ARTICLE

Managing National Security Risk in an Open Economy: Reforming the Committee on Foreign Investment in the United States

Jonathan Wakely & Andrew Indorf*

* Jonathan Wakely is an associate at Covington & Burling LLP where he regularly advises clients on transactions before the Committee on Foreign Investment in the United States. He holds a B.A. from Haverford College and a J.D. from Georgetown University. Andrew Indorf is a law clerk at Covington & Burling LLP. He holds a B.S. from Georgetown University and a J.D. from Stanford Law School. We thank the editors of the Harvard National Security Law Journal for their contributions to this piece, as well as Linda Atiase for her assistance. The views expressed in this article are those of the authors, and do not represent those of Covington & Burling LLP or any of its clients.

Abstract

National security experts have long recognized that foreign investment, despite bringing significant economic benefits, can also create risks to national security. The United States maintains an extensive framework of laws and regulations to manage these risks. Among these is the Committee on Foreign Investment in the United States, or "CFIUS," an inter-agency committee in the Executive branch tasked with reviewing transactions that may result in foreign control of U.S. businesses. In light of changes in geopolitics and the nature of foreign investment in the United States, there is now a significant effort to reform and strengthen CFIUS. This Article proposes foundational principles to govern any reform of CFIUS in order to ensure that the United States may continue to welcome foreign investment while also protecting national security. The article also evaluates specific proposed reforms, in particular the Foreign Investment Risk Review Modernization Act introduced in November 2017.

Table of Contents

Introduction

In 2010, the People's Republic of China surpassed Japan to become the world's second-largest economy, after the United States.[1] While the implications of China's rise are myriad and hotly debated, one consequence is clear: we will soon live in a world where the world's two largest economies are also arguably the world's foremost geopolitical rivals.[2] Those circumstances may not be unprecedented, but what is unprecedented is the volume of economic interaction and cross-border investment between two geopolitical rivals that we now see between the United States and China.[3] That reality presents a challenge for policymakers in the United States: how to welcome foreign investment, including from nations that may be viewed as rivals, while also addressing national security risks that those investments may present.

National security professionals have long recognized that economic relationships and interactions, despite their vast benefits, also create risks to national security.[4] Businesses can provide cover for spies and opportunities to establish relationships that may provide access to sensitive information.[5] Militaries and intelligence agencies depend on the private sector for essential goods and services, including from companies that may be owned by foreign parties.[6] Private enterprises may develop technologies that have national security-related applications and these technologies may be lost when those businesses are acquired by foreign parties.[7]

---

[1] *See* Andrew Monahan, *China Overtakes Japan as World's No.2 Economy*, WALL ST. J. (Feb. 14, 2011), https://www.wsj.com/articles/SB10001424052748703361904576142832741439402.

[2] *See* Ryan Brown, *Top US General: China Will Be 'Greatest Threat' to US by 2025*, CNN (Sept. 27, 2017), https://www.cnn.com/2017/09/26/politics/dunford-us-china-greatest-threat/index.html [https://perma.cc/NNS2-DR8K].

[3] In 2017, for example, trade between the United States and China totaled over $635 billion. *Trade in Goods with China*, U.S. CENSUS BUREAU, https://www.census.gov/foreign-trade/balance/c5700.html (last visited May 15, 2018) [https://perma.cc/Q4TN-8FRJ]. By contrast, U.S. trade with the Soviet Union averaged approximately $2 billion annually during the mid-1980s. *See Trade in Goods with U.S.S.R.*, U.S. CENSUS BUREAU, https://www.census.gov/foreign-trade/balance/c4610.html (last visited May 15, 2018) [https://perma.cc/7SHA-FK64].

[4] *See generally*, Brian Champion, *Spies (Look) Like Us: The Early Use of Business and Civilian Covers in Covert Operations*, 21 INT'L J. INTEL. & COUNTERINTEL. 530 (2008).

[5] *See id*.

[6] *See Top 100 for 2017*, DEF. NEWS, http://people.defensenews.com/top-100/ (last visited Mar. 13, 2018) [https://perma.cc/PG5N-J7TV] (showing that of the top ten defense contractors in 2017 by revenue, four were headquartered outside of the United States).

[7] A Department of Defense sponsored report concluded last year that foreign acquisitions of early stage technology companies could result in losses of commercial technologies that have national security applications. *See* Paul Mozur & Jane Perlez, *China Tech Investment Flying Under the Radar, Pentagon Warns*, N.Y. TIMES (Apr. 7, 2017),

The subject of this Article is how governments manage the national security risks arising from economic interactions. The question is especially relevant for countries like the United States that have open economies, and that necessarily must accept risks to national security that arise from having an open economy. By contrast, closed economies like the Soviet Union had much more capacity to control risks, though at considerable economic cost.[8] The United States maintains an extensive framework of laws designed to manage national security risks, including multiple export control regimes, government procurement regulations, and other authorities. Like some other countries, the United States also maintains a special process to review certain foreign direct investments for national security reasons through the Committee on Foreign Investment in the United States, or "CFIUS."[9]

There is now a significant effort to reform and strengthen CFIUS's authority to address new perceived risks arising from investment in the United States. As described further in Part III below, these perceived risks arise from the changing composition of foreign direct investment in the United States, and also from concerns that foreign direct investment is increasingly being used to advance state policies rather than accomplish commercial goals. The past year saw multiple bills introduced in Congress that would materially change CFIUS's authority and processes.[10] Most significantly, in November 2017, Senator John Cornyn introduced a wide-ranging bill titled the Foreign Investment Risk Review Modernization Act (FIRRMA) that would reform CFIUS's authority and processes.[11] This Article examines those efforts in light of the existing legal framework and makes recommendations to improve CFIUS while preserving the United States' policy of openness to foreign investment.

In Part I, we examine the existing legal authorities available to the Executive Branch to address perceived national security risks arising from foreign

---

https://www.nytimes.com/2017/04/07/business/china-defense-start-ups-pentagon-technology.html?search-input-2=china+defense+start+ups+pentagon+technology.

[8] While state ownership of key industries avoids the risks that may be presented by foreign ownership of companies in those industries, it also eliminates foreign sources of capital that may help drive innovation. *See generally*, CIA DIRECTORATE OF INTEL., A COMPARISON OF THE US AND SOVIET INDUSTRIAL BASES (1989), https://www.cia.gov/library/readingroom/docs/DOC_0000292337.pdf [https://perma.cc/58DA-M885].

[9] *See* 50 U.S.C. § 4565 (2015). Australia conducts foreign investment reviews pursuant to the Foreign Acquisitions and Takeovers Act 1975. *Foreign Acquisitions and Takeovers Act 1975* (Cth) (Austl.). Canada's foreign investment review system is codified in the Investment Canada Act and its accompanying regulations. Investment Canada Act, R.S.C. 1985, c 28. And on March 15, 2018, the U.K. government introduced legislation to Parliament that would strengthen its ability to review national security implications arising from foreign investment into emerging technologies. *See* Enterprise Act of 2002 (Share of Supply Test) (Amendment) Order 2018.

[10] *See infra* Part II.

[11] Foreign Investment Review Modernization Act of 2017, S. 2098, 115th Cong. § 1 (2017).

trade and investment. In Part II, we examine perceived weaknesses in the existing legal framework. Part III examines the current geopolitical and other conditions that are driving the present attempt to reform the CFIUS process. Part IV sets forth recommended principles to govern reforms to CFIUS. Part V evaluates current proposals to reform CFIUS in light of the principles described in Part IV. Part VI makes specific recommendations for how to improve CFIUS.

I. Authorities to Address National Security Risks

Before turning to recent developments, we first provide a summary of authorities available to the Executive Branch under existing law to address national security risks arising from foreign investment.

As an initial matter, the President has certain authorities in the area of national security that derive directly from the Constitution, including the President's role as Commander in Chief. For example, the President has the authority to classify and declassify information, and, as a consequence, to prescribe which companies may receive classified information and prohibit the receipt of classified information from companies that are under foreign ownership, control, or influence (FOCI).[12] The rules that the Executive Branch has established to ensure the protection of classified information are detailed in the National Industrial Security Program (NISP), which governs private-sector access to classified information and is overseen by the Defense Security Service (DSS).[13] Depending on the nature of the FOCI (including the existence of any foreign government ownership in the acquirer), DSS may require that parties enter into an agreement that prohibits the foreign acquirer from accessing classified information and limits the foreign owner's ability to control the U.S. business.[14]

---

[12] *See* Dep't of Navy v. Egan, 484 U.S. 518, 527 (1988) ("The President, after all, is the 'Commander in Chief of the Army and Navy of the United States.' His authority to classify and control access to information bearing on national security . . . flows primarily from this constitutional investment of power in the President, and exists quite apart from any explicit congressional grant." (citation omitted)).

[13] *See* Exec. Order No. 12,885, 58 Fed. Reg. 65,863 (Dec. 16, 1993), *amending* Exec. Order No. 12,829, 58 Fed. Reg. 3,479 (Jan. 6, 1993).

[14] For example, DSS may require the parties to enter into a Special Security Agreement or Proxy Agreement. A Special Security Agreement mandates changes in the U.S. business' governance, visitation policies, and security practices in order to mitigate foreign control. Such agreements often include limitations on the foreign parent's representation on the U.S. business' board of directors (and the addition of several "outside directors") and the establishment of a security committee to enforce policies preventing the foreign parent from accessing or inadvertently receiving classified information. *See FOCI Mitigation Instruments*, DEF. SEC. SERV., U.S. DEP'T OF DEF., http://www.dss.mil/isp/foci/foci_mitigation.html#spec_sec_agree (last visited Mar. 21, 2018) [https://perma.cc/574F-Z6QY]. Under a Proxy Agreement, the foreign parent's shares in the U.S. business are vested in U.S. citizens, cleared by the U.S. government. These proxy holders

But in the area of trade and investment, the Constitution assigns the greatest authority to Congress.[15] The Constitution specifically assigns Congress the authority to "regulate Commerce with foreign Nations, and among the Several States."[16] Thus, to the extent that the President wishes to interfere in foreign or interstate commerce to address national security risks, the President must find his authority either in a specific constitutional grant or in a specific grant from Congress.[17] As a practical matter, however, Congress has provided the President with a broad range of authorities to take action to protect U.S. national security related to trade and investment, as detailed further below.

A. *CFIUS*

Chaired by the Secretary of the Treasury, CFIUS is an inter-agency committee specifically focused on risks that arise from transactions that may result in foreign control of U.S. businesses.[18] To that end, Section 721 of the Defense Production Act of 1950 provides that CFIUS has authority to review any "covered transaction," which "means any merger, acquisition, or takeover that is proposed or pending after August 23, 1988, by or with any foreign person which could result in foreign control of any person engaged in interstate commerce in the United States."[19]

CFIUS's jurisdiction is very broad. Essentially any collection of assets in the United States that arguably constitute a going concern may be a "U.S. business."[20] "Control" is defined by regulation to mean the power "direct or indirect, whether or not exercised, through the ownership of a majority or a dominant minority of the total outstanding voting interest in an entity, board representation, proxy voting, a special share, contractual arrangements, formal or informal arrangements to act in concert, or other means, to determine, direct, or decide important matters affecting an entity."[21] In practice, CFIUS interprets "control" very broadly, such that even minority voting interests in the range of ten

---

serve on the board of directors, and, in general, manage and operate the U.S. business independent from the foreign parent. *See id.*

[15] *See* U.S. CONST. art. II, § 2.

[16] *Id.* art. I, § 8, cl. 3.

[17] *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 585 (1952).

[18] The other members are the Departments of Justice, State, Energy, Commerce, Homeland Security, and Defense; the U.S. Trade Representative; and the White House Office of Science and Technology Policy.

[19] Defense Production Act of 1950 § 721, 50 U.S.C. § 4565(a)(3) (2015), (*amended by* the Foreign Investment and National Security Act of 2007).

[20] Regulations Pertaining to Mergers, Acquisitions and Takeovers by Foreign Persons, 31 C.F.R. § 800.226 (2017).

[21] *Id.* § 800.204.

percent may be deemed controlling, especially when combined with other rights or relationships between the parties.[22]

Once CFIUS has jurisdiction, it may review a transaction upon receipt of a voluntary notification from the parties or by its own initiative.[23] If the parties do not file voluntarily and do not receive approval from CFIUS, there is no statute of limitations preventing CFIUS from exercising its authority to initiate a review in the future.[24] Conversely, once CFIUS has reviewed a transaction and determined that there is no unresolved risk to national security, the transaction receives a legal "safe harbor" and CFIUS generally is estopped thereafter from reviewing the transaction except in very narrow and exceptional circumstances.[25] For these reasons, parties generally will file voluntarily with CFIUS if they expect that the Committee may take an interest in the transaction.

When filing with CFIUS, parties provide the Committee with a range of information regarding the U.S. business, the foreign company, and the parties' plans with respect to the proposed transaction.[26] After receiving the required information, CFIUS undertakes an initial 30-day "review" to evaluate and address any national security concerns raised by the transaction.[27] If, at the end of this review, CFIUS determines that there are "no unresolved national security concerns" with the transaction, CFIUS submits a certification and report to Congress and the action is concluded.[28] If CFIUS cannot certify to this standard, it must immediately initiate a second-stage investigation.[29] This investigation may last up to 45 days, during which the parties may submit additional supplementary information, including proposals to mitigate perceived national security risks.[30]

CFIUS treats each transaction on a case-by-case basis and undertakes a three-part national security analysis: "(i) it assesses whether the acquirer has the ability or intent to exploit or cause harm (the 'threat analysis'); (ii) it considers the U.S. business at issue, including its relationship to any weakness or shortcoming in the U.S. national defense or any susceptibility to impairment of the U.S. national security (the 'vulnerability analysis'); and (iii) it evaluates the

---

[22] *See generally* Jonathan Wakely & Lindsay Windsor, *Ralls on Remand: U.S. Investment Policy and the Scope of CFIUS' Authority*, 48 INT'L LAW. 105 (2014) (providing more in-depth analysis of CFIUS's jurisdiction).
[23] 50 U.S.C. § 4565(b)(1).
[24] *See id.* § 4565(b)(1)(D) (describing the scope of CFIUS's authority to initiate a review of a covered transaction, including covered transactions previously filed with CFIUS).
[25] *Id.*
[26] 31 C.F.R. § 800.402 (describing the contents of a voluntary notice to CFIUS).
[27] *Id.* at § 800.502 (describing procedures for the 30-day review period).
[28] *Id.* § 4565(b)(3)(C)(ii).
[29] *See id.* § 4565(b)(2)(A).
[30] *See id.* § 4565(b)(2)(C).

consequences if threat and vulnerability interact as the result of a particular transaction (the 'risk analysis')."[31]

If concerns regarding a transaction persist, the Committee has broad authority to take action to protect U.S. national security. The Committee may "enter into or impose, and enforce any agreement or condition with any party to the covered transaction in order to mitigate any threat to the national security of the United States that arises as a result of the covered transaction."[32] Examples of mitigation that CFIUS may consider to address national security risks include, among others, limitations on access to certain information, technology, or physical locations; prohibitions of certain types of communications between the U.S. business and the foreign acquirer; or requirements that the foreign person place their interests in the U.S. business into a trust controlled by U.S. persons.[33] Further, the President "may take such action for such time as the President considers appropriate to suspend or prohibit any covered transaction that threatens to impair the national security of the United States."[34]

In light of CFIUS's already broad authority, some experts question whether reforms to the statute are necessary to address emerging national security risks.[35] However, the sponsors of FIRRMA believe that there are gaps that need to be addressed, including to permit CFIUS to review transactions that do not result in "control" of a U.S. business by a foreign person, but that nonetheless may provide the foreign person with access to sensitive information or technology.[36] The perceived gaps in CFIUS's authorities are discussed further in Part II.

---

[31] ORG. FOR INT'L INV., THE CFIUS PROCESS 3, http://www.ofii.org/sites/default/files/OFII_CFIUS_Primer.pdf (last visited Apr. 17, 2018).

[32] 50 U.S.C. § 4565(*l*)(1)(A).

[33] *See FOCI Mitigation Instruments*, *supra* note 14 (describing common mitigation structured implemented by DSS, which may be imposed by CFIUS).

[34] 50 U.S.C. § 4565(d)(1).

[35] *See e.g.*, *CFIUS Reform: Examining the Essential Elements: Hearing on S. 2098 Before the S. Comm. on Banking, Hous., and Urban Affairs*, 115th Cong. 2 (2018) (statement of Gary Clyde Hufbauer, Reginald Jones Senior Fellow, Peterson Institute for International Economics) ("Using existing authorities, President Trump could achieve the objectives sought by [FIRRMA]."); *Evaluating CFIUS: Challenges Posed by a Changing Global Economy: Hearing Before the H. Comm. on Fin. Servs.*, 115th Cong. 4 (2018) (statement of Theodore Kassinger, Partner, O'Melveny & Myers LLP) [hereinafter *Kassinger Testimony*] (noting that "there is no question that CFIUS possesses—and exercises—jurisdiction over acquisitions of control of U.S. business [in a variety of contexts]," and that CFIUS's jurisdiction should not extent to outbound investment).

[36] OFFICE OF SEN. JOHN CORNYN, BACKGROUND ON FOREIGN INVESTMENT RISK REVIEW MODERNIZATION ACT (FIRRMA) 1 (Nov. 7, 2017) (on file with author) [hereinafter BACKGROUND ON FIRRMA].

B. *IEEPA*

The International Emergency Economic Powers Act (IEEPA) provides the President with broad authority to take adverse economic actions upon a finding of a national emergency. The statute was passed to refine the President's emergency powers, which previously had been governed by the Trading With the Enemy Act of 1917 (TWEA).[37] The authorities granted in Section 201 of IEEPA are essentially the same as those that were provided in Section 5(b) of the TWEA, though the conditions and procedures for exercising them are different.[38]

IEEPA empowers the President to "prevent or prohibit, any acquisition, holding . . . use, transfer . . . importation or exportation of . . . any property in which a foreign country or national thereof has an interest."[39] This power may be exercised "to deal with any unusual and extraordinary threat, which has its source in whole or in substantial part outside the United States, to the national security, foreign policy, or economy of the United States, if the President declares a national emergency with respect to such threat."[40] If the United States has been attacked by a foreign country, IEEPA further permits the President to "confiscate any property" of any foreign person, organization, or country that aided in the attack.[41] To avoid treading on the First Amendment, however, IEEPA's authority does not extend to "any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value."[42]

To exercise these authorities with continuity, the President must regularly consult with and report to Congress,[43] and must annually reaffirm each emergency to avoid automatic termination.[44] By executive order and annual notice to Congress, the President has declared or reaffirmed approximately two dozen national emergencies.[45] Among these is the national security threat resulting from the expiration of another export control authority, the Export Administration Act of 1979.[46]

---

[37] *See Youngstown*, 343 U.S. at 647 n.16 (1952) (Jackson, J., concurring in the judgment).
[38] *See* Regan v. Ward, 468 U.S. 222, 224 (1984).
[39] 50 U.S.C. § 1702 (a)(1)(B) (2012).
[40] *Id.* § 1701(a); s*ee also id.* § 1621 (process for declaring national emergencies).
[41] *Id.* § 1702 (a)(1)(C).
[42] *Id.* § 1702(b)(1).
[43] *See id.* § 1703.
[44] *See* National Emergencies Act, 50 U.S.C. § 1622(d) (2015).
[45] *See* 50 U.S.C. § 1701 (listing status of declared national emergencies).
[46] *Id.*; Continuation of the National Emergency With Respect to Export Control Regulations, 82 Fed. Reg. 39,005 (Aug. 15, 2017).

C. *EAR*

The Export Administration Act of 1979 (EAA) provides additional legal authority by which the Executive Branch may control exports to promote U.S. national security and U.S. foreign policy. Although the EAA most recently expired on August 17, 2001, U.S. presidents have annually extended its authority by issuing a notice under IEEPA, discussed above.[47] President Trump issued the most recent notice on August 15, 2017, declaring a "national emergency" under IEEPA "[b]ecause the Congress has not renewed the Export Administration Act."[48]

The EAA authorizes the Secretary of Commerce[49] to "prohibit or curtail the export of any goods or technology" that would "make a significant contribution to the military potential of such country or a combination of countries which would prove detrimental to the national security of the United States."[50] To administer these restrictions, the EAA requires the Secretary to develop "control list[s]" identifying "all goods and technology subject to export controls," as well as all countries to which an export of a controlled item would prove "detrimental" to national security.[51] When determining whether a license should be required, the Secretary should consider the country of export, the good or technology controlled, and the degree to which the good or technology is already available without restriction from sources outside the United States.[52]

The Secretary of Commerce implements the requirements of the EAA through the Export Administration Regulations (EAR) administered by the Bureau of Industry and Security (BIS).[53] First, the EAR establishes a comprehensive Commerce Control List (CCL) that identifies and organizes all items subject to the export licensing authority of BIS.[54] BIS has divided the CCL

---

[47] *See* JOHN T. MASTERSON, JR., LEGAL AUTHORITY: EXPORT ADMINISTRATION REGULATIONS 86 (2017); *see also* 50 U.S.C. § 1701.

[48] Notice, Continuation of the National Emergency With Respect to Export Control Regulations, 82 Fed. Reg. 39,005 (Aug. 15, 2017).

[49] The authority granted to the President by the EAA has been delegated to the Secretary of Commerce pursuant to 50 U.S.C. § 4603(e). *See* Exec. Order No. 12,214, 45 Fed. Reg. 29,783 (May 2, 1980).

[50] 50 U.S.C. § 4604(b)(1); 50 U.S.C. § 4602(2)(a).

[51] *Id.* § 4604(b)(1), (c)(1).

[52] *See id.* § 4603(c), § 4604(f).

[53] Although the EAR are designed primarily to implement the EAA (through IEEPA), the EAR also implement numerous other statutory authorities and executive orders listed in the federal register. *See generally* OFFICE OF THE CHIEF COUNS. FOR INDUS. AND SEC., U.S. DEP'T OF COM., LEGAL AUTHORITY: EXPORT ADMINISTRATION REGULATIONS (Jan. 4, 2017), https://www.bis.doc.gov/index.php/documents/Export%20Administration%20Regulations%20Training/876-legal-authority-for-the-export-administration-regulations/file [https://perma.cc/6E9P-SBE4].

[54] *See* 15 C.F.R. § 738.1 (2018).

into ten broad categories, such as nuclear materials, electronics, and avionics, and further arranged items within each category into groups, such as materials, software, and technology.[55] Within each group, individual goods or technology are classified by an Export Control Classification Number (ECCN) specifying the item's category, group, and reason for export control. Consistent with the EAA, goods and technologies identified on the CCL are primarily "dual-use," meaning they "have both commercial and military or proliferation applications."[56]

Second, the EAR publishes a comprehensive Commerce Country Chart that lists the specific export controls and licensing requirements that apply to each foreign country[57]—or each foreign person. Importantly, the release of technology to a foreign national in the United States, whether through a demonstration or oral briefing, is "deemed" an export under the EAR.[58] To determine whether an item listed on the CCL requires a license before export, the exporting party may cross-reference the Commerce Country Chart and consider whether the purpose of the export falls within a controlled category. If a license is required, the EAR further describe the necessary application procedures. Thus, while there are opportunities for further administrative guidance,[59] the EAR ordinarily relies on self-classification of controlled items and voluntary licensing applications. To incentivize compliance, however, the EAA authorizes significant civil and criminal penalties for unlicensed exports.[60]

D. *ITAR*

Whereas the EAA and the EAR focus on dual-use technologies, the Arms Export Control Act (AECA)[61] provides the statutory framework for the President "to control the import and the export of defense articles and defense services."[62] To do so, AECA directs the President to "designate those items which shall be considered as defense articles and defense services . . . and to promulgate regulations for the import and export of such articles and services."[63] This list of

---

[55] *See id.* § 738.2(a)–(b).
[56] *See id.* § 772 (defining "dual use"); 50 U.S.C. § 4604(d)(1) (explaining that items listed on the control list should be narrowly tailored to include only "militarily critical goods and technologies").
[57] *See* 15 C.F.R. § 738 (Supp.).
[58] *Id.* § 730.5(c).
[59] *See id.* §§ 748.1, 748.3 (describing the procedures for obtaining a Commodity Classification Automated Tracking System (CCATS) number, as well as procedures for obtaining other guidance on a particular item's ECCN); *see also infra* note 66 (describing commodity jurisdiction procedures).
[60] *See* 50 U.S.C. § 4610(b)–(c) (describing civil and criminal penalties).
[61] 22 U.S.C. § 2751 (2016).
[62] *Id.* § 2778(a)(1).
[63] *Id.*

designated items constitutes "the United States Munitions List,"[64] and the regulations issued comprise the International Traffic in Arms Regulations (ITAR) administered by the Directorate of Defense Trade Controls (DDTC) at the Department of State.[65]

Similar to the Commerce Control List under the EAR, the U.S. Munitions List described in Part 121 of the ITAR describes in detail the "articles, services, and related technical data" that are subject to DDTC's jurisdiction for export control.[66] This list is intended to be comprehensive, as is the definition of "export" provided in the regulations. As defined in Part 120, an "export" includes not only an "actual shipment or transmission out of the United States," but a range of activities that may transfer technical data to a foreign person or foreign country.[67] For example, an export may also include "[t]ransferring technical data to a foreign person in the United States," "[t]ransferring registration, control, or ownership" of certain items to a foreign person, "[t]ransferring a defense article to an embassy," or "performing a defense service" for a foreign person."[68] Any entity seeking such an export of items or services identified on the U.S. Munitions List must first register with the DDTC and procure the appropriate license.[69] As with the EAR, the Department of State and Department of Justice have broad discretion to punish violations of the ITAR within significant civil and criminal penalties.[70]

---

[64] *Id.*

[65] The International Traffic in Arms Regulations, 22 C.F.R. § 120.1(a) (2017) ("The statutory authority of the President to promulgate regulations with respect to exports of defense articles and defense services is delegated to the Secretary of State by Executive Order 13637. This subchapter implements that authority, as well as other relevant authorities in the Arms Export Control Act.").

[66] *Id.* § 121.1(a). While the U.S. Munitions List is organized to make the list of covered items accessible, it may not always be clear whether a particular item should be controlled by the Department of Commerce (under the EAR) or the Department of State (under the ITAR). In such circumstances, the entity seeking export may submit a commodity jurisdiction request. *See Id.* § 120.4(a) ("The commodity jurisdiction procedure is used with the U.S. Government if doubt exists as to whether an article or service is covered by the U.S. Munitions List. . . . Upon electronic submission of a Commodity Jurisdiction (CJ) Determination Form (Form DS-4076), the Directorate of Defense Trade Controls shall provide a determination of whether a particular article or service is covered by the U.S. Munitions List. The determination, consistent with §§120.2, 120.3, and 120.4, entails consultation among the Departments of State, Defense, Commerce, and other U.S. Government agencies and industry in appropriate cases.").

[67] *Id.* § 120.17.

[68] *Id.*

[69] *Id.* §122.1, § 123.

[70] *See id.* § 127 (describing violations, penalties, and enforcement tools); *id.* § 122.27 (describing over one dozen criminal statutes pursuant to which the Department of Justice may charge individuals or entities of violating the ITAR).

E. *Government Procurement Regulations*

In addition to CFIUS and export controls, the President also has authority to mitigate national security risks that may arise through government procurement from foreign entities. This authority derives primarily from the Federal Acquisition Regulations System (FARS),[71] in particular the Department of Defense Supplement (DFARS)[72] and the Department of Energy Supplement (DEAR),[73] promulgated pursuant to the Office of Federal Procurement Policy Act of 1974.[74]

These government procurement regulations provide various restrictions on a foreign government's participation in certain federal contracts. First, they implement broad restrictions against certain countries posing significant threats to national security. For example, the DFARS prohibits the award of contracts or subcontracts of $150,000 or more to any firm in which a state sponsor of terrorism holds a "significant interest."[75] A "significant interest" may be "substantially less than actual ownership or control," and may include interests as low as five to ten percent in the firm or its subsidiary's securities or assets.[76] A similarly broad prohibition exists for contracts with Chinese companies. Under DFARS Part 225.770, the Department of Defense may not acquire "supplies or services" listed on the U.S. Munitions List through any contract or subcontract from any Chinese military company.[77] These prohibitions may be waived only when "necessary for"—or at least "not inconsistent with"—the national security objectives of the United States.[78]

More significantly, both the DFARS and the DEAR also prohibit[79] their respective agencies from awarding a national security contract to an entity "controlled by a foreign government" if the contract would require access to

---

[71] *See id.* §§ 1–99 (2017).
[72] *See id.* § 201.
[73] *See* 49 C.F.R. § 901.
[74] 41 U.S.C. §1101 et seq. (2016).
[75] 48 C.F.R. § 225.771-2; *id.* § 252.225-7050 (defining "state sponsor of terrorism" as "a country determined by the Secretary of State, under section 6(j)(1)(A) of the Export Administration Act of 1979 (50 U.S.C. § 4605 (j)(1)(A)), to be a country the government of which has repeatedly provided support for acts of international terrorism").
[76] J. EUGENE MARANS ET AL., MANUAL OF FOREIGN INVESTMENT IN THE UNITED STATES § 9:2 (2013).
[77] 48 C.F.R. § 225.770.
[78] *Id.* § 225.770-5(a) ("The prohibition in 225.770-2 may be waived, on a case-by-case basis, if an official . . . determines that a waiver is necessary for national security purposes."); *id.* § 225.771-4 ("The prohibition in 225.771-2 may be waived if the Secretary of Defense determines that a waiver is not inconsistent with the national security objectives of the United States.").
[79] This prohibition is waivable by each respective agency if a waiver is "essential to the national security interests of the United States." *See e.g.*, 49 C.F.R. § 904.7102.

"proscribed information."[80] Under the regulations, an entity is "effectively owned or controlled" by a foreign government whenever that government "has the power, either directly or indirectly, whether exercised or exercisable, to control the election, appointment, or tenure of the Offeror's officers or a majority of the Offeror's board."[81] "Proscribed information" is defined as top secret information, communications security (COMSEC) material, sensitive compartmented information (SCI), Special Access Program (SAP) information, and other data restricted under the Atomic Energy Act of 1954.[82] Thus, under the DFARS and DEAR these companies and their subsidiaries are prohibited from performing on the most classified government contracts.

II. Perceived Weaknesses in Existing Legal Framework

Notwithstanding the range of authorities available to the President to address national security risks from trade and investment, some legislators and other officials believe that existing legal frameworks have room for improvement. For example, although CFIUS has broad jurisdiction to review transactions that result in foreign control, critics of the existing CFIUS statute highlight its limits, such as CFIUS's lack of legal authority to review greenfield investments, technology transfers outside the context of a covered transaction, or certain non-passive minority investments. Similarly, certain critics perceive a variety of weaknesses in the President's authority to address national security through existing export control laws. These perceived weaknesses may arise not only from difficulties identifying sensitive technologies, but also from enforcing the laws when violations occur. This Section describes the perceived shortcomings that have been suggested with regard to CFIUS, export control laws, and related statutes to adequately address national security risks arising from foreign investment in the United States.

A. *CFIUS*

The perceived weaknesses in CFIUS's authority center on the Committee's lack of jurisdiction to review certain types of transactions, notably: (1) certain joint ventures, (2) greenfield investments and certain real estate transactions, and (3) minority investments that do not confer "control" of a U.S. business but nonetheless may raise national security concerns.

First, a leading critique of CFIUS concerns the scope of its jurisdiction regarding joint ventures. Although CFIUS has interpreted broadly its authority to review any "merger, acquisition, or takeover" that will result in foreign "control"

---

[80] 48 C.F.R. §§ 252.209-7002(b); 49 C.F.R. § 904.7100.
[81] 48 C.F.R. §§ 252.209-7002; 49 C.F.R. § 904.7100.
[82] 48 C.F.R. §§ 252.209-7002; 49 C.F.R. § 904.7100.

of a U.S. business,[83] there are certain categories of transactions and technology transfers that are beyond its jurisdiction.[84] Joint ventures, which typically are formed when two or more businesses each contribute assets to a new entity to undertake a new business, have been the subject to particular attention. Under existing law, CFIUS has jurisdiction to review the formation of joint ventures that result in foreign control of a U.S. business. For example, if a foreign company and a U.S. company form a joint venture in which the foreign person owns a fifty-one percent interest (or any other interest sufficient for CFIUS to find "control"), and the U.S. company contributes assets sufficient to comprise a "U.S. business" under the CFIUS regulations, then the formation of that joint venture is subject to CFIUS jurisdiction. But if the U.S. business contributes only intellectual property, and no other assets, then no "U.S. business" has been contributed to the foreign-controlled joint venture, and CFIUS jurisdiction is not implicated. Although technology transfers in the context of joint ventures are subject to export controls, some critics have suggested that CFIUS's lack of jurisdiction over certain joint ventures has resulted in transfers of sensitive technology to foreign countries.[85]

Second, there have also been criticisms of CFIUS's lack of jurisdiction to review greenfield investments and certain real estate transactions. In most cases, a pure greenfield investment—where a foreign investor builds a new business from the ground up—does not involve the acquisition of a "U.S. business" as defined under the CFIUS regulations, and therefore is not subject to CFIUS jurisdiction.[86] Likewise, the acquisition of real estate is not subject to CFIUS jurisdiction, unless the real estate is the home to a U.S. business (such as an office building that is leased to commercial tenants). Thus, although purchasing a *business* in close proximity to a military base would trigger CFIUS's jurisdiction, purchasing mere *real estate* does not—even if the foreign investor builds a new business onsite.[87] Depending on the location and the purchasing foreign entity, some commentators

---

[83] *See supra* notes 19–22 and accompanying text (describing CFIUS's jurisdiction under Section 721).

[84] *CFIUS Reform: Administration Perspectives on Essential Elements: Hearing on S. 2098 Before the S. Comm. on Banking, Hous., and Urban Affairs*, 115 Cong. 4 (2018) (statement of Heath P. Tarbert, Assistant Secretary of the Treasury for International Markets and Investment Policy) [hereinafter *Tarbert Testimony*] (explaining that these jurisdictional gaps are of particular concern from a national security perspective).

[85] For example, testifying at a CFIUS hearing before the Senate Committee on Banking, Housing, and Urban Affairs, Dr. James Mulvenon argued that joint ventures in China have allowed the Chinese government to seize sensitive supercomputing technology critical to maintaining the U.S. nuclear arsenal. *See CFIUS Reform: Examining the Essential Elements: Hearing on S. 2098 Before the S. Comm. on Banking, Hous., and Urban Affairs*, 115th Cong. 6–7 (2018) (statement of Dr. James Mulvenon, General Manger, Special Programs Division, SOS International) [hereinafter *Mulvenon Testimony*].

[86] *See* 48 C.F.R. §§ 225.771-2; 48 C.F.R. §§ 252.225-7050.

[87] *See Tarbert Testimony*, *supra* note 84, at 4.

have suggested that such investments may raise unaddressed national security concerns.

Third, some commentators argue that minority transactions that do not confer "control" of a U.S. business may nonetheless raise national security concerns related to access to technology or information.[88] Such investments, which may take the form of a minority investment under ten percent equity interest but where the investor gains access to certain information or technology, exist in a gray area of CFIUS's jurisdiction. Although CFIUS has a history of stretching to find jurisdiction when necessary,[89] these forms of investments may result in foreign access to sensitive information or technology without triggering CFIUS jurisdiction. In the views of these critics, revisions to the statute would better enable the Committee to consider new threats of the digital age, such as vulnerabilities related to foreign access to personal data of Americans.[90] In addition, whereas for most of the twentieth century government funding drove technological progress, we are now in an era where commercial innovation drives military technology, and where the underlying technology in a Silicon Valley product may be potentially sensitive.[91]

---

[88] *See* Sens. John Cornyn & Dianne Feinstein, *FIRRMA Act Will Give Committee on Foreign Investment a Needed Update*, THE HILL (Mar. 21, 2018), http://thehill.com/blogs/congress-blog/technology/379621-firrma-act-will-give-committee-on-foreign-investment-a-needed [https://perma.cc/9SGV-H4Z6] ("China has also been able to exploit minority-position investments in early-stage technology companies to gain access to cutting-edge IP, trade secrets, and key personnel.")

[89] *See Kassinger Testimony*, *supra* note 35, at 4 ("In practice, CFIUS has increasingly lowered the bar to finding that a 'U.S. business' exists for its jurisdictional purposes, to the point where there is no material limitation on its jurisdiction on this ground.").

[90] *See CFIUS Reform: Examining the Essential Elements: Hearing on S. 2098 Before the S. Comm. on Banking, Hous., and Urban Affairs*, 115th Cong. 6–7 (2018) (statement of Sen. John Cornyn) [hereinafter *Cornyn Testimony*] (arguing that gaps in export controls do not cover transfers of U.S. data, including personally identifiable information of U.S. citizens); *Mulvenon Testimony*, *supra* note 85, at 9 ("FIRRMA . . . [a]dds badly needed new evaluation factors, including cybersecurity threats and protection of personally identifiable information (PII).")

[91] *See* Ash Carter, Former Sec'y of Def., Remarks at the George Washington University Elliot School of International Affairs: Building the First Link to the Force of the Future (Nov. 18, 2015) ("When I began my career, most technology of consequence originated in America, and much of that was sponsored by the government, especially the Defense Department. Today, much more technology is commercial."), https://www.defense.gov/News/Transcripts/Transcript-View/Article/630419/building-the-first-link-to-the-force-of-the-future/source/GovDelivery [https://perma.cc/H6UA-WYT3]; *see also* Cade Metz, *Pentagon Wants Silicon Valley's Help on A.I.*, N.Y. TIMES (Mar. 15, 2018), https://www.nytimes.com/2018/03/15/technology/military-artificial-intelligence.html (describing the role of private companies in developing artificial intelligence for certain military applications).

B. *Export Controls*

Export controls identify and seek to control national security risks in a way that is more proactive, but less flexible, than the CFIUS process. Given the need to identify and publish these controls in advance, export controls are sometimes criticized for failing to capture cutting-edge technologies that raise national security risks, or, to the extent they do, telegraphing to the public which technologies are most valuable to the U.S. government. In addition, violations of export controls may be difficult to enforce, and their effectiveness relies in large part on compliance by private parties. These perceived weaknesses may leave the United States vulnerable to certain national security threats, according to some critics.

First, as described in Part I, above, export controls such as the EAR and the ITAR function by identifying lists of items and technology that could threaten the national security of the United States if exported to certain countries.[92] For the Departments of Commerce and State charged with implementing these regulations, maintaining control lists can be a challenging task. On one hand, control lists must be narrow enough to provide adequate guidance for companies. If U.S. companies had to request guidance from the government for each item exported,[93] federal agencies would be overwhelmed and U.S. outbound investment would suffer. On the other hand, control lists must be broad enough to ensure they capture all varieties of dual-use technologies and defense articles. Finally, control lists must be current. An over-inclusive control list could impair U.S. economic growth, while an under-inclusive list may allow for unwanted technology transfers.

Critics contend that federal agencies have failed to balance these interests, and that even if they did, the structure of export controls causes unintended consequences for national security. Some critics, for example, argue that export controls are too narrow to adequately contain technology transfers. According to James Mulvenon's testimony at a Senate FIRRMA hearing, the feature-specific nature of export control lists may allow U.S. companies to "'design out' or de-architect' specific aspects of the technology being transferred that would otherwise trigger export controls."[94] This approach may provide "70 percent of the latest technology" to China, a country which, in Mulvenon's view, has a demonstrated ability to use other investment and espionage tactics to close the gap.[95]

---

[92] *See supra* notes 47–70 and accompanying text.
[93] *See supra* note 59 and accompanying text (describing procedures for obtaining Commodity Jurisdiction and CCATS rulings).
[94] *See Mulvenon Testimony*, *supra* note 85, at 10.
[95] *Id.*

Perhaps more importantly, the increased nexus between commercial and military applications of emerging technology[96] has made it difficult to timely identify new dual-use technologies.[97] Identifying these technologies requires foresight and flexibility—a task for which a large federal bureaucracy may not be well suited. Moreover, the very nature of control lists may inadvertently telegraph to America's adversaries technologies of interest to the U.S. government. Even if export controls are nimble enough to accommodate changing technological landscapes, publishing control lists may undermine an early technological edge—the identification of the military application itself. This is especially true, critics note, if U.S. export controls operate unilaterally. If the U.S. government does not coordinate with its allies to control new technologies, the identification of a new dual-use item may alert U.S. adversaries of its military applications without constraining their ability to access the technology in other markets.[98]

Second, violations of export controls may be difficult to enforce, and full enforcement may not remedy the damage caused by an unauthorized technology transfer. Although violations of the EAR and ITAR carry significant civil and criminal penalties,[99] it may be difficult for enforcement agencies to identify undisclosed violations. This is especially so in the context of joint ventures where U.S. persons may inadvertently (or intentionally) transfer sensitive "know-how" to other engineers or employees. As described in Part I, above, both the EAR and the ITAR define exports to include transfers of certain technology and know-how to foreign persons—even if they are located within the United States.[100] According to critics, however, it is difficult for engineers to avoid transfers of know-how when operating a joint venture in a foreign country, especially when under significant pressure to perform.[101] In part due to the myriad of circumstances in which unlawful transfers could occur, it also requires significant

---

[96] *See infra* notes 132–137 (describing nexus between commercial start-up technology companies and military applications for semiconductors, artificial intelligence, and robotics).

[97] *See infra* notes 132–137 (describing nexus between commercial start-up technology companies and military applications for semiconductors, artificial intelligence, and robotics); *Mulvenon Testimony*, *supra* note 85, at 10 (highlighting the difficulty of identifying rapidly emerging technologies).

[98] *See Evaluating CFIUS: Challenges Posed by a Changing Global Economy: Hearing Before H. Comm. of Fin. Servs.*, 115th Cong. 7 (2018) (statement of Scott Kennedy, Director, Project on Chinese Business and Political Economy, Center for Strategic and International Studies) (explaining that "American efforts to constrain inappropriate technology diffusion to strategic rivals requires it to expand coordination with its allies in Europe and Asia" because "[d]ifferences in American policy and regulation . . . can and have been exploited by [adverse nations]").

[99] *See supra* notes 60, 70.

[100] *See supra* note 58 and accompanying text (describing "deemed" exports).

[101] *See Mulvenon Testimony, supra* note 85, at 10 ("It is highly unrealistic . . . to expect export controls, including deemed exports, to be able to protect against certain transfers of 'know-how' from individual engineers or subject matter experts operating inside of a joint venture on Chinese soil."); Cornyn & Feinstein, *supra* note 88.

resources for U.S. enforcement agencies to investigate and prosecute these violations. This is part of the reason why export controls generally rely on private companies to police their own practices—and to voluntarily disclose violations when they occur.[102]

III. Factors Driving Effort to Reform CFIUS

Part II described the authorities available to the Executive Branch to address national security risks presented by foreign investment and perceived weaknesses in that legal framework. In this Part, we first provide background on prior efforts to reform CFIUS, and then describe the three factors that are driving the current effort to reform CFIUS: (1) the changing composition of foreign investment in the United States; (2) the evolving destinations for foreign investment, especially in certain sensitive sectors; and (3) a perception that investment is being used by foreign governments to accomplish state objectives rather than commercial goals.

A. *Prior Reforms to CFIUS*

As described below, prior efforts to reform CFIUS have generally been driven by changes in the nature of foreign direct investment (FDI) in the United States or specific transactions that raised concerns about the United States' ability to monitor FDI and take action to protect U.S. national security. The Committee's history can be roughly broken into three distinct periods: (1) from the Committee's formation in 1975 until the passage of the Exon-Florio amendment in 1988, (2) from 1988 until the passage of the Foreign Investment and National Security Act of 2007 (FINSA), and (3) from 2007 until today. If current efforts to reform CFIUS are successful, they will mark the beginning of the fourth significant period in CFIUS's history.

CFIUS was originally established by President Ford in 1975, partly due to concerns about increased investments from Organization of Petroleum Exporting Countries.[103] As originally conceived, the Committee was directed to (1) arrange for the preparation of analyses of trends and significant developments in foreign investment in the United States; (2) provide guidance on arrangements with

---

[102] *See* 15 C.F.R. § 764.5 (2018) ("[The Department of Commerce] strongly encourages disclosure to [the Office of Export Enforcement (OEE)] if you believe that you may have violated the EAR, or any order, license or authorization issued thereunder. Voluntary self-disclosure is a mitigating factor in determining what administrative sanctions, if any, will be sought by OEE.").

[103] *See The Operations of Federal Agencies in Monitoring, Reporting on, and Analyzing Foreign Investments in the United States: Hearings Before a Subcomm. on Commerce, Consumer, and Monetary Affairs of the Comm. on Gov't Operations*, 96th Cong. 334–35 (1979) (statement of Philip E. Coldwell, Governor, Federal Reserve System); *see also* JAMES K. JACKSON, CONG. RESEARCH SERV., RL33388, THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS) 1 (2018).

foreign governments for advance consultations on prospective major foreign governmental investment in the United States; (3) review investment in the United States which, in the judgment of the Committee, might have major implications for United States national interests; and (4) consider proposals for new legislation or regulations relating to foreign investment as may appear necessary.[104] It would be more than a decade before CFIUS would be given express statutory authority to review transactions and to take action to protect national security.[105]

CFIUS operated pursuant to Executive Order 11,858 for over a decade.[106] In the 1980s, however, concerns about an influx of investments from Japanese companies led to the first significant reform to CFIUS in what became known as the Exon-Florio Amendment.[107] In particular, Fujitsu Ltd.'s proposed acquisition of Fairchild Semiconductor generated concern in Congress and elsewhere about the capacity of the U.S. government to review and, as appropriate, take action with regard to FDI to protect U.S. national security.[108] The Defense Department "opposed the acquisition because some officials believed that the deal would have given Japan control over a major supplier of computer chips for the military and would have made U.S. defense industries more dependent on foreign suppliers for sophisticated high-technology products."[109] The Exon-Florio Amendment, adopted by Congress as part of the Omnibus Trade and Competitiveness Act of 1988 and signed by President Reagan, codified in legislation CFIUS's authority to review transactions that could result in foreign control of U.S. businesses.[110] It also confirmed the President's authority to suspend or prohibit transactions that threaten to impair U.S. national security.[111] Foreshadowing today's debate about the proper scope of CFIUS's authority, the Reagan Administration objected to proposed language that would have defined CFIUS's remit as "national security and essential commerce" on the basis that the addition of the phrase "and essential commerce" would improperly expand CFIUS's authority outside of national security.[112] There have been several more recent attempts to add such economic considerations to CFIUS's authority, as described further in Part V below.

---

[104] *See* Exec. Order No. 11,858 (b), 40 Fed. Reg. 20,263 (May 7, 1975).

[105] *See* JACKSON, *supra* note 103, at 4–5.

[106] *See id*. at 3–4.

[107] *See id*. at 5.

[108] *See id*.

[109] Stuart Auerbach, *Cabinet to Weigh Sale of Chip Firm*, WASH. POST (Mar. 12, 1987), https://www.washingtonpost.com/archive/business/1987/03/12/cabinet-to-weigh-sale-of-chip-firm/63c934e8-0393-43eb-9ca2-a2ccd1d926fe/?utm_term=.9235ffc1cc5c [https://perma.cc/N7XU-QDK7].

[110] *See* JACKSON, *supra* note 103, at 5.

[111] *See id.* at 6.

[112] *See id.*

The current iteration of CFIUS traces its lineage to the passage of the Foreign Investment and National Security Act of 2007 (FINSA).[113] In this case, it was one particular transaction that caught Congress's attention and sparked the move for reform. Specifically, in 2006 CFIUS approved the acquisition of operations at certain U.S. ports from a U.K. firm by Dubai Ports World, an established port operator based in the United Arab Emirates.[114] Although the UAE is (and was at the time) an ally of the United States, the transaction took place at a time of intense focus on terrorism-related threats following the attacks of September 11, 2001.[115] CFIUS's approval of the transaction sparked a firestorm of criticism, focused on whether the Committee fully considered the effects of the transaction on U.S. critical infrastructure, especially with regard to port security and protection against terrorist threats.[116] While CFIUS ultimately determined that the transaction presented no unresolved national security risks and approved it on that basis, some in Congress disagreed with that decision, and sought to reform CFIUS to tighten its processes and give Congress more oversight.[117] FINSA reformed CFIUS in a number of ways, including giving the Committee greater authority to impose mitigation on its own, adding the protection of critical infrastructure to CFIUS's responsibilities, and providing for an increased role for Congress to receive briefings and certifications from CFIUS.[118]

B. *Changing Composition of Foreign Investment in the United States*

Like the changes in foreign investment that led to the creation of CFIUS and the Exon-Florio Amendment, the current movement to reform CFIUS is driven by significant changes in the composition of FDI in the United States. This time the impetus is the dramatic expansion in investment from China in the past five or so years. In 2007, when Congress passed FINSA, Chinese investment in the United States totaled about $356 million for the year, according to data from the Rhodium Group, an economic consultancy that tracks Chinese investment in

---

[113] Foreign Investment and National Security Act (FINSA) of 2007, Pub. L. No. 110-49, 121 Stat. 246.

[114] *See* Andreas Paleit, *How the DP World Deal Unravelled*, FIN. TIMES, (Mar. 10, 2006), https://www.ft.com/content/29e99f06-b065-11da-a142-0000779e2340.

[115] *See* Eben Kaplan, *The UAE Purchase of American Port Facilities*, COUNCIL FOREIGN REL. (Feb. 21, 2006), https://www.cfr.org/backgrounder/uae-purchase-american-port-facilities [https://perma.cc/B63F-XJ2W].

[116] *See* JACKSON, *supra* note 103, at 1–2.

[117] *See id.*

[118] *See* §§ 2(a)(5)–(6), 5, 7, 121 Stat. at 246. According to the Report of the House Financial Services Committee, which had jurisdiction over FINSA, the bill "improves accountability for the process within in the Administration and Congress" and "established a clear and transparent process." H.R. REP. NO. 110-24(I), at 11 (2007), *as reprinted in* 2007 U.S.C.C.A.N. 102, 104.

the United States.[119] By 2012, total Chinese FDI for the year increased to $7.6 billion, an increase of more than twenty times the amount only five years prior.[120] Annual growth in the period from 2010 to 2015 averaged thirty-two percent.[121] Even those very significant numbers, however, were dwarfed by 2016, which marked a breakout year in which Chinese FDI jumped to $45.2 billion, roughly triple that of 2015.[122]

This dramatic expansion is reflected in the number of Chinese transactions reviewed by CFIUS. For many years, the largest number of transactions filed with CFIUS was from the United Kingdom, reflecting the significant economic relationship between the two countries and high level of direct investment by U.K. companies.[123] Starting in 2012, however, Chinese acquirers filed more transactions with CFIUS than those from any other country, including the United Kingdom.[124] By 2015, CFIUS reviewed 29 transactions involving Chinese acquirers compared to 22 transactions from Canadian acquirers, 19 from U.K. acquirers, and 12 from Japanese acquirers.[125] While figures for 2016 are not currently available, it is reasonable to conclude that the significant increase in Chinese FDI corresponded to a similar increase in the number of transactions filed with CFIUS.

C. *Changing Destinations for Foreign Investment*

The sheer volume of Chinese investment is not the only factor regarding the composition of FDI in the United States that is drawing attention. Policymakers are also paying attention to the types of assets in which Chinese

---

[119] *See China Investment Monitor: Tracking Chinese Direct Investment in the U.S.*, RHODIUM GROUP, http://cim.rhg.com/interactive/china-investment-monitor (last visited Apr. 17, 2018) [https://perma.cc/MHV4-WBK2].

[120] *See id*.

[121] *See id*.

[122] *See id*.

[123] *See, e.g.*, U.S. DEP'T OF TREASURY, CFIUS ANNUAL REPORT TO CONGRESS 19 (2010), https://www.treasury.gov/resource-center/international/foreign-investment/Documents/2011%20CFIUS%20Annual%20Report%20FINAL%20PUBLIC.pdf [https://perma.cc/UL3T-UAC7] (describing the number of covered transaction by country from 2008 through 2010).

[124] *See* U.S. DEP'T OF TREASURY, CFIUS ANNUAL REPORT TO CONGRESS 17 (2012), https://www.treasury.gov/resource-center/international/foreign-investment/Documents/2013%20CFIUS%20Annual%20Report%20PUBLIC.pdf [https://perma.cc/YBE5-NW3S] (describing the number of covered transactions by country from 2010 through 2012).

[125] *See* U.S. DEP'T OF TREASURY, CFIUS ANNUAL REPORT TO CONGRESS 16–17 (2015), https://www.treasury.gov/resource-center/international/foreign-investment/Documents/Unclassified%20CFIUS%20Annual%20Report%20-%20(report%20period%20CY%202015).pdf [https://perma.cc/22NA-HNH5] (describing the number of covered transaction by country from 2013 through 2015).

firms are investing and how those investments align with China's state policies.[126] In May 2015, China announced its "Made in China 2025" plan, which provides for enormous government support to certain sectors that are seen as important to China's development over the next decade.[127] The plan sets an ambitious target of raising the domestic content of core components and materials to forty percent by 2020 and seventy percent by 2025.[128] A background paper circulated by FIRRMA's sponsors specifically refers to the Made in China 2025 Plan and notes that "China targets these industries with the goal of acquiring the know-how for its own domestic companies" and that these companies "with state support, guidance, and capital—are using their investments to generate large-scale technology transfer back to China of cutting-edge U.S. technologies."[129]

The Made in China 2025 plan expressly focuses on ten priority sectors, including artificial intelligence, advanced manufacturing and robotics, and biopharma and advanced medical products.[130] While these sectors may be principally commercial in nature, they also are sectors that the U.S. Defense Department believes may be the building blocks of the next generation of weapons systems and military technology.[131] As a result, investments by Chinese parties in these sectors of the U.S. economy may be subject to greater scrutiny from CFIUS, as a result of concerns that the investments may advance governmental as well as commercial objectives.

While investments in any of the sectors listed in the Made in China 2025 plan may draw special scrutiny, probably no sector has received more attention than the semiconductor sector. Semiconductors are the building blocks of nearly all electronics and therefore have the potential to implicate a range of national security concerns.[132] While other sectors, such as artificial intelligence and robotics, present special concerns principally because parts of the U.S. government view them as technologies that are likely to be important to future weapons systems, semiconductors are already essential to nearly every weapons

---

[126] *See, e.g.*, BACKGROUND ON FIRRMA, *supra* note 36, at 2.
[127] *See* Scott Kennedy, *Made in China 2025*, CTR. FOR STRATEGIC & INT'L STUD. (June 1, 2015), https://www.csis.org/analysis/made-china-2025 [https://perma.cc/3UB3-HTCK].
[128] *See id*.
[129] *See* BACKGROUND ON FIRMA, *supra* note 36, at 2.
[130] *See id*.
[131] *See generally* MICHAEL BROWN & PAVNEET SINGH, CHINA'S TECHNOLOGY TRANSFER STRATEGY: HOW CHINESE INVESTMENTS IN EMERGING TECHNOLOGY ENABLE A STRATEGIC COMPETITOR TO ACCESS THE CROWN JEWELS OF U.S. INNOVATION (2017), https://new.reorg-research.com/data/documents/20170928/59ccf7de70c2f.pdf [https://perma.cc/Q63P-W3YE].
[132] *See* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., EXECUTIVE OFFICE OF THE PRESIDENT, REPORT TO THE PRESIDENT: ENSURING LONG-TERM US LEADERSHIP IN SEMICONDUCTORS 2 (2017), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_ensuring_long-term_us_leadership_in_semiconductors.pdf [https://perma.cc/YWP2-P5CZ].

system and military technology.[133] Thus, semiconductors implicate not only concerns about maintaining technological leadership, but also about maintaining secure supply chains for essential semiconductors. In late 2016, at the end of the Obama Administration, the President's Council on Science and Technology issued a report titled "Ensuring Long-Term U.S. Leadership in Semiconductors."[134] The report concluded that Chinese actions in the semiconductor sector threaten U.S. national security, and that the United States should take action to counter China's moves.[135] The report notes that semiconductors are central to national security not only because they are essential to important defense systems, but also because ensuring the integrity of semiconductor components is essential to mitigating cybersecurity risks.[136] The report concluded that "Chinese industrial policies in this sector, as they are unfolding in practice, pose real threats to semiconductor innovation and U.S. national security."[137]

The focus on the semiconductor sector is not new. Indeed, as indicated above, in the 1980s it was an attempted acquisition by a Japanese company of Fairchild Semiconductor that led to the passage of the Exon-Florio amendment.[138] CFIUS has also scrutinized semiconductor transactions in recent years, especially transactions involving China.[139] For example, in 2016, acting on CFIUS's recommendation, President Obama issued an executive order prohibiting the acquisition of Aixtron, a manufacturer of semiconductor manufacturing equipment by a Chinese acquirer.[140] Then in 2017, President Trump acted on a recommendation from CFIUS to prohibit the acquisition of Lattice Semiconductor, a manufacturer of semiconductor equipment, by Chinese controlled investor Canyon Bridge.[141] Thus, while not the only example, the semiconductor sector is perhaps the most extreme example of emerging national security concerns.

---

[133] *See* BROWN & SINGH, *supra* note 131, at 7.
[134] *See generally* PRESIDENT'S COUNSEL OF ADVISORS ON SCI. AND TECH., *supra* note 132.
[135] *See id.* at 2.
[136] *See id*.
[137] *See id*. at 7.
[138] JACKSON, *supra* note 103, at 5–6.
[139] *See* COVINGTON & BURLING LLP, PRESIDENTIAL REPORT RECOMMENDS U.S. ACTION TO COUNTER CHINESE POLICIES IN THE SEMICONDUCTOR INDUSTRY 1–2 (2017), https://www.cov.com/-/media/files/corporate/publications/2017/01/presidential_report_recommends_us_action_to_counter_chinese_policies_in_the_semiconductor_industry.pdf [https://perma.cc/J6QX-7XVW].
[140] *See* Exec. Order No. 81, Fed. Reg. 88,607 (Dec. 7, 2016).
[141] *See* Exec. Order No. 82, Fed. Reg. 43,665 (Sept. 18, 2017).

D. *The "Weaponization of Investment"*

In addition to more general concerns about the volume and direction of Chinese investment, there are also more specific concerns that China is using investments to accomplish non-commercial objectives that will advance its military and intelligence capabilities. U.S. officials have made no secret of their concerns about the intent behind certain Chinese investments. According to FIRRMA's sponsors, "China is weaponizing its investment in the U.S. to exploit national security vulnerabilities, including the back-door transfer of dual-use U.S. technology and related know-how, aiding China's military modernization and weakening the U.S. defense industrial base."[142] They further conclude that "[i]n recent years, China has embarked on a campaign to systematically vacuum up advanced U.S. technology using various means, including gaming the export control system, taking advantage of universities and other research institutions, and theft through cyber and other means."[143]

The concern about Chinese investment is not limited to large, headline-grabbing deals. To the contrary, some of the investments that have caused greatest concern are small, minority investments in start-up technology companies. In February 2017, the Defense Intelligence Unit Experimental (DIUx), a component of the Department of Defense, prepared a report titled "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation."[144] The report concludes that "[t]he technologies China is investing in are the same ones that we expect will be foundational to future innovation in the U.S.: artificial intelligence, autonomous vehicles, augmented/virtual reality, robotics and blockchain technology."[145] The report further concludes that CFIUS should be reformed to "expand [the Committee's] jurisdiction to review all technology transfer transactions and restrict investments in and acquisition of critical technology companies by adversaries."[146] Notably, however, the report does not explain how such minority investments necessarily provide Chinese parties with access to the technologies of the companies in which they invest or, conversely, deny access to those same technologies to the U.S. Defense Department or other U.S. government customers.

The attention to Chinese investment and concerns about the adequacy of CFIUS are not limited to lower-level officials, but rather have received attention from multiple cabinet officials. Indeed, the senior leadership of the U.S. intelligence and defense communities appear to be in general agreement that

---

[142] *See* BACKGROUND ON FIRRMA, *supra* note 36, at 1.
[143] *Id*. at 1–2.
[144] *See generally* BROWN & SINGH, *supra* note 131.
[145] *Id*. at 2.
[146] *Id.* at 24.

concerns about Chinese investment require reform to CFIUS. Attorney General Jeff Sessions stated that CFIUS "is not able to be effective enough" and that "[FIRRMA] has great potential to push back against the abuses and dangers we face."[147] Secretary of Defense James Mattis likewise concluded that CFIUS is "outdated" and "needs to be updated to deal with today's situation."[148] Director of National Intelligence Dan Coats echoed those comments, stating that the United State should undertake "a significant review of the current CFIUS situation to bring it up to speed."[149] The White House also formally endorsed FIRRMA, issuing a public statement on January 25, 2018 that "[t]he Administration supports House and Senate passage of . . . [FIRRMA]. Modernizing [CFIUS] in line with FIRRMA would achieve the twin aims of protecting national security and preserving the longstanding United States open investment policy."[150]

While the support for CFIUS reform swelled in the first year of the Trump Administration, the concerns about the national security effects of foreign investment were also heightened at the end of the Obama Administration. As noted, it was the Obama Administration that most publicly raised concerns about Chinese investment in the semiconductor industry through the PCAS report, and CFIUS scrutiny of Chinese investment heightened significantly in 2015 and 2016 under the Obama Administration.[151] Also, FIRRMA has attracted Democratic co-sponsors, including Senator Dianne Feinstein.[152] Thus the concerns about foreign investment and desire to reform CFIUS should not be viewed as a partisan effort.

IV. Principles for Reform

Before examining the specific proposals that have been put forward to reform CFIUS, we first wish to reflect on the foundational principles that we believe should guide government national security reviews of foreign investments. Our analysis starts with the proposition that the protection of national security is the highest priority for any government, and that it is therefore

---

[147] Press Release, Office of Sen. John Cornyn, Cornyn, Feinstein, Burr Introduce Bill to Strengthen the CFIUS Review Process, Safeguard National Security (Nov. 8, 2017), https://www.cornyn.senate.gov/content/news/cornyn-feinstein-burr-introduce-bill-strengthen-cfius-review-process-safeguard-national [https://perma.cc/3KBD-FUCX] [hereinafter Cornyn Press Release].

[148] *Id*.

[149] *Id*.

[150] Press Release, White House, Statement by the Press Secretary Supporting the Foreign Investment Risk Review Modernization Act (Jan. 24, 2018), https://www.whitehouse.gov/briefings-statements/statement-press-secretary-supporting-foreign-investment-risk-review-modernization-act/ [https://perma.cc/S46S-RHPZ].

[151] *See*, COVINGTON & BURLING LLP, NEWLY-RELEASED CFIUS ANNUAL REPORT FOR 2015 FORESHADOWS HEIGHTENED SCRUTINY OF FOREIGN INVESTMENT 3 (2017), https://www.cov.com/-/media/files/corporate/publications/2017/09/newly_released_cfius_annual_report_for_2015_foreshadows_heightened_scrutiny_of_foreign_investment.pdf [https://perma.cc/W3X3-X3UL].

[152] *See* Cornyn Press Release, *supra* note 147.

appropriate to ensure that the law is sufficient to address any risk to national security presented by foreign investments.[153] Accordingly, we agree with Senator Cornyn and the other sponsors of FIRRMA that U.S. law, including CFIUS, should be modernized as necessary to ensure that the Executive Branch has the full range of authorities necessary to address any risk that arises from trade and foreign investment.[154] We further note that national security is a dynamic concept that changes as technologies and threats evolve. It is therefore appropriate for U.S. law to provide sufficient flexibility to the Executive Branch to adapt as necessary to a changing national security landscape, and for Congress from time to time to evaluate whether existing law is sufficient.

However, our analysis is also based on the proposition that the United States should simultaneously seek to advance its own economic interests, including through trade and investment. It is well established that nations' economic and national security interests are intertwined.[155] Unnecessarily restricting trade and investment would not only do economic harm to the U.S. economy, but also would have indirect adverse consequences for U.S. national security.[156] Building on that foundation, we propose the following principles to guide potential reforms to CFIUS:

> Principle 1: *Reforms should be narrowly tailored to avoid interfering with commercial activity except as necessary to protect national security*

The United States has a longstanding policy of promoting international trade and being open to foreign investment. Indeed, that policy has been a rare example of consistent bipartisan consensus for many decades.[157] That policy has

---

[153] To be clear, in this regard we refer to the *incremental* risks that arise directly from the foreign investment being contemplated; not any risks to national security that may exist separately from the proposed investment. FINSA provides that "[t]he Committee or a lead agency may, on behalf of the Committee, negotiate, enter into or impose, and enforce any agreement or condition with any party to the covered transaction in order to mitigate any threat to the national security of the United States that *arises as a result of the covered transaction*." 50 U.S.C. § 4565(*l*)(1)(A) (emphasis added).

[154] *See generally* BACKGROUND ON FIRRMA, *supra* note 36.

[155] *See generally* Steven M. Rinaldi, *Modeling and Simulating Critical Infrastructures and Their Interdependencies*, 37 HAW. INT'L CONF. ON SYS. SCI. (2004).

[156] Foreign investment can directly advance national security by, for example, providing capital to spur technological innovation or modernizing infrastructure. *See, e.g.*, ALAN P. LARSON & DAVID M. MARCHICK, FOREIGN INVESTMENT AND NATIONAL SECURITY: GETTING THE BALANCE RIGHT 22 (2006); *see also generally* U.S. CHAMBER OF COMMERCE, FROM INTERNATIONAL TO INTERSTATES: ASSESSING THE OPPORTUNITY FOR CHINESE PARTICIPATION IN U.S. INFRASTRUCTURE (2013); Matthew Slaughter & Michael Morell, *Foreign Investment Helps Boost U.S. National Security*, CIPHER BRIEF (Nov. 10, 2017), https://www.thecipherbrief.com/column_article/foreign-investment-helps-boost-u-s-national-security [https://perma.cc/DMH2-NZMT].

[157] Every recent presidential administration has explicitly stated a policy of openness to foreign investment. *See* U.S. Dep't of Treasury, Off. of Inv. Sec., Guidance Concerning the National

been under pressure from the Trump Administration, which has, for example, withdrawn the United States from negotiations regarding the Trans-Pacific Partnership and imposed tariffs on steel and aluminum, purportedly on national security grounds.[158] Even the Trump Administration, however, has acknowledged the benefits of trade and investment and their importance to U.S. national security.[159] The National Security Strategy of the United States published in December 2017 notes that "[f]or 70 years, the United States has embraced a strategy premised on the belief that leadership of a stable international economic system rooted in American principles of reciprocity, free markets, and free trade served our economic and security interests" and that "economic system continues to serve our interests, but it must be reformed."[160] In endorsing FIRRMA, the Trump Administration also re-affirmed the U.S. policy of openness to foreign investment in a public statement: "FIRRMA, by modernizing CFIUS, would strengthen our ability to protect national security and enhance confidence in our longstanding open investment policy."[161]

The existing CFIUS statute has a number of attributes that help ensure that the Committee's actions do not extend beyond those necessary to protect U.S. national security. The President may exercise his powers under the statute only where he determines that "provisions of law, other than [Section 721] and the International Emergency Economic Powers Act, do not, in the judgment of the President, provide adequate and appropriate authority for the President to protect the national security in the matter before the President."[162] This ensures that the President does not use the significant authorities of Section 721 to prohibit economic activity where other less draconian legal authorities would be sufficient to address the national security risks raised by a transaction. Further, the current statute does not extend to cover greenfield investments—meaning "start-up" investments that do not involve existing U.S. businesses—perhaps reflecting a judgment that those investments are most likely to result in economic benefits and

---

Security Review Conducted by CFIUS on Foreign Investment in the United States, 73 Fed. Reg. 74,567–68 (Dec. 8, 2008); Exec. Order No. 13,456, 73 Fed. Reg. 4677 (Jan. 25, 2008); President's Message to the Congress Transmitting the 1990 Economic Report, 26 WEEKLY COMP. PRES. DOC. 180, 183 (Feb. 6, 1990); Statement by President Ronald Reagan on International Investment Policy, 19 WEEKLY COMP. PRES. DOC. 1214, 1216 (Sept. 9, 1983).

[158] *See* Peter Baker, *Trump Abandons Trans-Pacific Partnership, Obama's Signature Trade Deal*, N.Y. TIMES (Jan. 23, 2017), https://www.nytimes.com/2017/01/23/us/politics/tpp-trump-trade-nafta.html; *Trump Formally Orders Tariffs on Steel, Aluminum Imports*, NAT'L PUB. RADIO (Mar. 8, 2018), https://www.npr.org/2018/03/08/591744195/trump-expected-to-formally-order-tariffs-on-steel-aluminum-imports.

[159] White House, *supra* note 150.

[160] WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE UNITED STATES 17 (Dec. 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [https://perma.cc/F85X-VVLT].

[161] White House, *supra* note 150.

[162] 50 U.S.C. § 4565(d)(4)(B).

least likely to present national security risks that cannot be addressed through other authorities.[163]

In our view, any reforms to CFIUS should maintain similar protections to ensure that the authorities that Congress assigns to the Executive Branch may be used only as necessary to protect U.S. national security. This principle is consistent with the idea of "regulatory proportionality" advanced by guidelines issued by the Organization for Economic Cooperation and Development (OECD Guidelines), which suggest that with respect to national security investment policies, "[r]estrictions on investment, or conditions on transaction, should not be greater than needed to protect national security and they should be avoided when other existing measures are adequate and appropriate to address a national security concern."[164]

Principle 2: *National security considerations should be addressed separately from economic considerations*

Over the years, there have been a number of proposals put forth that would have CFIUS consider economic factors, such as whether a transaction would present a "net benefit" to the United States, or result in job losses.[165] There have also been proposals to create new review authorities, apart from CFIUS, that would have the authority to restrict foreign investment based on similar economic factors. Most recently, certain Democrats, including Senator Schumer, the Senate minority leader, proposed an "American Jobs Security Council" that could prohibit transactions based on jobs concerns. While an analysis of those types of separate review mechanisms is outside the scope of this Article, we believe that it would be a mistake to add economic considerations to CFIUS's remit or otherwise combine economic considerations with national security considerations as part of one review process. Doing so would either impair CFIUS's ability to perform its national security function or create a review process that is unaccountable and easily politicized.

In any regulatory process, there are competing arguments for transparency versus secrecy. Transparency advances political accountability and also helps ensure that the regulatory body is relying on the best possible information in making determinations. Secrecy may be necessary to ensure the protection of confidential or sensitive information, and to insulate the regulatory body from

---

[163] *See* 31 C.F.R. § 800.301 (noting that a greenfield investment is not a covered transaction).

[164] ORG. FOR ECON. COOPERATION AND DEV., OECD GUIDELINES FOR RECIPIENT COUNTRY INVESTMENT POLICIES RELATING TO NATIONAL SECURITY (2008), https://www.oecd.org/daf/inv/investment-policy/41807723.pdf [https://perma.cc/H7CW-XWZ4].

[165] *See, e.g.*, Press Release, Office of Rep. Rosa DeLauro, DeLauro Reintroduces the Foreign Investment and Economic Security Act (June 15, 2017), https://delauro.house.gov/media-center/press-releases/delauro-reintroduces-foreign-investment-and-economic-security-act [https://perma.cc/G2AE-UCHL].

undue political pressure. The appropriate balance between the competing considerations, however, is entirely different in an economic review as opposed to a national security review. In a national security review, the balance of these factors weighs more heavily in favor of secrecy, whereas in an economic review the emphasis should be on transparency.

The CFIUS process was designed from the ground up to be a national security review.[166] For that reason, CFIUS operates very differently from most other regulatory processes. Most notably, the Committee deliberates in secret, relies extensively on classified information that is not released to the parties, and is required by law to provide confidential treatment to all information received by parties in connection with CFIUS reviews (and not just specific categories of confidential information), subject even to potential criminal penalties for unauthorized release of such information.[167] These aspects of the Committee's operations ensure that CFIUS has the best information available to assess any national security risks because it can consider the full range of classified information available to the government, and also because parties may provide information to the Committee without fear of public disclosure.[168] In addition, CFIUS is not obligated to follow its own precedents, and decisions of the President made pursuant to Section 721 are not subject to CFIUS review.[169]

These unusual procedures, while appropriate in the context of a national security review, are entirely inappropriate for a review process focused on economic factors. In a review focused on economic factors there would be little or no need for the government to rely principally or even significantly on classified information. Nor would there be any need for the review to operate in secret (except to the limited extent necessary to protect proprietary or confidential business information submitted). To the contrary, there would be strong public policy reasons to have any foreign investment review focused on economic factors to maintain a high level of transparency to guard against the risk that decisions are subject to undue political influence. Likewise, there would be strong public policy reasons for an economic review process to follow precedent and be subject to judicial review, in order to promote transparency, predictability, and fairness.

---

[166] JACKSON, *supra* note 103, at 1.
[167] *Id*. at 19.
[168] 50 U.S.C. § 4565(c).
[169] *Id.*

Principle 3: *To the extent consistent with the requirements of national security, CFIUS should provide legal certainty to U.S. businesses and foreign investors*

It is important to bear in mind that CFIUS serves multiple policy purposes. First and foremost, of course, the process permits the U.S. government to address national security risks arising from transactions.[170] But equally important, it encourages foreign investment by providing investors with legal certainty that comes with a CFIUS approval.[171] We agree in this respect with the OECD Guidelines, which provide that "regulatory objectives and practices should be made as transparent as possible so as to increase the predictability of outcomes."[172] Thus, existing law provides that if parties voluntarily notify their transaction to CFIUS and receive approval, the U.S. government will not later come and seek to unwind or frustrate their transaction (except in very narrow circumstances).[173] Without CFIUS, investors may be deterred from undertaking acquisitions of potentially sensitive companies because they would not know whether the U.S. government may at some time in the future seek to take action to protect U.S. national security in a manner that would impair their commercial interest.[174] Any reforms to CFIUS should ensure the protection of the safe harbor that CFIUS affords to investors and encourage parties to voluntarily notify the Committee of transactions.

Principle 4: *Prohibiting a transaction should be a last resort; CFIUS should lean in favor of addressing identified risks through mitigation*

Congress did not provide CFIUS with the authority to prohibit a transaction; only the President has that authority.[175] Existing law does, however, provide CFIUS the authority to enter into mitigation agreements with parties to address national security risks associated with transactions.[176] These agreements provide CFIUS the authority to address national security risks arising from a proposed transaction without resorting to prohibiting the transaction outright. These agreements may include, for example, excluding sensitive assets from the

---

[170] *Id.* § 4565(b)(1)(A)(i).
[171] The President or CFIUS may only initiate a review of a transaction that has previously been reviewed or investigated if (1) a party submitted false or misleading material information to the Committee or made a material omission, or (2) a party intentionally breached a mitigation agreement or condition imposed by CFIUS, and CFIUS determined that there are no other remedies of enforcement tools to address the breach. *Id.* § 4565(b)(1)(d).
[172] ORG. FOR ECON. COOPERATION AND DEV., *supra* note 164, at 1.
[173] *Id.*
[174] *See* LARSON & MARCHICK, *supra* note 156, at 11.
[175] *See* 50 U.S.C. § 4565(d); *see also* Wakely & Windsor, *supra* note 22, at 107.
[176] *See* Wakely & Windsor, *supra* note 22, at 111.

scope of a transaction, limiting access to certain locations or information, and enhancing data security measures.[177]

Congress reserved the power to prohibit a transaction to the President and afforded CFIUS the lesser authority to enter into mitigation agreements. This decision reflects a judgment that prohibiting a transaction is the last resort to be used when there is no other option to address the national security risk arising from a transaction.[178] Indeed, the Report of the House Financial Services Committee, which had jurisdiction over FINSA, states that "[t]he Committee believes that mitigation agreements play a critical role in the CFIUS process, allowing CFIUS to fully address security concerns *without resorting to an outright rejection of the transaction when concerns arise*."[179] The report further provides that "[t]hese agreements are intended to mitigate the possible national security threats posed by a transaction *short of requiring that the parties abandon the transaction altogether*."[180] This intent is consistent with the OECD Guidelines, which suggest that, "[i]f used at all, restrictive investment measures should be tailored to the specific risks posed by specific investment proposals . . . . This would include providing for policy measures (especially risk mitigation agreements) that address security concerns, but fall short of blocking investments."[181]

To be sure, some transactions will present risks so great that they cannot be resolved through mitigation,[182] and in that case the Executive Branch should have the authority to prohibit the transaction. But in all other instances the law should be designed to permit and encourage CFIUS to address risks through mitigation.

Principle 5: *CFIUS should be limited to addressing risks that arise from foreign control of U.S. businesses*

As described in Part I above, existing law provides a broad range of authorities for the Executive Branch to address national security risks that arise from trade and investment.[183] Within that framework, CFIUS has been designed to address the risks that may arise from FDI, and specifically investments that

---

[177] *See On Foreign Investment, Jobs and National Security: The CFIUS Process: Hearing Before H. Fin. Servs. Comm.*, 109th Cong. 5 (2006) (statement of David Marchick, Partner, Covington & Burling LLP).
[178] *See* Wakely & Windsor, *supra* note 22, at 111.
[179] H.R. REP. NO. 110-24(I), at 16 (2007), *as reprinted in* 2007 U.S.C.C.A.N. 102, 104.
[180] *Id.* at 11 (emphasis added).
[181] ORG. FOR ECON. COOPERATION AND DEV., *supra* note 164, at 1.
[182] To use an extreme case as an example, it is difficult to conceive of how the national security risks presented by an acquisition of a U.S. defense contractor by an investor from a country hostile to the United States could be mitigated.
[183] *See supra* Part I.

may result in control of U.S. businesses.[184] Importantly, this definition of "control" is extremely broad, and has been used by CFIUS to review, for example, transactions that provide the foreign investor as little as 9.9% equity interest in a U.S. business together with a right to appoint an observer to the company's board of directors.[185]

Despite this broad definition of "control" there have been proposals (including FIRRMA) that would expand the Committee's jurisdiction to address other business activities or transactions that do not confer control of U.S. businesses to foreign persons.[186] As described further in Part V, below, FIRRMA as introduced would expand CFIUS's jurisdiction for the first time to review certain *outbound* transactions of intellectual property from U.S. businesses to foreign persons.[187] The fact that CFIUS has broad authorities, including the authority to recommend that the President prohibit a transaction, makes CFIUS an attractive vehicle to address perceived national security risks, including risks that do not relate to transactions resulting in foreign control of U.S. businesses.[188]

While we agree with the sponsors of FIRRMA that it is appropriate to ensure CFIUS's authorities are sufficient to address the full range of national security risks,[189] it is also important to recognize that CFIUS is only one of the many authorities available to the executive branch to address national security risks, as described fully in Part I. In deciding whether to expand CFIUS's jurisdiction, Congress should not only ask whether there is a risk to national security that is not addressed by existing law, but also whether CFIUS is the appropriate legal authority to address that risk, as opposed to the export control laws or other mechanisms. In our view, CFIUS should remain focused on risks arising from transactions that result in foreign control of U.S. businesses; other risks should be addressed through other authorities.

---

[184] Section 721 of the Defense Production Act of 1950 authorizes the President to review mergers, acquisitions, and takeovers by or with any foreign person which could result in foreign control of any person engaged in interstate commerce in the United States, to determine the effects of such transactions on the national security of the United States. 50 U.S.C. § 4565 (1950).

[185] Indeed, we have represented parties in transactions where CFIUS asserted jurisdiction on these facts.

[186] For example, as described in Part I, FIRRMA would permit CFIUS to review certain contributions of intellectual property from U.S. businesses to foreign persons.

[187] *See generally* Foreign Investment Risk Review Modernization Act (FIRRMA) of 2017, S. 2098, 115th Cong. (2017).

[188] *See* LARSON & MARCHICK, *supra* note 156, at 1–4.

[189] *See* BACKGROUND ON FIRRMA, *supra* note 36, at 1.

Principle 6: *CFIUS should work collaboratively with allies to address risks that cross borders, not seek to assert jurisdiction over matters outside the United States*

In an era of multinational companies and globalized supply chains, there is no question that national security risks may cross borders.[190] For example, the acquisition of a U.K. defense company by a company headquartered in a country hostile to the United States could present risks to U.S. national security given the close cooperation with the United Kingdom on defense matters, even if the U.K. company has no business in the United States, by giving the hostile country access to allied military technology. Likewise, as noted above, U.S. officials have expressed significant concerns about China closing the technology gap with the United States in key security-related areas.[191] But those technologies do not exist solely in the United States.[192] They may be developed, for example, in Germany, Japan, South Korea, the United Kingdom, or any other country for that matter.[193] For policymakers who view the United States as being in a zero-sum competition with China for technological pre-eminence, any gain by China (including any gain resulting from investment in the businesses of a third country) may present a risk to U.S. national security by providing China with technology that could be used against the United States.

Under existing law, CFIUS regulations define a "U.S. business" as an "entity . . . engaged in interstate commerce in the United States, *but only to the extent of its activities in interstate commerce*."[194] Thus, for example, President Obama had the authority to prohibit a foreign person from acquiring "[t]he U.S. business of Aixtron" but had no authority to prohibit the acquisition of Aixtron's business and assets outside the United States.[195] The question then, is whether CFIUS could (or should) seek to review and act with regard to wholly foreign

---

[190] *See generally*, U.S. CHAMBER OF COMMERCE, PREVENTING DEGLOBALIZATION: AN ECONOMIC AND SECURITY ARGUMENT FOR FREE TRADE AND INVESTMENT IN ICT (2016) https://www.uschamber.com/report/preventing-deglobalization-economic-and-security-argument-free-trade-and-investment-ict [https://perma.cc/Z3GV-P6QZ] [hereinafter PREVENTING DEGLOBALIZATION].

[191] NAT'L SCI. BD., SCIENCE AND ENGINEERING INDICATORS 3 (2018), https://www.nsf.gov/statistics/2018/nsb20181/assets/nsb20181.pdf [https://perma.cc/H99G-7YHX].

[192] For example, in 2016, only eight of the top twenty semiconductor companies worldwide were headquartered in the United States. Three are headquartered in Japan, three in Taiwan, two in South Korea, and one in Singapore. *Top 20 Semiconductor Companies 2016*, ANYSILICON (May 23, 2016), http://anysilicon.com/top-20-semiconductor-companies-2016/ [https://perma.cc/D3Z6-8VBW].

[193] *Id*.

[194] 31 C.F.R. § 800.226 (emphasis added).

[195] Regarding the Proposed Acquisition of a Controlling Interest in Aixtron SE by Grand Chip Investment GmbH, Exec. Order, 81 Fed. Reg. 88,607 (Dec. 7, 2016).

transactions in the way that some other U.S. statutory regimes permit extraterritorial jurisdiction.[196]

In our view, expanding CFIUS in that manner would be a mistake. Seeking to assert extraterritorial jurisdiction may encourage other countries to try to impose their own extraterritorial restrictions. For example, could China seek to prohibit acquisitions by U.S. companies of Japanese or Korean companies that also do business in China, perhaps even denying access to the Chinese market as a coercive tool? Instead, the U.S. government should work with allies to address any risks that are presented by transactions outside the United States, including by encouraging ally countries to establish their own foreign investment review processes akin to CFIUS.

V. Evaluating the Proposals

A. *FIRRMA*

In many respects FIRRMA is consistent with the principles described above. Most important, Senator Cornyn and the other sponsors of FIRRMA have sought to keep the bill "laser focused on national security" and have not strayed into consideration of economic factors.[197] In other respects, though, FIRRMA as introduced departs from our recommended principles. While a number of changes have been made to FIRRMA since its introduction including through the committee-mark-up process, and more changes may be made in the future, this section evaluates the bill as originally introduced.

First, FIRRMA would expand CFIUS's jurisdiction to review a broad range of business relationships that do not result in control of a U.S. business. Most significantly, FIRRMA would expand CFIUS's jurisdiction to review "[t]he contribution (other than through an ordinary customer relationship) by a United States critical technology company of both intellectual property and associated support to a foreign person through any type of arrangement, such as a joint venture."[198] This provision would, for the first time, depart from CFIUS's exclusive focus on reviewing inbound foreign investment, and expand its remit to include *outbound* contributions of certain intellectual property by U.S. businesses. In that sense, CFIUS's jurisdiction would overlap with (and perhaps duplicate) the export control regimes described in Part I, above. Thus, if FIRRMA were enacted, it is conceivable that CFIUS could review and prohibit the contribution of a technology that is not controlled for export purposes pursuant to the ITAR or

---

[196] *See generally* Anthony J. Colangelo, *What is Extraterritorial Jurisdiction?*, 99 CORNELL L. REV. 1303 (2014).
[197] *See* BACKGROUND ON FIRRMA, *supra* note 36, at 1.
[198] S. 2098, 115th Cong. (2017) § 3(a)(5)(B)(v).

EAR. This would lead to significant uncertainty for businesses, which must make decisions based on expectations about whether technologies will be exportable.

In addition, FIRRMA would expand CFIUS's jurisdiction for the first time to include certain real estate transactions that do not involve the acquisition of control of U.S. businesses, departing from CFIUS's traditional exclusion of "greenfield" investments. Specifically, CFIUS would have the authority to review "[t]he purchase or lease by a foreign person of private or public real estate that . . . is located in the United States and is in close proximity to a United States military installation or to another facility or property of the United States Government that is sensitive for reasons relating to national security."[199] Under existing law, CFIUS can review real estate transactions that result in control of a U.S. business, such as the acquisition of a commercial office building, but cannot review the purchase of vacant real estate because it does not constitute a "U.S. business" under the CFIUS regulations.[200] This would represent a vast expansion of CFIUS's jurisdiction, potentially requiring the Committee to expend unnecessary resources reviewing thousands of non-sensitive transactions.

Second, FIRRMA would reduce the legal certainty and transparency associated with CFIUS reviews by (1) reducing the effectiveness of a legal safe harbor that a CFIUS approval provides, and (2) insulating the Committee's actions from judicial review. As explained above, the benefit of filing a transaction with CFIUS is that once an approval is received, CFIUS or the President cannot later disturb the transaction, except on narrow grounds, such as if a party provided materially false information to CFIUS or intentionally and materially breaches a mitigation agreement. FIRRMA would remove the requirement that a breach be intentional. Instead CFIUS would be permitted to re-open its review of the transaction, and potentially refer the matter to the President for a divestiture or other action, if CFIUS, in its sole discretion, determines that there has been a material breach of the mitigation agreement, regardless of whether such breach was intentional.[201] This change would diminish the certainty to investors ensured by the legal safe harbor of CFIUS approval.

Further limiting the safe harbor assurance, FIRRMA would largely exempt CFIUS action from judicial review. Actions of the President pursuant to Section 721 are not currently subject to judicial review, but actions by CFIUS are, including on due process grounds. Indeed, in the only decision of a U.S. Court of Appeals regarding a CFIUS matter, the D.C. Circuit found that CFIUS had failed to provide constitutionally adequate process to a Chinese investor. FIRRMA would significantly expand the exemption from judicial review, and provide that

---

[199] *Id.* § 3(a)(5)(B)(ii)(I).
[200] *See* 31 C.F.R. § 800.226 (defining "U.S. business" as "any entity, irrespective of the nationality of the persons that control it, engaged in interstate commerce in the United States").
[201] S. 2098, § 16(4)(D).

"the actions and findings of the Committee . . . and any assessment of penalties or use of enforcement authorities under this section, shall not be subject to judicial review."[202] This exemption includes claims brought under the Administrative Procedures Act,[203] but provides for a narrow right to petition for a "violation of a constitutional right, power, privilege, or immunity."[204] While litigation concerning CFIUS has been very limited, the fact that the Committee's actions may be subject to review incentivizes the Committee to act in a manner that comports with due process and is not arbitrary or capricious, in order to avoid being hauled into court. Removing the prospect of judicial review would remove one incentive for a Committee that already acts in secret to maintain high standards of fairness.

B. *ECRA*

On February 15, 2018, House Foreign Affairs Committee Chairman Ed Royce introduced the Export Control Reform Act of 2018 (ECRA) to modernize the United States' export control regulation of commercial and dual-use items.[205] The proposed legislation seeks to establish a permanent statutory basis for export controls (currently enacted pursuant to IEEPA[206]), and to provide an alternative to some aspects of FIRRMA, such as FIRRMA's expansion of CFIUS jurisdiction to cover certain outbound transfers of technology.[207] As Congressman Royce emphasized when introducing the bill, much of the motivation behind ECRA is to protect critical and emerging technologies, which some critics argue are not sufficiently captured by either CFIUS or the EAR.[208]

In addition to establishing a permanent legal basis for export regulation, ECRA would significantly expand U.S. export control jurisdiction. For example, ECRA would extend U.S. jurisdiction to any "commodity, software, or technology,"[209] regardless of whether the item is within the United States, of U.S. origin, composed of U.S. content, or even a direct product of U.S. technology.[210] ECRA's jurisdictional reach would also extend to technology transfers to

---

[202] *Id.* § 14(2)(A).
[203] *Id.*
[204] *Id.* § 14(2)(B)(ii)(I).
[205] Press Release, House Foreign Aff. Comm., Royce Introduces Bipartisan Export Control Reform Bill (Feb. 15, 2018), https://foreignaffairs.house.gov/press-release/royce-introduces-bipartisan-export-control-reform-bill [https://perma.cc/5D7N-45HW].
[206] *See supra* notes 46–47 and accompanying text.
[207] *See supra* note 198 and accompanying text.
[208] *See supra* notes 94–102 and accompanying text; Press Release, House Foreign Aff. Comm., *supra* note 205.
[209] Export Control Reform Act of 2018, H.R. 5040, 115th Cong. (2018) § 115(b)(2)(A), https://foreignaffairs.house.gov/wp-content/uploads/2018/02/hr-5040.pdf [https://perma.cc/TY6H-KSMR].
[210] *Id.* § 2(6).

companies in the United States that are majority owned by foreign entities.[211] Under the proposed legislation, transfers to these entities would be "deemed" an export in the same way as transfers to non-U.S. natural persons.[212] Finally, ECRA would expand export control jurisdiction to the earliest stages of technological development, such as "foundational information" and technological "know-how."[213] To implement this final element, ECRA would require the President to establish a regular interagency process to identify emerging and critical technologies.[214]

Although ECRA would significantly impact the landscape of U.S. export controls, the legislation is largely consistent with the six principles we have discussed. Enhanced export controls may be less likely to adversely impact commercial investment or conflate national security concerns with economic priorities. Additionally, the forward-looking nature of export controls typically provides a reasonable degree of certainty regarding what information and technology is subject to regulation. Although ECRA addresses only some of the weaknesses that FIRRMA seeks to resolve, it does so without several of the adverse consequences that may result from an expansion of CFIUS's jurisdiction.

C. *USFIR*

Senators Chuck Grassley and Sherrod Brown offered a third alternative to CFIUS reform when they introduced the United States Foreign Investment Review Act (USFIR) on October 18, 2017.[215] USFIR would not reform CFIUS, but would implement an independent regulatory process to determine "the economic effect" of certain foreign investments in the United States.[216] A press release by Senator Grassley's office stated that the proposed legislation is necessary because "[n]o current mechanism allows the U.S. government to evaluate foreign investment for its long-term economic benefit to the U.S."[217] The

---

[211] *Id.* §2(12)(B).

[212] *Id.* § 2(3) (defining "export" to include "the release or transfer or technology or source code relating to the item to a foreign person in the United States"); *cf.* 15 C.F.R. § 730.5(c) (2018) (describing deemed exports under the EAR).

[213] H.R. 5040, § 2(9)(A)(ii).

[214] *Id.* at § 109 ("The President shall . . . establish and . . . lead a regular, ongoing interagency process to identify emerging critical technologies that are not identified in any list of items controlled for export under United States law or regulations, but that nonetheless could be essential for maintaining or increasing the technological advantage of the United States over countries that pose a significant threat to the national security of the United States . . . .").

[215] Press Release, Office of Sen. Chuck Grassley, Grassley, Brown Introduce Bipartisan Bill to Make Sure Foreign Investments Don't Hurt U.S. Economy, Jobs (Oct. 18, 2017), https://www.grassley.senate.gov/news/news-releases/grassley-brown-introduce-bipartisan-bill-make-sure-foreign-investments-don%E2%80%99t-hurt [https://perma.cc/4PER-643C].

[216] *See* United States Foreign Investment Review Act of 2017, S. 1983, 115th Cong. (2017) § 1002.

[217] Press Release, Office of Sen. Chuck Grassley, *supra* note 215.

press release further states that such a review is necessary because "[r]ecent patterns of foreign investment in the U.S. have raised concerns that overseas competitors, including state-owned enterprises, are pursuing investments to make strategic gains in the U.S. market or to benefit their own domestic industries."[218]

In order "to determine the economic effect of the transaction on the United States," USFIR would mandate filing for (1) any "transaction involving a state-owned enterprise" that could result in foreign control of a U.S. business valued at $50 million or more; or (2) any transaction that could result in foreign control of a U.S. business valued at or above $1 billion.[219] Upon receiving notice of the transaction, the Secretary of Commerce would have 15 days to either approve the transaction or inform the parties that the Secretary requires more time to review its economic impact. No more than 45 days after the end of the 15-day period, the Secretary would be required to approve, prohibit, or request modification of the transaction.[220] Decisions by the Secretary would be public, and there would be a period of public comment of not more than ten days for transactions that proceed to the additional 45-day review period.[221]

In making determinations, the Secretary would be required to consider a variety of factors, including the long-term strategic economic interests of the United States, the history of distortive trade practices within the foreign entity's country of domicile, the nature of the foreign ownership, and the impact on the domestic industry.[222]

Because USFIR would create a separate regulatory process outside CFIUS, it would not implicate the concerns identified in Principle 2, above. However, USFIR would conflict with Principle 1, the idea that reforms should minimize interference with commercial activity only to the extent necessary to protect national security. As described above, the United States has long maintained a policy of open investment, and the benefits of regulatory proportionality are well accepted.[223] By further regulating—and potentially prohibiting—numerous investments for causes unrelated to national security, USFIR would likely discourage foreign investment and inhibit U.S. economic growth.

---

[218] *Id.*
[219] *See* S. 1983, § 1001(2)(b).
[220] *Id.* § 1002(c)(2).
[221] *Id.* § 1002(c).
[222] *Id.* § 1002(d).
[223] ORG. FOR ECON. COOPERATION AND DEV., *supra* note 164, at 1.

D. *FIESA*

A fourth alternative approach is set forth in the Foreign Investment and Economic Security Act (FIESA), introduced by Representative Rosa DeLauro in the House of Representatives on July 7, 2016.[224] Modeled after the Investment Canada Act[225] and similar to USFIR, the bill sought to make two key changes to the CFIUS process. First, like FIRRMA, it would have expanded CFIUS's jurisdiction to cover not only mergers and acquisitions, but also greenfield investments—"any construction of a new facility in the United States by a foreign person."[226] Second, FIESA would have amended Section 721 of the Defense Production Act of 1950 by requiring CFIUS to consider the "net benefit" of the proposed transaction from an economic perspective if the transaction would also need to be filed under the Hart-Scott-Rodino Antitrust Improvements Act (HSR).[227] To assess economic "net benefit"—defined as "the effect on the level of economic activity in the United States"—the bill would have required CFIUS to consider several new factors, including whether the transaction would impact the level and quality of employment, the use of parts or services produced within the United States, and U.S. exports.[228] Review of these economic considerations would be led by a separate committee within CFIUS, which would include the Secretaries of Commerce, Labor, and Treasury, as well as the Attorney General and the U.S. Trade Representative.[229]

FIESA has gained no traction in Congress,[230] and in our view should not. It is directly contrary to Principle 2, discussed above: that national security considerations should be addressed separately from economic considerations. Inclusion of a "net benefit" test would be inconsistent with the United States' open investment policy and undermine the effectiveness of CFIUS.[231] When reviewing transactions, CFIUS operates with substantial discretion, evaluating a variety of national security risks based on an interagency assessment of sensitive and classified information. This model is simply not well suited to consider

---

[224] *See* H.R. 5665, 114th Cong. (2016), https://www.congress.gov/bill/114th-congress/house-bill/5665/text [https://perma.cc/S6HN-C375]. A nearly identical version of this bill was introduced by Representative DeLauro on September 18, 2014. *See* H.R. 5581, 113th Cong. (2014). Neither bill acquired significant support in Congress.

[225] *See generally* Investment Canada Act, R.S.C. 1985, c 28.

[226] H.R. 5665, § 2(3).

[227] *Id.* § 3. The HSR is codified at Section 7A(a) of the Clayton Act, 15 U.S.C. § 18a(a) (2016).

[228] H.R. 5665, § 3(a)(2)(o).

[229] *See id.* § 3(6).

[230] *All Actions H.R. 2932—115th Congress (2017-2018)*, CONGRESS.GOV, https://www.congress.gov/bill/115th-congress/house-bill/2932/all-actions?overview=closed#tabs (last visited Apr. 12, 2018) [https://perma.cc/9WJS-7P9A].

[231] *See supra* text accompanying notes 165–169.

economic impact, which should be subject to open and transparent discussions about competing political priorities.[232]

VI. Recommendations for CFIUS Reforms

While we believe the recent proposals to reform CFIUS raise a number of concerns, we do believe there are other reforms that could be made to CFIUS that are consistent with the principles described above and that would enhance the Committee's ability to protect the national security of the United States while encouraging and indeed facilitating foreign direct investment.

A. *Clarify the definition of "passive" investments that are not subject to CFIUS jurisdiction and make clear that the United States particularly welcomes passive investments, including from China*

By definition, truly passive investments should, except in unusual cases, raise no national security concerns. By "passive investment," we mean any investment that gives the foreign investor no *de jure* or *de facto* capacity to control, direct, or decide any matters of the U.S. business. In that sense, passive investments are similar to acquisitions of small blocks of shares on the open market: they provide the investor with a financial return on their investment, but no meaningful ability to influence any decision of the company. In that sense, we believe that passive investments by foreign parties should presumptively be viewed as beneficial to the United States: they add to the U.S. economy by bringing in foreign capital to support U.S. businesses while not resulting in any foreign control over those businesses.

In part for those reasons, passive investments, like greenfield investments, are excluded from CFIUS's jurisdiction.[233] Both types of investment benefit the U.S. economically and are unlikely to present national security risks that cannot be addressed through other legal authorities.[234] Indeed, FIRRMA recognizes the value of passive investments; the draft bill notes that "foreign investment provides substantial benefits to the United States . . . especially when those investments are truly passive in nature."[235] For that reason, we believe U.S. law should encourage passive investments by exempting them from CFIUS review, and providing clarity to investors as to what exactly constitutes a passive investment.

---

[232] *See id.*

[233] *See* 31 C.F.R. § 800.302(b).

[234] Greenfield investments are less likely to raise national security concerns for a number of reasons, including because there are no pre-existing contracts or other relationships with U.S. government customers and other customers that may be sensitive from a national security perspective and no pre-existing technology that could be sensitive that could not otherwise be readily acquired.

[235] S. 2098, 115th Cong. § 2(1) (2017).

While current law does exempt passive investments from CFIUS's jurisdiction (as would FIRRMA), the standard for what is a "passive investment," is less than clear.[236] Under existing regulations, "[a] transaction that results in a foreign person holding ten percent or less of the outstanding voting interest in a U.S. business" is not a covered transaction, but only if the transaction is "solely for the purpose of passive investment."[237] The regulations further provide that "[o]wnership interests are held or acquired *solely for the purpose of passive investment* if the person holding or acquiring such interests does not plan or intend to exercise control, does not possess or develop any purpose other than passive investment, and does not take any action inconsistent with holding or acquiring such interests solely for the purpose of passive investment."[238] These standards are at best vague. Indeed, they do not actually define what "passive" means. This vagueness creates confusion for investors, including with regard to what transactions need to be notified to CFIUS.[239] As a result, some transactions that should be notified likely are not, and, conversely, CFIUS is required to expend resources to review transactions that are in fact passive.[240] This lack of clarity has been exacerbated by the fact that CFIUS's interpretation has tended to evolve over time, and has tended to change depending on the facts of the case before the Committee.[241]

---

[236] LATHAM & WATKINS LLP, OVERVIEW OF THE CFIUS PROCESS 2 (2017) ("While [the passive investment] formulation appears straightforward, a closer read reveals that the 'passive' nature of the investment can be called into question in light of 'other' facts deemed relevant by CFIUS—*e.g.*, contractual or other arrangements between the foreign investor and the target.").

[237] *Id*. § 800.302(b).

[238] 31 C.F.R. § 800.223 (emphasis in original).

[239] For example, is an acquisition of a five percent equity interest in a U.S. business where the foreign person has rights to non-public financial information of the business but no other special rights "solely for the purpose of passive investment"? What about a foreign party who acquires seven percent of the membership interests in an investment fund structured as a limited partnership, and obtains the right to participate in a limited partner advisory committee that can advise the U.S. general partner? Both of these fact patterns fall into a gray area under existing law.

[240] Because CFIUS is a voluntary filing process, parties must weigh the costs and benefits of filing versus not filing. Where the law is vague on the types of transactions that are and are not subject to CFIUS jurisdiction, it is inevitable that cautious parties will file some transactions that CFIUS determines are not covered transactions and, conversely, other parties will choose not to file transactions that CFIUS would determine to be covered transactions that should be reviewed.

[241] The vagueness inherent in the statute and regulations, combined with the fact that CFIUS is not legally obligated to follow its own precedents, permits CFIUS to make policy judgments about the types of transactions that it reviews. For example, CFIUS could determine that 15 percent investment in an ice cream factory is not a covered transaction, but that a five percent investment by the same party and on the same terms in a defense contractor is a covered transaction. It is also our experience, based on representing parties before CFIUS, that the Committee in recent years has become more aggressive in asserting jurisdiction over minority investments. *See* COVINGTON & BURLING, LLP, CFIUS REFORM LEGISLATION INTRODUCED IN CONGRESS 1 (2017), https://www.cov.com/-/media/files/corporate/publications/2017/11/cfius_reform_legislation_introduced_in_congress.pdf (noting that FIRRMA would "codify existing practices of CFIUS that have evolved recently").

FIRRMA seeks to clarify the definition of "passive investment"[242] and, in that sense, we agree with the bill's sponsors. Under FIRRMA, a passive investment would be one that does not provide the foreign person with:

1. access to any nonpublic technical information in the possession of the United States business;[243]
2. access to any nontechnical information in the possession of the United States business that is not available to all investors;[244]
3. membership or observer rights on the board of directors or equivalent governing body of the United States business or the right to nominate an individual to such a position; or[245]
4. any involvement, other than through voting of shares, in substantive decisionmaking pertaining to any matter involving the United States business;[246]

and "under which the foreign person and the United States business do not have a parallel strategic partnership or other material financial relationship."[247] While some aspects of this definition add clarity, others have the potential to introduce even more confusion. What is "technical information"? What is a "parallel strategic relationship" or a "material financial relationship"? The definition of passive investment should be clarified to define what these terms mean in a manner that is appropriately scoped to permit CFIUS to review transactions that conceivably could present national security risks while not overwhelming the Committee with notices of transactions that are not relevant to national security.

The definition of "passive" investment should also be defined in reference to common types of investments so as to provide greater clarity to transaction parties. For example, the following are other examples of investments that are "passive" under our definition, but not addressed in current law:

- purchases of securities on the open market that provide the acquirer with no input into any decisionmaking of the U.S. business;
- acquisitions of interests in mutual funds, exchange-traded funds, index funds, and other types of funds in which the acquirer has no control over the investment selections of the fund or operations of the investments;
- investments in funds organized by U.S. general partners that do not afford the foreign person any ability to control the funds; and

---

[242] S. 2098, 115th Cong. § 3(D) (2017).
[243] *Id*. § 3 (a)(5)(D)(i)(II)(aa).
[244] *Id*. § 3 (a)(5)(D)(i)(II)(bb).
[245] *Id*. § 3 (a)(5)(D)(i)(II)(cc).
[246] *Id*. § 3 (a)(5)(D)(i)(II)(dd).
[247] *Id*. § 3 (a)(5)(D)(i)(III).

- acquisitions of limited partnership interests that provide the foreign person no ability to influence the decisions of a U.S. general partner.

The latter two points are especially relevant in the context of venture funds, which are typically organized as limited partnerships.[248] In this structure, the general partner generally controls all important decisions, and the limited partners are passive investors in the funds with limited rights, if any.[249] If CFIUS were to review every acquisition or investment by a U.S. private equity fund in which there is one or more foreign limited partners, it would quickly overwhelm the Committee with transactions that are likely to present no national security risks because the foreign limited partners exercise no control over the fund, which is instead fully under the control of the U.S. general partner.[250] Instead, U.S. law should encourage passive investments, including in funds structured as limited partnerships, by clarifying that such investments do not make the funds "foreign persons" for CFIUS purposes, provided that the limited partners have no rights to direct the general partner with respect to the U.S. assets owned by the fund. To be sure, this principle should not extend to fund structures where foreign limited partners in fact have any *de jure* ability to control the general partner (or the U.S. business owned by the fund), or where CFIUS determines conclusively that the foreign party has any *de facto* ability to control the general partner or the U.S. business; in those circumstances, CFIUS should have the authority to address any risk to national security presented by that foreign control.

B. *Amend CFIUS certification requirement to avoid disincentivizing mitigation outcomes that enhance U.S. national security*

CFIUS should have the authority and freedom to take the action that best protects U.S. national security, regardless of the politics of that outcome. One change that FINSA made to Section 721 was to require that for each transaction CFIUS approves, the chairperson of the Committee and the head of the lead agency must certify that "in the determination of the Committee, there are no unresolved national security concerns with the transaction that is the subject of the notice or report."[251] For cases that proceed to the "investigation" stage, which today is the majority of transactions, these certifications can be delegated no lower than the Deputy Secretary—the number two official in the department.[252] The certification requirement and the limits on delegation ensure senior-level political accountability before CFIUS may approve a transaction.

---

[248] *CFIUS Reform: Examining the Essential Elements: Hearing on S. 2098 Before the S. Comm. on Banking, Hous., and Urban Affairs*, 115th Cong. 1 (2018) (statement of Scott Kupor, Chair, National Venture Capital Association).
[249] *Id*.
[250] *Id*.
[251] 50 U.S.C. App. § 4565(b)(3)(C)(ii) (2018).
[252] *Id*. § 4565(b)(3)(C)(iv)(II).

While it is important to ensure political accountability, it is also important to ensure that the certification requirement does not encourage perverse results that are contrary to the purpose of the statute. As explained in Part I above, CFIUS plays a limited role within the broader landscape of authorities to address national security risks: the Committee is specifically charged with identifying and addressing any risk that arises from a specific foreign investment (i.e. the incremental risk that a transaction presents, apart from any extant risk that is unrelated to the transaction). The current certification requirement, however, is phrased in much more absolute terms, requiring there to be "no unresolved national security concerns" regarding the transaction.[253] In turn, this extreme requirement can create incentives for CFIUS to act in ways that result in *worse* outcomes for U.S. national security. Consider the following example, which is not atypical of the types of questions CFIUS faces: a U.S. software company with U.S. government customers is acquired by a foreign company. The U.S. company currently performs key parts of its product development in locations around the world, including China. As a condition of CFIUS approval, the foreign party is willing to agree to move all business operations into the United States, and subject them to strict governance and auditing requirements to ensure product integrity. Arguably, CFIUS approval of the transaction subject to those mitigation measures may put the United States in a *better* national security position than if CFIUS does not approve the transaction, even if there is still some measureable risk resulting from the foreign ownership. But the requirement that senior political officials certify that there is "no unresolved risk" may result in that same transaction being prohibited, despite the fact that an approval may actually be preferable from a national security perspective.

A more appropriate certification requirement should reflect that CFIUS's role is to manage, not eliminate, national security risks, and incentivize CFIUS to enter into mitigation agreements that advance U.S. national security (even if some risk remains). For example, CFIUS could certify that its action "better protects the national security of the United States by comparison to other options available to the Committee."

C. *Require formal mechanisms to coordinate with allied countries*

As explained in Part 1, national security risks increasingly cross borders.[254] Acquisitions of companies that are located in allied countries may present risks to U.S. national security even if those companies have no business in the United States (and therefore are not subject to CFIUS jurisdiction).[255] Moreover, many companies, especially in the IT sector, are global companies

---

[253] *Id.* § 721(b)(3)(C)(2)(ii).
[254] *See infra* Part I.
[255] *Id*.

with operations in dozens of countries.[256] It would therefore seem incomplete for the U.S. government to address only the U.S. aspects of acquisitions of those global businesses without coordinating with allied governments.

There are some indications that CFIUS officials have undertaken steps to cooperate with counterparts with allied countries. For example, President Obama's order prohibiting the acquisition of Aixtron followed a series of events in which German authorities first issued and then withdrew a clearance certificate regarding the transaction.[257] German press quoted senior German officials as saying that the decision came as "the [German] federal government has received previously unknown security-related information."[258] These reports suggested that U.S. officials may have coordinated with German authorities to make the latter aware of risks related to the acquisition of Aixtron, and encouraged them to take action.[259] In turn, this suggests that there the United States at least used informal mechanisms to work with allies to address risks presented by transactions that cross multiple borders.

FIRRMA also contains several provisions that appear intended to help CFIUS engage with foreign counterparts. FIRRMA would expressly permit disclosure by CFIUS of "[i]nformation to any domestic *or foreign* governmental entity, under the direction of the chairperson, to the extent necessary for national security purposes and pursuant to appropriate confidentiality and classification arrangements."[260] It would also give CFIUS the authority, through regulations, to exempt from several of the bill's more onerous provisions transactions involving investors from certain countries based on factors including "the national security review process for foreign investment of that country."[261] This provision appears designed, among other things, to incentivize allied governments to establish their own CFIUS-like national security reviews.

More can and should be done to facilitate cooperation among allied governments regarding national security aspects of cross-border transactions. Congress should expressly authorize the Executive Branch to establish formal mechanisms to work with allies on matters related to national security reviews of

---

[256] For a discussion of the global nature of the IT industry, see PREVENTING DEGLOBALIZATION, *supra* note 190.

[257] COVINGTON & BURLING LLP, PRESIDENT OBAMA BLOCKS CHINESE ACQUISITION OF AIXTRON SE (2016), https://www.cov.com/-/media/files/corporate/publications/2016/12/president_obama_blocks_chinese_acquisition_of_aixtron_se.pdf [https://perma.cc/2VXQ-QJC5].

[258] *Germany Blocks Aixtron Sale to China's FGC*, DEUTSCHE WELLE (Oct. 24, 2016), http://www.dw.com/en/germany-blocks-aixtron-sale-to-chinas-fgc/a-36133472 [perma.cc/3W9S-7S8S].

[259] *Id*.

[260] S. 2098, 115th Cong. § 12(2)(C) (2017) (emphasis added).

[261] *Id*. at § 3(A)(5)(C)(ii)(III).

foreign investment and technology transfers outside the United States that may affect U.S. national security. The Administration could then, through executive order, direct the Department of the Treasury as chair of CFIUS to lead and coordinate the establishment of formalized mechanisms to exchange information and coordinate action regarding national security aspects of investments. Congress could further require the Executive Branch to report periodically regarding the progress made in establishing those mechanisms.

D. *Incentivize research and development in the United States*

As explained in Part II above, a principal motivation of the current CFIUS reform effort is to protect potentially sensitive technologies that currently exist in the United States from being lost to rivals, especially China.[262] But keeping technology within the United States is only one aspect of maintaining the United States' technological edge. To stay ahead of rivals, the United States, and especially U.S. industry, must continue to develop *new* technologies and innovate in the United States.

There are two ways in which CFIUS reform could inadvertently impair technological innovation in the United States. First and foremost, many of the most innovative companies are global companies with operations around the world.[263] These companies have choices as to where they locate their research and development (R&D) facilities and intellectual property.[264] While the United States is a leading choice due to its skilled workforce and strong intellectual property protections, among other reasons, it is not the only option.[265] Europe, Japan, India, and, increasingly, China also offer alternative homes in which to establish new businesses and locate R&D centers.[266] Many of these same companies also have business operations, often manufacturing, in China that may require limited transfers of intellectual property.[267] If these companies perceive that CFIUS's authority is overly broad, such that non-sensitive intellectual property may become "trapped" in the United States and unable to be used in pursuit of business operations in other countries, they may rationally choose not to develop that technology in the United States.

---

[262] *See infra* Part II.

[263] *See* PREVENTING DEGLOBALIZATION, *supra* note 190.

[264] JERRY THURSBY & MARY THURSBY, HERE OR THERE? A SURVEY OF FACTORS IN MULTINATIONAL R&D LOCATION 2 (2006), https://www.kauffman.org/what-we-do/research/2009/04/here-or-there-a-survey-of-factors-in-multinational-rd-location [https://perma.cc/YHK9-QLVC].

[265] *Id*. at 10 ("7.2 percent of the respondents expect an increase in technical employment in the United States, whereas 11 percent anticipate a decrease in the United States.").

[266] *Id*. at 9–11.

[267] *Id*. at 23 ("51 percent of . . . sites [outside a company's home country] are in India or China.").

Second, R&D and innovation is an expensive process. Many of the same companies that are leaders in driving innovation in the United States also derive substantial income from developing markets, including China.[268] If CFIUS's authority is overly broad and interferes with companies' ability to conduct business in the Chinese market, they will have fewer resources to devote to R&D in the United States. For these reasons, appropriately scoping CFIUS's authority is not only important so as to avoid restricting legitimate commerce, but is also essential to protecting national security by keeping important R&D assets in the United States and not incentivizing companies to move those resources to countries where the technology may be less protected.

E. *Incentivize filings with CFIUS by requiring risks to be addressed through mitigation where possible*

CFIUS is designed not only to act to address risks, but also to provide the U.S. government with information regarding the investments that may present national security risks.[269] Indeed, the risks presented by a transaction may not be apparent to the parties, or even initially to CFIUS, until the Committee completes a full analysis of the transaction. That objective is frustrated, however, if the law is structured in a manner that disincentivizes parties from bringing transactions to the Committee for review.

Where CFIUS is perceived to be oriented toward prohibiting transactions rather than addressing risks through mitigation, it creates incentives for parties to accept the risks of not filing, or alternatively, to structure their business relationships in a manner that is not subject to CFIUS jurisdiction but may nonetheless present national security risks. For example, if a foreign party is prohibited from acquiring a U.S. business, the foreign party may instead: (i) enter into a license agreement, (ii) hire the U.S. company's key management or personnel, or (iii) enter into an informal cooperative business relationship. Any of these business relationships could present national security risks, but are not currently subject to CFIUS jurisdiction, nor would they be under any of the reform proposals described herein.

The CFIUS statute and regulations should incentivize parties to submit transactions for review by CFIUS by requiring the Committee to resolve risks through mitigation, where consistent with national security, rather than prohibiting transactions. When parties believe that CFIUS's default position is to

---

[268] *See* Paul R. La Monica, *China's Tariffs Would Hurt Apple and These Other US Companies*, CNN MONEY (Apr. 4, 2018), http://money.cnn.com/2018/04/04/news/companies/china-tariffs-us-multinational-sales/index.html [https://perma.cc/5TKH-UZKX] ("Apple . . . generated $18 billion in revenue—20% of its total sales—by selling iPhones, iPads and Macs to Chinese consumers in just its most recent *quarter*.").

[269] JACKSON, *supra* note 103, at 6.

block transactions rather than to seek to resolve risks through mitigation, transaction parties are incentivized instead to accomplish their business objectives through transactions that are not subject to CFIUS's jurisdiction, such as licensing agreements.

Conclusion

CFIUS plays an essential role in protecting the national security of the United States. As the national security challenges facing the United States evolve, so too should our national security laws, including those governing CFIUS. However, lawmakers and policymakers should recognize that CFIUS is only one tool in the proverbial toolbox, and it is not the right tool to address every new risk that may arise. Any reforms to CFIUS should be consistent with the principles described herein to ensure that the United States can continue to advance simultaneously its economic and national security interests.