COMMENTS

THE PROBLEM WITH FOREIGN INVESTMENT: USING CFIUS & FIRRM A TO PREVENT UNAUTHORIZED FOREIGN ACCESS TO INTELLECTUAL PROPERTY

SONIYA SHAH*

INTRODUCTION ............................................................................................................. 1
I. A HISTORY OF CFIUS, FIRRM A, AND THE INTERSECTION WITH INTELLECTUAL PROPERTY ................................................................. 4
   A. Understanding the Role of Intellectual Property Rights ......................... 4
   B. Origins and History: The Impact of FIRRM A on CFIUS ...................... 7
II. ANALYZING THE IMPACT OF FIRRM A ON INTELLECTUAL PROPERTY .......................................................................................... 15
   A. Facing FIRRM A: Expanding CFIUS’s Authority .............................. 15
   B. CFIUS and FIRRM A: The Impact on Protecting Intellectual Property .. 19
III. RECOMMENDATIONS ......................................................................................... 24
CONCLUSION .............................................................................................................. 28

INTRODUCTION

Intellectual Property Rights (IPRs)—such as patents, copyrights, and trademarks—are intended to protect holders’ rights to use, commercialize, and market their creations, or prevent others from doing the same. There is often an unauthorized flow of intellectual property (IP) when foreign entities

* J.D. Candidate, American University Washington College of Law (2021); B.S., Technical Writing, Carnegie Mellon University (2015). Special thanks to my family and friends for their support and encouragement throughout my academic endeavors, especially my parents for their unwavering enthusiasm and guidance. I would also like to thank the Administrative Law Review staff for their editorial support and assistance in preparing this piece.
are involved because foreign economies benefit when technology transfers from U.S. businesses to foreign entities. Foreign direct investment (FDI) heightens this risk for U.S. businesses. Along with establishing a foreign presence in the United States, such foreign entities can also bypass U.S. regulatory procedures. Foreign ownership allows for theft of American technology and IP, which are further impacted by international technology transfer, where transfer occurs from one country to another. The annual cost of IP theft exceeds $225 billion in counterfeit goods, and theft of pirated software and trade secrets could be as high as $600 billion. The Committee on Foreign Investment in the United States (CFIUS), an interagency committee, addresses fears that technologies and funds from an acquired U.S. business could transfer to a sanctioned country as a result of a foreign acquisition. Today, CFIUS reviews more than just transactions with

1. See Elias G. Carayannis & Jeffrey Alexander, Technology Transfer, Reference for Business, https://www.referenceforbusiness.com/management/Str-Ti/Technology-Transfer.html (last visited Aug. 13, 2020) (explaining that technology transfer is when technology is transferred to a group that does not possess specialized technical skills and therefore cannot create the technology themselves).


3. See James Chen, Foreign Direct Investment (FDI), Investopedia, https://www.investopedia.com/terms/f/fdi.asp (last updated Feb. 24, 2020) (defining foreign direct investment (FDI) as “an investment made by a firm or individual in one country into business interests located in another country”).


5. See Carayannis & Alexander, supra note 1 (defining technology transfer).


7. See Committee Composition, U.S. Dept’ of the Treasury, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius-cfius-overview (last visited Aug. 13, 2020) (explaining that the Committee on Foreign Investment in the United States (CFIUS) is chaired by the secretary of the Treasury, with eight members from other departments).

sanctioned countries. In 2018, Congress updated CFIUS’s power and jurisdiction through the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA).

Prior to FIRRMA, CFIUS reviewed controlling investments in U.S. businesses by foreign persons because the investments were considered covered transactions. Under FIRRMA, CFIUS reviews noncontrolling investments by foreign persons in U.S. businesses if the investment is a covered investment in technology, infrastructure, or data—known as TID businesses—and covers investments in U.S. businesses involving critical technologies, critical infrastructure, or sensitive personal data.

There is a gap in the legal framework that could allow for an outflow of IP, enabling foreign entities to gain access to U.S. IP. However, the new CFIUS jurisdiction works to close this gap. Now, U.S. companies considering deals with foreign entities must comply with CFIUS’s jurisdiction and undergo a review. Because FIRRMA relies heavily on voluntary notices and declarations, the regulations still allow foreign entities to access U.S. IP without authorization. Once foreign entities invest in a U.S. company, they often have access to that company’s IP. FIRMA legislation is a necessary step to prevent leakage of U.S. IP to foreign entities.

Part I of this Comment explores CFIUS’s background and the reasons for legislating FIRRMA. It also discusses the history of IPRs in the United States and the evolution of IPR protection from unauthorized access by foreign

9. Id.
13. See CFIUS & FIRRMA, supra note 8 (discussing how CFIUS’s expanded jurisdiction means that companies must now jump through more hoops).
15. See CFIUS & FIRRMA, supra note 8 (discussing how CFIUS scrutinizes investments in foundational technology and underlying intellectual property (IP) as a safeguard).
entities. Part II analyzes CFIUS’s impact, and how FIRRMA changes and expands the scope of CFIUS’s jurisdiction, while exploring potential gaps that FIRRMA fails to address. Finally, Part III recommends potential ways Congress could amend FIRRMA to close the gap on unauthorized foreign access to IP through interim rules and the administrative process.

I. A HISTORY OF CFIUS, FIRRMA, AND THE INTERSECTION WITH INTELLECTUAL PROPERTY

A. Understanding the Role of Intellectual Property Rights

IPRs are essential to encouraging innovation and developing new products in the United States. There are several types of IPRs, including patents,\(^{16}\) copyrights,\(^{17}\) trademarks,\(^{18}\) and trade secrets.\(^{19}\) International law intersects with protecting these IPRs.\(^{20}\) Preventing IP theft depends on IPRs’ relationship to trade as well as the overlapping relationship with CFIUS and FIRRMA.

While the United States signed several conventions related to IP protection, including international conventions, such agreements fail to fully protect U.S. IPRs because strategic diplomacy with other nations remains the

---


17. 17 U.S.C. § 102(a) (defining protection under the Copyright Act for “original works for authorship fixed in any tangible medium of expression”).

18. 15 U.S.C. § 1127 (defining a trademark as “any word, name, symbol, or device, or any combination thereof—(1) used by a person, or (2) which a person has a bona fide intention to use in commerce and applies to register on the principal register established by this chapter, to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods, even if that source is unknown.”).


best way to both avoid IP theft and encourage IPR enforcement. Current international agreements lack protection and underscore the importance of including IP in the CFIUS framework. CFIUS assesses national security risks; adding an additional component to assess how a foreign company obtains IP from an acquisition could close the gap on foreign access to IP.

The Congressionally mandated Special 301 Report emphasized that providing adequate protection and enforcement of IPRs is a top trade priority for the United States. The Office of the U.S. Trade Representative produces the Special 301 Report using written submissions from the public, intensive deliberations with government agencies, and a case-by-case country assessment. Trade laws play an important role in enforcing certain IPRs. Enforcement actions occur under Section 301 of the Trade Act of 1974, which gives the United States the authority to enforce trade agreements, resolve trade disputes, and open foreign markets to U.S. goods and services. United States involvement in trade agreements prevents harmful technology transfers and foreign entities from creating barriers to market access by requiring IP as the price of market entry. Section 301 also authorizes the President to impose sanctions against foreign countries that fail to meet their IPR obligations. Section 337 of the Tariff Act of 1930 addresses imported products that violate IPRs, and if infringement is found, the International Trade Commission can issue orders excluding products from gaining entry into the United States. While useful for accused

21. See id. (explaining that two major IPR agreements are the Paris Convention, which deals with patents and trademarks, and the Berne Convention, which addresses copyright issues).

22. See infra Part III (outlining recommendations to protect IP under CFIUS).


24. See id. at 8–9 (explaining how the U.S. Trade Representative compiles its report).

25. See id. (outlining ways in which international trade laws intersect with IP rights).


27. See OFF. OF THE U.S. TRADE REPRESENTATIVE, supra note 23, at 6, 22–24 (explaining harm occurs when foreign companies gain access to U.S. companies through technology transfers).


imports, Section 337 fails to address outbound products to foreign entities that impact IPRs.

Developing IP is a time-intensive, expensive venture, and inadequate protection of IPRs can result in loss of an investment. U.S. IP theft directly affects national security in a few ways. First, the theft presents major economic harm because IP greatly benefits the U.S. economy. Many unauthorized acquisitions of U.S. IP result from cybertheft. For example, other countries use cyberattacks to “acquire intellectual property and proprietary information illicitly to advance their own economic and national security objectives.” The economic impact of IP theft in the U.S. is far reaching and well documented. The National Security Strategy highlights IP protection as a priority action, stating that “competitors such as China steal United States intellectual property valued at hundreds of billions of dollars[,]” and “[s]tealing proprietary technology and early-stage ideas allows competitors to unfairly tap into the innovation of free societies.” Enforcing IPRs is difficult because law enforcement lacks the capacity to patrol every facet of IPRs. Moreover, foreign entity involvement decreases the chances of such entities ever being tried in an American court. Second, IP theft often targets military technologies. For example, the Chinese military seized blueprints of the F-35 joint strike fighter from a U.S. contractor, demonstrating the serious implications of IP theft, especially in the military sector.


34. See NAT’L BUREAU OF ASIAN RSCH., supra note 6, at 8.

35. See id. (explaining that IP protection is important to every business but that measuring economic impact is difficult because of the illicit nature of piracy).

36. See U.S. NATIONAL SECURITY STRATEGY, supra note 33.

While IP theft remains a major concern, defense against theft resulted in several positive developments, including a decrease in cyberattacks, more awareness around IP theft, and the recent implementation of the Defend Trade Secrets Act of 2016. The 2015 National Defense Authorization Act introduced Section 1637, which addressed economic or industrial espionage in cyberspace, including concerns about foreign countries enforcing laws that bolstered their domestic companies at the expense of U.S. companies, as well as access to IP and proprietary information. While these developments are encouraging, theft still occurs at costs as high as $600 billion annually.

B. Origins and History: The Impact of FIRRMA on CFIUS

The United States is the largest recipient of FDI driving the start-up economy, which often relies on early stage investment from foreign investors. CFIUS review is often required when foreign entities are involved in the aforementioned investment process. In 1975, Congress created CFIUS pursuant to the Exon-Florio Amendments to block foreign takeovers of American businesses based on national security threats. CFIUS is headed by the Secretary of the Treasury and includes the Secretaries of State, Defense, Homeland Security, Commerce, Energy; the Attorney General; the U.S. Trade

38. See Nat’l Bureau of Asian Rsch., supra note 6, at 3 (noting the developments that have occurred over the past decade).


40. See Nat’l Bureau of Asian Rsch., supra note 6, at 1 (acknowledging the costs of IP theft due to counterfeit goods, pirating software, trade secret theft, and patent infringement).


Representative; and the Director of the Office of Science and Technology policy.\textsuperscript{44} CFIUS’s mission is to “determine the effects on national security of mergers, acquisitions, and takeovers . . . by or with foreign persons which could result in foreign control of persons engaged in interstate commerce in the United States.”\textsuperscript{45} Companies involved in potential mergers or acquisitions with foreign entities must notify CFIUS.\textsuperscript{46} CFIUS reviews the anticipated transactions and decides whether they pose a national security threat.\textsuperscript{47}

After CFIUS receives notice, either through a voluntary or mandatory declaration, an investigation must commence within thirty days.\textsuperscript{48} If all CFIUS members unanimously decide not to undertake an investigation, the matter is closed with no further action.\textsuperscript{49} However, should CFIUS decide an investigation is warranted, the committee has forty-five days under FIRRMA to complete its work—a fifteen-day extension from the prior thirty-day limit.\textsuperscript{50} CFIUS considers three conditions in its national security investigation:

\begin{enumerate}
\item The transaction threatens to impair U.S. national security and the threat was not mitigated during or prior to a review of the transaction;
\item the foreign person is controlled by a foreign government; or
\item the transaction would result in control of any critical infrastructure by a foreign person, the transaction could impair the national security, and such impairment has not been mitigated.
\end{enumerate}

\begin{itemize}
\item \textsuperscript{44} Committee Composition, supra note 7; see also Chelsea Naso, 5 Ways CFIUS Will Change With New Law, Law360 (Aug. 7, 2018, 4:34 PM), https://www.law360.com/corporate/articles/1070864/5-ways-cfius-will-change-with-new-law?hl_pk=72e67b2b-a356-4164-9e1a22d84373149&utm_source=newsletter&utm_medium=email&utm_campaign=corporate (noting that CFIUS is an interagency committee).
\item \textsuperscript{46} See Jackson, supra note 42, at 22 (explaining the notification procedures pursuant to the Exon-Florio amendments).
\item \textsuperscript{47} Amy S. Josselyn, Comment, National Security at all Costs: Why the CFIUS Review Process May Have Overreached Its Purpose, 21 GEO. MASON. L. REV. 1347, 1348 (2014).
\item \textsuperscript{49} FIRRMA § 1709(2)(C); see also Jackson, supra note 42, at 22 (stating that, during the review, CFIUS members must consider twelve factors mandated by Congress and six new FIRRMA factors).
\item \textsuperscript{50} 50 U.S.C. app. § 2170(a); see also Jackson, supra note 42, at 13 (explaining that during the review period the Director of National Intelligence (DNI) carries out a thorough analysis and that the DNI must incorporate the views of “all affected or appropriate” agencies).
\item \textsuperscript{51} See Jackson, supra note 42, at 23 (noting the relevant conditions).
\end{itemize}
If at least one of these three conditions exists, the President must conduct a national security investigation. During the review or investigation process, CFIUS has the authority to “negotiate, impose, or enforce any agreement or condition with the parties” to mitigate national security concerns.

Because CFIUS is only an investigative body, it reports its findings to the U.S. President along with a recommendation. The President must then make specific findings that there is evidence to believe the foreign interest might take action that could threaten national security, but has nearly unlimited authority in making a decision. For example, through the CFIUS process, President Trump used a Presidential Order to block the Singaporean company Broadcom from taking over the American company Qualcomm. To initiate the process, the President must make an announcement within fifteen days after CFIUS completes its investigation, and immediately report the action and mandatory factual findings to Congress. President Trump’s prohibition shows CFIUS is a powerful tool that the government can use against foreign entities attempting to acquire U.S. businesses with national security implications.

On August 13, 2018, President Trump signed FIRRMA into law. To better address concerns about national security ramifications in foreign investment, FIRRMA expanded CFIUS’s jurisdiction to also review noncontrolling investments in U.S. companies in three areas: critical

52. See id. (clarifying that if a condition exists, the President must conduct a National Security Investigation and take any necessary action within forty-five days).
53. See id. at 23–24 (concluding that CFIUS determines what recommendation to offer to the President).
55. 50 U.S.C. app. § 2170(c); see also Jackson, supra note 42, at 23–24 (confirming that the President’s actions are not subject to judicial review).
56. Presidential Order Regarding the Proposed Takeover of Qualcomm Incorporated by Broadcom Limited, 83 Fed. Reg. 11,631 (Mar. 12, 2018) [hereinafter Presidential Order] (demonstrating that a President can completely prohibit a transaction through the CFIUS review process if there are national security concerns).
57. 50 U.S.C. app. § 2170(g), (k).
technologies, critical infrastructure, and sensitive personal data. While the changes expand CFIUS’s jurisdiction, FIRRMA fails to explicitly define “non-controlling investments.” Prior to FIRRMA, “a ‘covered transaction’ subject to CFIUS review was limited to mergers, acquisitions, or takeovers by a foreign person,” and the definition of “control” was limited to majority control. Currently, under FIRRMA, CFIUS reviews “foreign investments that do not result in foreign control” as long as the transaction involves one of the three categories mentioned above.

While CFIUS remains the lead interagency committee handling issues with FDI and national security, FIRRMA expands its authority and jurisdiction. Throughout the FIRRMA implementation process, the Department of the Treasury issued regulations on behalf of CFIUS in three phases released in October 2018, September 2019, and January 2020. The

60. See FIRRMA § 1703(a)(6)(A) (defining the term “critical technologies” to include “[d]efense articles or services on the United States Munitions List”; “[i]tems on the Commerce Control List”; “[s]pecially designed and prepared nuclear equipment . . . software, and technology”; nuclear facilities and equipment; “select agents and toxins”; and “[e]merging and foundational technologies controlled [by] the Export Control Reform Act of 2018”).

61. See id. § 1703(a)(5) (defining the term “critical infrastructure” as “subject to regulations prescribed by the Committee, 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”).

62. See id. § 1703(a)(4)(B), (D); see also Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 85 Fed. Reg. 3112, 3132–33 (Jan. 17, 2020) (to be codified at 31 C.F.R. pt. 800–01) (defining sensitive personal data generally as identifiable data that could include personally identifiable information).

63. See generally FIRRMA § 1703 (failing to define noncontrolling investments); see also OFF. OF PUB. AFFS., DEP’T OF THE TREASURY, supra note 59, at 2 (clarifying that “[n]oncontrolling investments that afford a foreign person certain access, rights, or involvement in certain U.S. businesses” are now covered investments under FIRRMA).


65. Id.


Department of the Treasury then issued the second set of proposed regulations “as the first step in a notice-and-comment rulemaking process.”\(^6\) On January 13, 2020, the Department of the Treasury issued its final regulations regarding CFIUS, which are effective as of February 13, 2020, as required by FIRRMA.\(^6\) These final regulations amend part 800 of the Code of Federal Regulations to implement changes that FIRRMA made to CFIUS’s jurisdiction and process.\(^7\) Specifically, “the regulations broaden the scope of transactions subject to CFIUS’s review,” including key developments such as changes to the mandatory declaration requirement, updated definitions, rules for excepted foreign states, and alternatives to the traditional voluntary notice.\(^8\) This Comment incorporates the final regulations from January 13, 2020.

FIRRMA allows CFIUS to review transactions that do not result in the foreign control of a U.S. business.\(^9\) FIRRMA mandates that companies submit a declaration to CFIUS whenever transactions in an acquisition of U.S. businesses relate to critical technology.\(^10\) The definition of “critical technology” includes “emerging and foundational technologies controlled pursuant to . . . the Export Control Reform Act of 2018.”\(^11\) The Export Control Reform Act (ECRA) has two major components: it applies controls for a deemed export\(^12\) “to transfers of controlled technology to United States companies, unless they are majority-owned by a United States entity,” and answered (noting that “on October 10, 2018, the Department of the Treasury issued regulations on behalf of CFIUS as the first part of a phased implementation of FIRRMA.”).

The Department of the Treasury issued a second set of regulations, on September 17, 2019, to implement additional provisions of FIRRMA.\(^3\) Id.

68. Id.; see also OFF. OF PUB. AFFS., DEPT. OF THE TREASURY, supra note 59, at 1 (explaining that the proposed September 2019 rule would “comprehensively implement FIRRMA” and that the Treasury, on behalf of CFIUS, was providing an opportunity for public comment for a thirty-day period. Comments would “inform the . . . final regulations to implement FIRRMA.”).


72. See OFF. OF PUB. AFFS., DEPT. OF THE TREASURY, supra note 59, at 2; see also Levine & Paretzky, supra note 11, at 1–2 (clarifying the expanded CFIUS jurisdiction under FIRRMA).


74. Id. § 1703(a)(6)(A)(vi).

75. 15 C.F.R. § 734.13(a)(2) (2019) (defining deemed exports as “[r]eleasing or otherwise transferring technology or source code to a foreign person in the United States”).
it establishes control over the release of technology that includes information essential to protecting emerging technology.\textsuperscript{76}

FIRRMA emphasizes the complementary nature between CFIUS and export controls by including ECRA in the definition of critical technologies. Taken together, FIRRMA and ECRA preserve export controls as the means of restricting international transfers of U.S. technology.\textsuperscript{77} While prior versions of FIRRMA included screening inbound and outbound investments, Congress ultimately limited screening to inbound investments and restricted outbound technology transfer review to ECRA.\textsuperscript{78}

The CFIUS Critical Technology Pilot Program also evidences the complimentary nature between export controls and CFIUS. FIRRMA authorizes CFIUS to conduct pilot programs on certain legislative provisions.\textsuperscript{79} Accordingly, CFIUS implemented a new pilot program in November 2018 that required parties to make mandatory declarations to CFIUS prior to closing certain transactions, related to twenty-seven specified industries, with foreign entities involving critical technology.\textsuperscript{80} Prior to FIRRMA, the CFIUS national security review jurisdiction was limited to transactions that could result in foreign control of a U.S. business.\textsuperscript{81} The CFIUS pilot program expanded the scope of covered transactions to include noncontrolling investments in U.S. businesses that produce, design, test, manufacture, fabricate, or develop one or more “critical technologies” in

\textsuperscript{76} See David N. Fagan et al., Export Control Reform Act Introduced in Congress, NAT’L L. REV. (Mar. 8, 2018), https://www.natlawreview.com/article/export-control-reform-act-introduced-congress (explaining that the FIRRMA definition of critical technology is cross-referenced in the Export Control Reform Act of 2018 (ECRA)).

\textsuperscript{77} See id. (noting that ECRA also aims to protect critical technology).


\textsuperscript{80} See OFF. OF PUB. AFF’NS, DEP’T OF THE TREASURY, supra note 59, at 1–2 (emphasizing the main change was in mandatory declarations).

\textsuperscript{81} See id. at 2 (expanding CFIUS authority to cover more foreign investments).
twenty-seven specified industries. Implementing the program was an important first step in CFIUS requiring greater due diligence and compliance with potential reviews. The final regulations, released on January 13, 2020, announced that the pilot program on critical technologies expired on February 12, 2020.

Notably, there are changes under the final regulations that impact the pilot program, among other issues. For the pilot program, the final regulations require mandatory declarations “for covered transactions involving certain U.S. businesses that produce, design, test, manufacture, fabricate, or develop one or more critical technologies.” Under the final regulations, most covered investments are triggered by voluntary notices to CFIUS, but there are some exceptions for mandatory declarations in cases where a foreign government is acquiring a substantial interest in specified types of American businesses. Although FIRRMA and the final regulations impact real estate transactions, this Comment focuses on the impact of minority investments in U.S. critical technology.

Noncompliance with CFIUS often results in civil penalties, which may amount to the total value of the transaction. FIRRMA authorizes CFIUS to: “conduct periodic reviews of mitigation agreements”; “negotiate, enter into or impose, and enforce any agreement or condition with any party to

82. Jackson, supra note 42, at 17 (stating that previously, a controlling interest was “at least 10% of the voting shares of a publicly traded company, or at least 10% of the total assets of a non-publicly traded United States company”); see also Reid Whitten et al., FIRRMA Takes Form as CFIUS Enacts a New Pilot Program Targeting “Critical Technologies,” NAT'L L. REV. (Oct. 11, 2018), https://www.natlawreview.com/article/firrma-takes-form-cfius-enacts-new-pilot-program-targeting-critical-technologies (defining the twenty-seven pilot industries).


84. See id. (explaining that the “Treasury anticipates issuing a notice of proposed rulemaking that would revise the mandatory declaration requirement regarding critical technology from one based on North American Industry Classification System codes to one based on export control licensing requirements,” and showing the continued balance between CFIUS and export controls).

85. See id. (noting that parties may elect to file a notice instead of a declaration).

86. See Levine & Paretzky, supra note 11 (stating that FIRRMA allows CFIUS review of covered real estate transactions near sensitive United States government property or with national security implications).

an investment transaction during and after consideration of a transaction to mitigate any risk to the national security of the United States”;
and review the appropriateness of an agreement or condition.
Before entering into a mitigation agreement, FIRRMA mandates that CFIUS consider whether the agreement will enable effective monitoring and enforcement of its terms.

Ralls Corporation (Ralls), a Delaware company owned by Chinese nationals, is the first foreign investor to reject a CFIUS order, claiming that the order violated its constitutional rights. Ralls submitted a voluntary notice to CFIUS regarding the acquisition of a turbine windfarm in Oregon, which triggered a CFIUS review because the wind farm was located near a U.S. Navy training facility.

Following a CFIUS review, a Presidential Order demanded Ralls halt all business because the covered transaction was prohibited. Ralls appealed, and the Court of Appeals held that the presidential veto deprived Ralls of its constitutionally protected property interests without procedural due process. Ralls’s property interest in the acquisition of the companies invoked the Due Process Clause, prompting the Court to apply a three-factor balancing test.

The Court considered the private interest affected by government action, the risk of erroneous deprivation of that interest, and the burden of additional or alternative procedures. The parties settled before the Court ruled on whether CFIUS exceeded its authority. The Ralls decision shows that litigation is an option for companies wishing to engage with CFIUS, and that foreign acquirers must be ready to face a scrutinious process when it comes to CFIUS review.

FIRRMA fails to define a process to contest

88. See Jackson, supra note 42, at 33 (emphasizing that CFIUS has broad enforcement power).
91. Ralls Corp. v. Comm. on Foreign Inv. in the U.S., 758 F.3d 296, 301, 304 (D.C. Cir. 2014).
92. Id. at 301–02; see also Jackson, supra note 42, at 22 (stating that the process by which the disposition of a transaction is determined is subject to judicial review to ensure constitutional rights are upheld).
93. Ralls Corp., 758 F.3d at 311.
95. See id. (expanding on the three-factor test).
96. Id.
a CFIUS order but gives CFIUS broad authority to impose penalties for compliance failures.97

FIRRMA expands CFIUS’s jurisdiction, giving CFIUS broader authority to launch reviews. However, FIRRMA’s limited impact on IP is not enough to close the gap on unauthorized foreign access to U.S. IP, allowing for potential leakage.

II. ANALYZING THE IMPACT OF FIRRMA ON INTELLECTUAL PROPERTY

A. Facing FIRRMA: Expanding CFIUS’s Authority

CFIUS is authorized to review transactions that may result in a foreign entity gaining control of a U.S. business and to determine the effect of such transactions on national security.98 The FIRRMA-amended CFIUS process maintains the President’s authority to block or suspend foreign “mergers, acquisitions, or takeovers” of U.S. entities that threaten national security.99 CFIUS may refer the transaction to the President (based on its initial investigation), who can then take further action, such as blocking or suspending a proposed or pending foreign investment that threatens national security.100 However, before the President may invoke his authority, he or she must conclude that other U.S. laws are inadequate or inappropriate to protect national security and that there is “credible evidence” that the foreign investment will impair national security.101

Since the creation of CFIUS, presidents have only blocked deals on five occasions.102 The first occurred in 1990 when President George H.W. Bush voided the sale of a Seattle-based aircraft parts manufacturer to a Chinese

98. Committee Composition, supra note 7; see, e.g., Diane Bartz, Tighter U.S. Foreign Investment Rules Aimed at China Start in November, Reuters (Oct. 10, 2018, 8:10 AM), https://www.reuters.com/article/us-usa-trade-security/tighter-u-s-foreign-investment-rules-aimed-at-china-start-in-november-idUSKCN1MK1IC (discussing that, when CFIUS ordered Chinese conglomerate HNA Group to sell its majority stake in a building whose tenants included police tasked with protecting Trump Tower, it presented a national security issue).
99. See JAMES K. JACKSON & CATHLEEN D. CIMINO-ISAACS, CONG. RSCH. SERV., IF10952, CFIUS REFORM UNDER FIRRMA 1 (2020) (clarifying that the new regulations include joint ventures as part of covered transactions subject to CFIUS review).
100. See id. at 11 (explaining when Presidents have blocked acquisitions).
101. See id. at 11 (showing that if CFIUS determines it does not have credible evidence that an investment will impair national security, then it is not required to undertake an investigation and the issue is unlikely to ever reach the President).
102. See Jackson, supra note 42, at 21 (describing the occasions).
entity. President Obama blocked Ralls Corporation from acquiring a wind farm in 2012, and used his authority again in 2016 to block the takeover of Aixtron, a German semiconductor company, by a Chinese entity with government ties in China. In 2017, President Trump blocked a Chinese investment firm from acquiring Lattice Semiconductor Corporation. In 2018, President Trump also stopped Broadcom from acquiring Qualcomm. On all five occasions, the President has generally relied on national security as justification for blocking the transactions, with little clarification about the plausibility of those concerns.

The United States left the term national security undefined for decades, which gave both CFIUS and the President flexibility in asserting jurisdiction. The Foreign Investment and National Security Act of 2007 mandates that CFIUS publish guidance on the “types of transactions that the Committee has reviewed and that have presented national security considerations.” While CFIUS guidance does not provide a definition, it does break national security concerns into two broad categories: those raising concerns due to “the nature of the U.S. business over which foreign control is being acquired” and those raising concerns due to “the nature of the foreign person who acquires control over the U.S. business.” For further guidance, CFIUS may consider eleven factors, giving the Committee the power to exercise its discretion in deciding which factors to consider.

104. See Jackson, supra note 42, at 21 (describing the Obama-era blockages based on CFIUS reviews).
105. See id. (noting President Trump’s use of CFIUS).
106. See Presidential Order, supra note 56 (detailing the near-takeover of Qualcomm by Singaporean company Broadcom).
107. See Jackson, supra note 42, at 22 (noting the President is authorized to take action as he deems appropriate to “suspend or prohibit any covered transaction that threatens to impair the national security of the United States,” and that such action is unappealable).
109. See id. at 1242–43 (explaining that the Guidance gives little predictive value because it does not provide comprehensive information on the types of transactions that presented national security concerns).
111. 50 U.S.C. § 4565(f).
factors are outlined in the Defense Production Act of 1950. The U.S. government does not restrict or monitor foreign investors from investing in early-stage technology. The tools it does have are CFIUS and export controls, which prevent and monitor the export of certain items abroad. CFIUS reviews specific deals on a case-by-case basis, as demonstrated when CFIUS required Japanese-owned company Softbank to agree to multiple mitigation measures when it acquired Sprint. Further, even with the increased regulations under FIRMA, CFIUS’s jurisdiction remains limited, especially because export controls do not mitigate all possible concerns with foreign investment.

Export controls can prevent technology transfer to foreign entities and are regulated by government organizations, including “the Export Administration Regulations (EAR), administered by the U.S. Department of Commerce, Bureau of Industry and Security (BIS), and the International Traffic in Arms Regulations.”

112. See id. (listing the relevant factors subject to interpretation by the Committee as: (1) “domestic production needed for the projected defense requirements”; (2) “the capability and capacity of domestic industries to meet national defense requirements”; (3) “control of domestic industries and commercial activities by foreign citizens as it affects” national security requirements; (4) “the potential effects of the proposed or pending transaction on sales of military goods, equipment, or technology to any country”; (5) “the potential effects of the proposed or pending transaction on United States international technological leadership in areas affecting national security”; (6) “the potential national security related effects on critical” infrastructure; (7) the potential national security related effects on critical technologies; (8) “whether the covered transaction is a foreign government controlled transaction”; (9) “whether transactions require an investigation”; (10) “the long term projection of United States requirements for sources of critical resources”; and (11) “other factors that the President or [CFIUS] deems appropriate”).


114. See id. at 2 (explaining that export controls help deter exports to sanctioned countries and help prevent sensitive products from being shipped to such countries).

115. See Wilson Sonsini Goodrich & Rosati, CFIUS in 2017: A MOMENTOUS YEAR 3 (2018), https://www.wsgr.com/publications/PDFSearch/CFIUS-Report/2017/CFIUS-YIR-2017.pdf (stating that CFIUS received more than 170 filings in 2016; see also Jackson, supra note 42, at 56 (noting that a complication with the transaction included that Sprint was to acquire Clearwire, a company that relied on Chinese firm Huawei for equipment. Softbank agreed to remove Huawei as a supplier to finalize the acquisition of Sprint)).

116. See Brown & Singh, supra note 113 (rejecting notion that CFIUS and export controls are enough to protect the United States from foreign investment national security concerns).
Regulations (ITAR), administered by the U.S. Department of State, Directorate of Defense Trade Controls (DDTC).”

While export controls are necessary to prevent theft, they only work if used in conjunction with other controls. FIRRMA expands CFIUS jurisdiction to cover noncontrolling investments, addressing a previous criticism of CFIUS by giving CFIUS greater control over covered investments with businesses involved in critical technologies, critical infrastructure, and sensitive personal data (the TID businesses). Previously, CFIUS could not review several transaction types, such as joint ventures and minority investments; however, they are now covered under FIRRMA. FIRRMA increases the number of transactions subject to CFIUS review, including—and most importantly—the noncontrolling investments in critical technology companies, in addition to any investment by a foreign person in a U.S. business, if there is a potential impact on national security.

This increase in the number of potential transactions subject to review signifies that CFIUS needs greater resources to address the expansions under FIRRMA. Importantly, the term “U.S. business” is broadly defined under CFIUS, which could subject transactions between two non-U.S. entities to CFIUS’s jurisdiction and a potential review if the venture involves a U.S. business because of interstate commerce.

Initially, FIRRMA established a voluntary declaration process, which requires parties to provide basic information about a transaction at least forty-five days before closing, or filing a full written notice no later than ninety days before closing. Under the final regulations, FIRRMA now requires mandatory disclosures for some foreign investments. Specifically, there are mandatory filing requirements for certain transactions in which a

119. See Brown et al., supra note 113, at 23 (emphasizing the importance of expanded CFIUS’s jurisdiction).
120. See 31 C.F.R. § 800.208 (maintaining that the definition of “control” remains unchanged).
121. See 31 C.F.R. § 800.252 (changing the definition of “U.S. business” to mean any entity engaged in interstate commerce in the United States).
123. Id. at 2.
124. Id.
A foreign person obtains a “substantial interest”\textsuperscript{125} in a TID U.S. business\textsuperscript{126} where a foreign government holds a “substantial interest” in the foreign person.\textsuperscript{127} The final regulations provide some clarity on the term “substantial interest,” stating that the phrase applies to a single foreign government and, in certain circumstances, may only apply to the foreign government’s interests in the general partner (disregarding limited partner interests).\textsuperscript{128} FIRRMA authorizes CFIUS to designate other transactions for mandatory disclosures based on underlying factors, including the sector of the U.S. business and the “difficulty of remedying the harm to national security” that the transaction would cause.\textsuperscript{129} There are also mandatory declaration requirements for the technologies covered under the pilot program.\textsuperscript{130}

To address public comments and the scope of mandatory declarations, the pilot program expired when the final regulations took effect under FIRRMA.\textsuperscript{131} While the pilot program is discontinued, CFIUS continues the mandatory declaration requirement for the twenty-seven industries addressed under the pilot program.\textsuperscript{132}

\textbf{B. CFIUS and FIRRMA: The Impact on Protecting Intellectual Property}

FIRRMA modernizes and strengthens CFIUS by broadening the scope of CFIUS’s jurisdiction to include transactions involving critical infrastructure, critical technology, and companies that maintain or collect sensitive personal data.\textsuperscript{133} FIRRMA also extends the CFIUS review process, introduces a declarations process that requires filings for certain transactions,

\begin{itemize}
  \item \textsuperscript{125} See 31 C.F.R. § 800.244 (defining the term “substantial interest” as a voting interest, direct or indirect, of 25\% or more by a foreign person in a U.S. business and a voting interest, direct or indirect, of 49\% or more by a foreign government in a foreign person).
  \item \textsuperscript{126} See id. § 800.248 (defining TID businesses).
  \item \textsuperscript{127} See 84 Fed. Reg. 50,179 (Sept. 24, 2019) (to be codified at 31 C.F.R. pt. 800) (clarifying that the proposed rule defines substantial interest with respect to a person’s ability to influence the actions of another person in a manner that has the potential, directly or indirectly, to impair the national security of the United States).
  \item \textsuperscript{128} See supra note 125 and accompanying text (defining substantial interest).
  \item \textsuperscript{129} See Thomas et al., supra note 122.
  \item \textsuperscript{130} See Off. of Pub. Affs., U.S. Dep’t of the Treasury, supra note 83 (explaining the final regulations for the pilot program).
  \item \textsuperscript{131} See generally 31 C.F.R. pt. 801 (2019) (explaining how the program terminates, and how mandatory declarations work, under the program); see also Off. of Pub. Affs., U.S. Dep’t of the Treasury, supra note 83, at 6 (noting that the pilot program was discontinued).
  \item \textsuperscript{132} See generally 31 C.F.R. pt. 801 (naming the industries, including manufacturing, nanotechnology, and biotechnology).
\end{itemize}
and establishes a process to voluntarily file.\textsuperscript{134} Congress failed to incorporate a technology transfer provision in the final FIRMA regulations even though it was included in original drafts.\textsuperscript{135}

Nevertheless, legislators sought to fill the gap through export controls. Under ECRA, the Department of Commerce can evaluate national security considerations related to technology transfer under certain conditions, such as reviewing export license applications.\textsuperscript{136} The congressional directive under FIRMA supplements ECRA, stating that FIRMA should identify “emerging and foundational technologies” essential to U.S. national security and not included in existing definitions of critical technology.\textsuperscript{137} The directive indicates that the Administration should take into account certain factors: the development of emerging and foundational technologies in foreign countries; the effect of U.S. export controls on the development of such technologies within the United States; and the effectiveness of export controls on limiting the proliferation of such emerging and foundational technologies to foreign countries.\textsuperscript{138} ECRA also contains exceptions to the requirement to impose export controls on emerging and foundational technologies. ECRA indicates a distinct difference between the ordinary course of business transactions and transactions with the potential to transfer fundamental technical knowledge to foreign persons.\textsuperscript{139} Through the exceptions, it appears Congress hopes to limit technology transfer in a way that it could not do through CFIUS or FIRMA. FIRMA allows CFIUS to recommend technologies for identification as “emerging and foundational” based on information from CFIUS reviews and investigations.

\textsuperscript{134} See Levine & Paretzky, supra note 11 (explaining how FIRMA impacts covered transactions and certain real estate transactions).


\textsuperscript{136} Id.


\textsuperscript{138} See id. (indicating that the process is aimed at limiting technology transfers).

as well as notices and declarations identified by CFIUS.\textsuperscript{140} It began this process with the pilot program implementation.\textsuperscript{141}

While both the FIRRMA legislation and ECRA fail to explicitly address IP as part of critical technologies or emerging and foundational technologies, it is likely that the broad definitions in both regulations are intended to address IP. A few factors that CFIUS considers in its review of national security requirements easily apply to IP.\textsuperscript{142} The broad legislation and the inclusion of critical technology as a factor may have been the legislature’s way of including IP. The seventh factor states that “the potential national security-related effects on United States critical technologies” captures a transaction where a foreign entity invests in a critical technology company in return for access to its IP.\textsuperscript{143} The broad definition of critical technology\textsuperscript{144} suggests that the regulations meant the term to cast a wide net, potentially allowing for the inclusion of IP. Additionally, Congress may have intended FIRRMA to lessen the impact of potential technology transfer with more stringent rules regarding passive limited partners. Prior to FIRRMA, acquisitions of less than 10\% of the business were outside of CFIUS’s jurisdiction.\textsuperscript{145} Now, a passive minority investment may be included within the scope of CFIUS’s jurisdiction if it involves one of the TID businesses—critical infrastructure, critical technologies, or sensitive personal data.\textsuperscript{146}

\textsuperscript{140} See id. (opining that the intertwined export control and FIRRMA process is designed to address a gap between sensitive technologies that are not captured by current export laws).

\textsuperscript{141} See Reid Whitten et al., supra note 82 (explaining the pilot program origins).


\textsuperscript{143} See 50 U.S.C. § 4565(f)(7) (taking into consideration the potential national security implications as they relate to critical technologies); see also Nastase, supra note 142, at 174–75.


\textsuperscript{145} See Jackson, supra note 42, at 17 (addressing concerns that, even where a foreign firm has a noncontrolling interest, there is the potential for that foreign entity to “affect certain decisions made by or obtain certain information from, a U.S. business with respect to the use, development, acquisition or release of critical technology”).

\textsuperscript{146} See Levine & Paretsky, supra note 11 (discussing activities that subject a foreign individual or state to heightened CFIUS scrutiny).
ECRA also codifies the regulatory process around imposing controls on technology that affect national security. During the legislative process, many members of Congress and commentators voiced concerns that if CFIUS had jurisdiction over outbound investments, it would discourage welcome foreign investments. However, if CFIUS had jurisdiction over outbound investments, it would have had jurisdiction over investments involving the transfer of IP. CFIUS would thus have authority to alter or block outbound investments that resulted in the transfer of critical technology and that the export system did not regulate. There were further concerns that jurisdiction over outbound investments would have only regulated the transfer of critical technologies in connection with covered investments, which presented a potential gap in the system. Therefore, the congressional solution was to put more effort into identifying emerging and foundational technologies through both export control regulations and FIRMA.

While identifying emerging and foundational technologies is important to address national security concerns, it fails to adequately address the impacts on IP. Public comments show the importance of distinguishing emerging technologies from mature technologies. For example, Amazon cited that some technologies, such as artificial intelligence and machine learning, are not emerging technologies but “ubiquitous” products resulting from decades of research. However, such blanket statements allow for certain IP to fall


148. Id.

149. See id. (demonstrating the lack of IP protection within FIRMA’s current implementation).

150. See id. (asserting that CFIUS jurisdiction over outbound investments would be both an over-control and an under-control. It would over-control benign investments that could place burdens on CFIUS and discourage welcome investments. It would under-control because it would regulate only the transfer of newly identified critical technologies, which means that identical technologies without government oversight could be transferred. Further, technologies could be transferred without government regulation to a foreign person if the transaction was not part of a covered investment).

151. See id. (clarifying that the law limits the scope of controls to those that both address national security concerns and are essential to national security, which potentially excludes IP).

into the hands of foreign investors if it remains unregulated, as it would not be emerging technology.

Technology transfer directly affects IP. Technology transfer includes formal channels like trade, licensing, joint ventures, and FDI. FDI in U.S. companies often means that foreign investors get access to the sensitive technologies that companies develop, which poses a potential national security concern. Foreign investment is often used as a strategic tool to obtain IP so foreign investors can boost their own technological capabilities. The issue is further complicated because many companies developing these technologies operate in the commercial sector and are not fully aware of the risks that technologies—such as dual-use technologies—pose. Examples include artificial intelligence and biotechnology. Countries like China invest in critical technologies that pose dual-use threats. China seeks access to key technologies in three ways: Chinese

iew.com/defining-emerging-technologies-industry-weighs-in-on-potential-new-export-contr-ols/ (noting that Genentech, a biotechnology company, stated that the biotechnology field is global and no longer emerging, and that “Boeing suggested that technology already subject to an export control regime . . . should be excluded from the definition of ‘emerging’”).  


155. See id. at 1 (stating that technology transfer can negatively affect U.S. technological superiority, and that access to sensitive information associated with critical technologies may be used by foreign countries for military applications).  

156. See id. at 7–8 (defining dual-use technologies as technologies that can be used both in the civilian and military sectors).  

157. Id. at 15–16 (demonstrating that biotechnology has the potential to develop chemical and biological weapons, which poses a greater risk than its use in civilian life to treat patients. Companies that operate in the commercial sector could be unaware that their IP could be used for dangerous applications).  

158. Id. at 17 (opining panelists’ beliefs that Chinese interests are increasingly focused on investing in U.S. companies developing technology to facilitate technology transfer, which reflects “an effort to build [the Chinese] economy and military at the expense of the United States”); see also U.S. DEP’T OF DEF., ASSESSING AND STRENGTHENING THE MANUFACTURING AND DEFENSE INDUSTRIAL BASE AND SUPPLY CHAIN RESILIENCY OF THE UNITED STATES: REPORT TO PRESIDENT DONALD J. TRUMP BY THE INTERAGENCY TASK FORCE IN
companies invest directly in established U.S. companies; Chinese companies
directly acquire U.S. companies; and Chinese private equity firms invest in
startups based in the United States.\textsuperscript{159}

While CFIUS does not enforce IPRs, FIRRMA allows it to review more
covered transactions.\textsuperscript{160} Mitigation measures could include “placing
intellectual property in escrow; controlling the foreign person’s access to the
intellectual property; requiring mechanisms to monitor and enforce such
access controls; and ensuring U.S. government access to, or insight into, the
intellectual property.”\textsuperscript{161} However, mitigation levels remain at the
discretion of CFIUS.

III. RECOMMENDATIONS

FIRRMA extends CFIUS’s jurisdiction to review noncontrolling
transactions that pose a threat to national security, including a broader
definition of critical technologies.\textsuperscript{162} CFIUS review now extends to “capture
a transaction in which a foreign entity invests a small, non-controlling stake
in a start-up critical technology company in return for access to its IP and
related support . . . .”\textsuperscript{163} Since CFIUS can now review noncontrolling
transactions under FIRRMA, the legislation takes some necessary steps to
prevent harmful IP acquisition.\textsuperscript{164}

\textsuperscript{159} See U.S. GOV’T ACCOUNTABILITY OFF., supra note 154, at 11 (explaining that many
investments are not tracked by the U.S. government, thus limiting visibility into foreign
investors and the technologies they are investing in).

\textsuperscript{160} See Covered Transactions, 85 Fed. Reg. 3112, 3128 [Jan. 17, 2020] (to be codified
at 31 C.F.R. pt. 800–01) (defining a covered transaction as: “(a) A covered control transaction;
(b) [a] covered investment; (c) [a] change . . . that [ ] could result in a covered control
transaction or a covered investment; or (d) [a]ny other transaction, transfer, agreement, or
arrangement . . . designed or intended to evade or circumvent” a CFIUS review).

\textsuperscript{161} 2019 EXEC. OFF. OF THE PRESIDENT ANN. INTELL. PROP. REP. TO CONG. 145,
Property-Report-to-Congress.pdf.

\textsuperscript{162} See CFIUS & FIRRMA, supra note 8 (discussing CFIUS’s expanded jurisdiction).

\textsuperscript{163} Ian DiBernardo & Chris Brewster, \textit{Are IP Licenses the Next Target for National Security

\textsuperscript{164} See OFF. OF PUB. AFFS., DEP’T OF THE TREASURY, supra note 59 (explaining
noncontrolling investments).
However, FIRRMA must address IP more explicitly. While the final regulations went into effect on February 13, 2020,\(^\text{165}\) the regulations could be updated in the future. First, while export controls cover part of the outbound technology transfer,\(^\text{166}\) CFIUS should close the gap by directly regulating outbound technology transfers pursuant to its authority under FIRRMA, rather than deferring to export controls to regulate this issue. Early drafts of FIRRMA called on CFIUS to review outbound technology transfers and IP transfers—a responsibility that was ultimately given to export controls.\(^\text{167}\) As economic security becomes more closely aligned with national security, it is now more important than ever to ensure IP technology transfers are regulated.\(^\text{168}\) Failing to do so could have devastating effects, especially given the rise of dual-use technologies.\(^\text{169}\) Limiting FIRRMA to only inbound investment, and regulating outbound investment only through export controls, poses a long-term risk.\(^\text{170}\)

Second, CFIUS could carve out IP as part of the FDI review process. The carveout could happen in one of two ways. First, CFIUS could review the IP that would be transferred as part of the investment before approving the transaction. The risk of technology transfer, and therefore the risk of IP acquisition by foreign investors, could be mitigated without rejecting

\(^{165}\) Off. of Pub. Affs., U.S. Dep’t of the Treasury, supra note 69.

\(^{166}\) See The Export Control, supra note 147 (explaining that outbound technology transfer involves an overseas transfer of IP and associated support).

\(^{167}\) See Naso, supra note 44 (clarifying the relationship between CFIUS and export controls); see also Covington, CFIUS Developments: Senate Banking Committee Releases Draft Manager’s Amendment to FIRRMA (2018), https://www.cov.com/-/media/files/corporate/publications/2018/05/CFIUS_developments_Senate_Banking_Committee_releases_draft_managers_amendment_to_firrma.pdf (noting that an amendment modified CFIUS provisions to remove earlier versions of FIRRMA that expanded CFIUS jurisdiction to review outbound transfers of IP that did not involve acquisition of a U.S. business, such as joint ventures. Reflecting the final regulations, the amendment replaced the provision with an export control process that would identify emerging and foundational technologies).

\(^{168}\) See U.S. Dep’t of Def., supra note 158, at 42 (explaining that predatory practices, including IP theft, destroy commercial product lines and markets, which directly impacts U.S. trade markets).

\(^{169}\) See U.S. Gov’t Accountability Off., supra note 154, at 15 (explaining dual-use technologies as those with both military and civilian uses).

\(^{170}\) See Jacqueline Varas, CFIUS, Export Controls, and National Security, Am. Action F. (May 21, 2018), https://www.americanactionforum.org/insight/cfius-export-controls-and-national-security/ (maintaining that there is a growing consensus that FIRRMA should be used to increase national security protections in the United States).
foreign investment. Alternatively, as part of its review process, FIRRMA could require that IP be carved out of foreign acquisitions entirely. In a carveout transaction, the U.S. business may exclude certain IP from the acquisition. Therefore, IP would not be included in the assets that foreign direct investors acquire or access. Through a carveout, CFIUS could require that IP is either removed entirely from a transaction or addressed through a review process before gaining CFIUS approval. The impact of the carveouts ensures that IP is reviewed before it reaches a foreign investor or that IP never reaches foreign investors because it is excluded entirely from the FDI process.

Third, export controls should not be the only means through which outbound technology transfers are regulated. FIRRMA should address technology transfer concerns through a mandatory process that evaluates the degree to which a foreign entity will protect the IP of the U.S. business it invests in. CFIUS already considers many factors when determining national security impact. CFIUS could add a factor that accounts for the degree of protection afforded to U.S. companies’ IP under CFIUS review. This addition could easily mitigate the issues of technology transfer at an early stage in the process. Adding this criteria to the legislation ensures that a review process exists as a check against foreign entities who may be investing only for access to IP. This is especially important when it comes to dual-use technologies given the risks and threats that such technology poses if it falls into the wrong hands and the role that dual-use


172. See Robert W. Dickey & Etienne Shanon, Carve-out Transactions, PRACTICAL LAW CO., Dec. 2010, at 1, Practical Law Practice Note 7-504-1544 (defining carveout transactions as “sale of a subsidiary, division or other smaller part of a larger business enterprise”).

173. See Jalious et al., supra note 139 (explaining that export controls protect emerging and foundational technologies while leaving a gap that is not covered by the current export control regulations).

174. See Defense Production Act of 1950, 50 U.S.C. § 4565 (listing the relevant factors that are subject to interpretation).

175. See generally MARIO W. CARDULLO, INTELLECTUAL PROPERTY – THE BASIS FOR VENTURE CAPITAL INVESTMENTS, WORLD INTELL. PROP. ORG. (2004), https://pdfs.semanticscholar.org/a0e4/f6d0ce3ed07a40b6d4a4624f8e043264135a6.pdf (demonstrating the intertwined nature of investments and access to IP because of the potential growth value of IP).
technologies play in defining critical technologies. While there is an argument that export controls will regulate these dual-use technologies, this will not be the case unless the technology is being exported to sanctioned parties or destinations.

Finally, it is well documented that there were gaps in CFIUS’s authority. For example, prior to FIRMA, purchasing a U.S. business in close proximity to a sensitive military location was subject to CFIUS review but purchasing real estate in the same location was not. Moving assets to avoid CFIUS review, among other evasive strategies, were part of the reason to revamp CFIUS through FIRMA. These issues evidence that the current FIRMA legislation allows for IP to slip through the gaps by not directly addressing it in the review process. If a review process is not feasible, then those who access IP without authorization should face heavy penalties. Because most of the CFIUS review process still relies on good

176. See Perspectives on Reform, supra note 171, at 50 (considering that technology transfer is especially critical in the FIRMA debate when it comes to dual-use technologies).

177. See Perspectives on Reform, supra note 171, at 15–16 (statement of Hon. Richard E. Ashooh, Assistant Secretary, Export Administration, U.S. Department of Commerce) (noting that many dual-use items are subject to the Export Administration Regulations, but are regulated only when they are exported to sanctioned destinations or parties).

178. See Perspectives on Reform supra note 171, at 10 (statement of Hon. Heath P. Tarbert, Assistant Secretary, International Markets and Investment Policy, U.S. Department of the Treasury) (explaining that prior to FIRMA, some parties structured transactions to stay below the control threshold for CFIUS review or moved critical technology and expertise to offshore joint ventures).

179. See id. at 10–11 (emphasizing that one could still place a business on purchased real estate, and that there are disparate outcomes in transactions presenting “identical national security threats”).

180. See id. (emphasizing that gaps can lead to disparate outcomes in transactions with identical national security threats); see also Varas, supra note 170 (demonstrating that new legislation was needed to address a changing foreign investment landscape, especially with the advent of noncontrolling investments and joint ventures).

181. See Perspectives on Reform, supra note 171, at 11 (statement of Hon. Heath P. Tarbert) (documenting the reasoning for implementing FIRMA as twofold: to close gaps in CFIUS’s authority by expanding the types of transactions subject to review and giving CFIUS greater ability to prevent parties from restructuring transactions to evade CFIUS review).

182. See Perspectives on Reform, supra note 171, at 94 (statement of Derek Scissors, Resident Scholar, American Enterprise Institute) [arguing that export controls and CFIUS review fail to address the problem of intellectual theft, especially from Chinese adversaries]; see also 31 C.F.R. § 800.901 (2020), WL 31 C.F.R. §§ 800.901 (defining the penalty regulations as “not to exceed $250,000 per violation or the value of the transaction, whichever is greater;” which shows that CFIUS does not shy away from heavy fines).
faith declarations, even when it comes to mandatory reporting, it is possible that parties will not comply.

CONCLUSION

There are conflicting views regarding the breadth of CFIUS’s authority. While concerns regarding harm to the industrial base are valid because foreign investment is often critical to helping smaller companies grow, such growth is not important enough to justify giving foreign investors unlimited access to companies. Export controls do not fill the gap that CFIUS leaves for evaluating IP impact. As technology continues to rapidly change, it remains critical for the United States to protect its IP technology. CFIUS can mitigate risks through FIRMA by implementing one of the aforementioned strategies as part of its review process. Failure to do so poses a major national security risk—one that CFIUS alone cannot fix.

183. See 31 C.F.R. § 800.402 (2020), WL 31 C.F.R. §§ 800.402 (indicating that most CFIUS reviews rely on voluntary declarations, which depend on the good faith of parties disclosing transactions to CFIUS).

184. See Perspectives on Reform, supra note 171, at 46–47 (explaining that one view asserts broader authority is necessary because technology evolves more quickly than regulations are updated, while the other view asserts the U.S. industrial base is harmed by additional regulatory burdens); see also Perspectives on Reform, supra note 171, at 80 (statement of Celeste Drake, Trade and Global Policy Specialist, AFL-CIO) (rebutting the presumption that FDI is always positive because some investors might invest with the intent to transfer IP).

185. See Perspectives on Reform, supra note 171, at 47 (opining that foreign parties may choose to invest in other countries that do not present such burdensome regulatory conditions).

186. See Kevin Wolf, Assistant Sec’y of Com. for Exp. Admin., U.S. Dep’t of Com., Remarks at the BIS Update Conference (Oct. 31, 2016), https://www.bis.doc.gov/index.php/about-bis/newsroom/speeches/speeches-2015/1164-remarks-of-assistant-secretary-kevin-j-wolf-at-the-2016-update-conference (demonstrating that there are two ways to simplify the system: requiring a license for all exports or not requiring a license unless specifically stated by the government. The former imposes massive burdens on the government while the latter does not satisfy national security concerns).

187. See supra Part III (outlining strategies to protect IP through the CFIUS review process).