by the public.[154] Treasury's policy statements are posted on Regulations.gov where the public can review and comment on the posted guidance.[155]

The annual policy statement need not exceed confidential parameters to communicate effectively. U.S. sellers and foreign buyers need only a clearer picture that informs them of what transactions are of significant interest to CFIUS such that if they decided not to file, there would be near certainty that CFIUS would not intervene. The Office of Investment Security at Treasury, which is led by the Assistant Secretary for Investment Security, and chairs CFIUS, is best poised to write and publish policy statements to Regulations.gov as well as to the Treasury main website.[156]

Using the hypothetical LogisticsWatch purchase of IntraCoastal Data as an example,[157] a proposed transaction that might be described in a policy statement could look like:

Corporation A, a foreign person, seeks to acquire a 100% interest in Corporation B, a U.S. business. Corporation A's affiliated country is not a foreign adversary; however, a foreign adversary invests heavily across their manufacturing and environmental technology sectors. The U.S. business does not deal in critical technology; however, their data collection methods incidentally capture activities conducted at U.S. military installations. The transaction constitutes a covered control transaction but is not subject to a 31 C.F.R. § 800.401 mandatory filing. Parties to such a transaction should consider a voluntary filing because the transaction could be implicated by national security factor (f)(3) of the DPA where incidental surveillance of military installations may "affect[] the capability . . . of the United States to meet

153. *Id.* at 61,734 (alteration in original) (emphasis added) (quoting ATT'Y GEN.'S MANUAL ON THE ADMIN. PROC. ACT 30 n.3 (1947)).

154. *Id.*

155. *Guidance Documents*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/guidance [https://perma.cc/95YE-DH4A] (last visited Oct. 25, 2025).

156. *See generally CFIUS Laws and Guidance*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-laws-and-guidance [https://perma.cc/6Y3T-9CMC] (last visited Oct. 26, 2025) (describing CFIUS guidance and the purpose of the CFIUS guidance published by Treasury).

157. *See supra* Part IV.B.

the requirements of national security," where such capability could be viewed as supporting sensitive military operations with discretion.[158]

The annual policy statement will make CFIUS more accessible to the American business community and provide a mutual benefit to CFIUS and U.S. businesses. CFIUS will develop a stronger understanding of the trends occurring in foreign investment and U.S. businesses will develop a better understanding of the national security perspective of the Committee. This is especially important where a U.S. business might deal in emerging technology. The annual policy statement would include the non-confidential type of emerging technology identified in the four quarterly reports made by the Emerging Technology and Research Advisory Committee.[159] This list can be compiled and shared in the annual policy statement along with the hypothetical transactions that fall under the voluntary filing regime but still raise national security concerns.[160]

Readers familiar with the CFIUS process might question the merits of what essentially is a "voluntold" system of filing in the instance where a transaction matches an example listed in a published policy statement. At present, CFIUS is overwhelmed with the amount of filings received, and those filings represent only a fraction of the cross-border transactions occurring on an annual basis that are within CFIUS's covered jurisdiction.[161] However, if Treasury paints a clearer picture of national security, both U.S. businesses and the Committee itself would have a stronger understanding of what they are looking for during the national security review process. Having a concrete idea of what constitutes a national security threat in different sectors of the American economy could speed up review and allow legitimately non-threatening transactions to be approved swiftly, while still allowing the Committee to ruminate on problematic transactions for the set forty-five-day statutory period of review.[162] CFIUS has proven that it is capable of sifting through hundreds of

158. 50 U.S.C. § 4565(f)(3); *see also* THEODORE H. MORAN, THREE THREATS: AN ANALYTICAL FRAMEWORK FOR THE CFIUS PROCESS 1 (Peterson Inst. for Int'l Econ. 2009) ("The 'Threat III' designation is for any proposed acquisition that could allow insertion of the means for . . . surveillance, . . . whether by a human or nonhuman agent, in goods or services crucial to the functioning of the US economy.").

159. *See* 50 U.S.C. § 4817(d).

160. *See* 31 C.F.R. § 800.501(a)–(b) (2025).

161. *See* Borut et al., *supra* note 11, at 9.

162. *See* 31 C.F.R. § 800.503 (2025); *see also* Tarbert, *supra* note 28, at 1523 ("If administered properly, the voluntary declarations process should thus encourage greater foreign investment in the United States.").

filings with respectable turnaround time for each transaction such that legitimate national security threats can be identified and addressed.[163]

President Trump recently issued a memorandum to his cabinet Secretaries calling for a change in the national security calculation of foreign investment that could make filing clearer for transactions involving allied countries and more complicated for transactions connected to foreign adversaries.[164] Simply put, President Trump has called for the creation of "an expedited 'fast-track' process, based on objective standards, to facilitate greater investment from specified allied and partner sources in United States businesses involved with United States advanced technology and other important areas," i.e., transactions that would require mandatory declarations.[165] This notion seems to be an expansion of the "excepted investor" category within CFIUS regulations.[166] However, it still does not provide the clarity needed for those U.S. businesses who receive offers from foreign countries that are not allies or partners but have deep economic ties with China (as is the case for most of the world's countries).[167] Articulating "objective" standards beyond the statutory national security considerations however, will be a substantive step forward, in conjunction with published annual policy statements, to bring transparency to what is an opaque national security deliberation process.[168]

---

163. *See* CFIUS, ANNUAL REPORT TO CONGRESS, *supra* note 15, at 16 (reporting that it took an average of 46.5 days to complete a review of a transaction and 87.5 days to complete an investigation of a transaction that were submitted via voluntary notice).

164. *See* Memorandum on America First Investment Policy, *supra* note 56.

165. *Id.*; 31 C.F.R. § 800.401 (2025).

166. 31 C.F.R. § 800.219 (2025) (defining an excepted investor in part as 1) a foreign national who is a national of one or more excepted foreign states and is not also a national of any foreign state that is not an excepted foreign state; 2) a foreign government of one of the excepted foreign states; or 3) an entity that a) is organized under the laws of the United States, b) has its principal place of business in the United States or aforementioned countries, c) has a board membership composed of at least 75% U.S. citizens or nationals of one of the aforementioned countries, and d) has major shareholders and ownership from U.S. citizens or nationals of one of the aforementioned countries); For the list of excepted foreign states *see CFIUS Excepted Foreign States*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-excepted-foreign-states [https://perma.cc/N5C2-RA7X] (last visited Nov. 14, 2025) (listing excepted foreign states as Australia, Canada, New Zealand, and United Kingdom of Great Britain and Northern Ireland).

167. *See* Mark A. Green, *China Is the Top Trading Partner to More Than 120 Countries*, WILSON CTR. (Jan. 17, 2023), https://www.wilsoncenter.org/blog-post/china-top-trading-partner-more-120-countries [https://perma.cc/8236-5L4R].

168. *See* Memorandum on America First Investment Policy, *supra* note 56.

B. Amending the Penalty Provisions

The other issue with the current voluntary filing system is that it allows U.S. businesses to escape the consequences of selling a TID U.S. business to foreign persons where those sales are found to present a national security threat post-closing.[169] To eliminate the incentive for U.S. companies not to file, Treasury should issue a Notice of Proposed Rulemaking (NPRM) that amends 31 C.F.R. § 800.901 "penalties and damages."[170] The amended § 800.901 should include, in its list of violations, a clawback provision stating: any and all owners of a TID U.S. business that do not file a voluntary notice prior to the sale of their business to a foreign person shall be subject to a post-closing fine "not to exceed $5,000,000 or the value of the transaction" if CFIUS finds that the transaction would have been deemed a national security risk during review.[171]

To amend the penalty provisions, Treasury, as chair of CFIUS, will have to "publish [an NPRM] in the *Federal Register* and provide interested persons an opportunity to submit written comments on [the] rulemaking proposal" pursuant to § 553 of the APA.[172] The U.S. business community members, who have been taking advantage of the gap in the penalty provisions, will likely comment in droves about the apparent drawbacks to a clawback scheme. The anticipated counterargument might be that a clawback provision discourages U.S. businesses from engaging in cross-border M&A deals entirely and thus will hurt the United States' overall objective to be a prime destination for FDI.[173] On the contrary, an amended penalty provision that gives U.S. businesses pause prior to engaging with possibly nefarious foreign actors in transactions that present national security threats is exactly in line with the national security vision for cross-border investment.[174] By imposing the prospect of severe financial penalties or even the value of the deal, U.S. businesses will not be incentivized to enter into transactions that could risk national security.[175]

---

169. *See generally supra* Part IV.

170. 31 C.F.R. § 800.901 (2025).

171. *Id.* § 800.901(b).

172. Admin. Conf. of the U.S., Recommendation 2024-6, *Public Engagement in Agency Rulemaking Under the Good Cause Exemption*, 89 Fed. Reg. 106,406, 106,408 (Dec. 30, 2024); *see also* Administrative Procedure Act, 5 U.S.C. § 553(b)–(c).

173. *See* Memorandum on America First Investment Policy, *supra* note 56 ("Welcoming foreign investment and strengthening the United States' world-leading private and public capital markets will be a key part of America's Golden Age.").

174. *See id.* ("Certain foreign adversaries . . . pursue[] these strategies [to obtain technology, IP, and leverage] in diverse ways, both visible and concealed, and often through partner companies or investment funds in third countries.").

175. *See infra* text accompanying notes 176–178.

A revised incentive-disincentive matrix is shown below where:

U.S. Business submits Voluntary Filing	**U.S. Business does not submit Voluntary Filing**
Outcome 1 Unknown probability that CFIUS identifies a national security threat and imposes an NSA or recommends the transaction to the President.[176]	**Outcome 2** Unknown probability that the non-notified team identifies the transaction and requests a voluntary notice or initiates a unilateral review.[177]
Outcome 3 Unknown probability that CFIUS grants Safe Harbor status—a benefit to both parties.[178]	**Outcome 4** Unknown probability that the U.S. business will be subject to a clawback provision.

Treasury will be required to review the public comments and incorporate those relevant into the final rule with concise reasoning explaining why they have chosen to reject "significant" public comments, as well as provide a general statement of the final rule's basis and purpose.[179] Treasury will post the final rule to the Federal Register where it will live for thirty days until it becomes a substantive rule in the Code of Federal Regulations.[180] The general statement of basis and purpose could read: the final rule amending 31 C.F.R. § 800.901 penalties and damages applies a penalty clawback provision to any and all owners of a TID U.S. business that do not file a voluntary notice, prior to the sale of their business to a foreign person, if CFIUS finds that the transaction would have been deemed a national security risk during review. The clawback provision closes a loophole for U.S. businesses that make a profit from transactions that do not require a mandatory filing yet still present a national security risk. The U.S. business who is found to have triggered the clawback provision will be subject to a post-closing fine not to exceed $5,000,000 or the value of the transaction. This penalty amount reflects the current penalty standard in the CFIUS regulations and will operate as a sufficient deterrent.[181]

176. *See CFIUS Mitigation*, *supra* note 15.

177. *See CFIUS Non-Notified Transactions*, *supra* note 132, at 33.

178. *See CFIUS Overview*, TREASURY, *supra* note 4.

179. *See* Administrative Procedure Act, 5 U.S.C. § 553(b)–(c); *see also* Perez v. Mortg. Bankers Ass'n, 575 U.S. 92, 96 (2015) ("An agency must consider and respond to significant comments received during the period for public comment.").

180. *See* 5 U.S.C. § 553(b)–(c).

181. 31 C.F.R. § 800.901 (2025).

CONCLUSION

The foremost obstacle facing U.S. businesses and CFIUS is a lack of clarity on what constitutes a national security threat and what critical technologies, infrastructure, and sensitive data they are most concerned with and why. While the regulations themselves (in some instances) detail the types of technology, infrastructure, and sensitive personal data that constitute a covered transaction where CFIUS has jurisdiction, the regulations do not clearly communicate why or where CFIUS will intercede in a deal. However, expecting the Executive Branch to constrain itself by more narrowly defining national security is unlikely. What CFIUS can do is issue a regular, annual policy statement containing nonexclusive types of transactions and emerging technologies that might merit a U.S. business to voluntarily file a notice. CFIUS is already well poised to provide these examples because it is a function they currently perform within their regulations.[182] Moreover, amending the penalty provisions to include a clawback provision will close the regulatory gap that has incentivized U.S. businesses to prioritize profit over our nation's national security interests. These changes can transform a process that has been critiqued and derided for being a "black box" into one that can be reasonably applauded for increased transparency and one that succeeds in its mission of safeguarding national security.[183]

182. *See* 31 C.F.R. § 800.241(c)(1) (2025).

183. *See generally Shining Some Light on CFIUS's Black Box: Biden Administration Releases an Updated List of High-Priority Critical and Emerging Technologies*, WINSTON & STRAWN LLP (Feb. 17, 2022), https://www.winston.com/en/blogs-and-podcasts/global-trade-and-foreign-policy-insights/shining-some-light-on-cfiuss-black-box-biden-administration-releases-an-updated-list-of-high-priority-critical-and-emerging-technologies [https://perma.cc/7HYL-BCCC] ("[T]he [National Science and Technology Council] Report gives dealmakers some insight into the types of critical and emerging technologies that CFIUS is focused on safeguarding from licit and illicit technology transfer mechanisms. . . . [T]he NSTC Report expressly states that agencies may use the Updated [Critical and Emerging Technology] List as a tool to 'protect sensitive technology from misappropriation and misuse,' which suggests that CFIUS member agencies may use the Updated CET List [as] a resource when evaluating CFIUS filings.").