Keeping up with CFIUS: A Practitioner's Report on National Security Trends in the United States

Farhad Jalinous & Timothy Sensenig*

Abstract

Since the enactment of the Foreign Investment Risk Review and Modernization Act of 2018, the Committee on Foreign Investment in the United States (or CFIUS or the Committee), has enjoyed some of its broadest authority since its establishment almost fifty years ago. Tasked with screening cross-border transactions that 'threaten to impair the national security of the United States', the Committee has discretion to define 'national security', and historically the definition has evolved with, among other elements, the geopolitical tenor of the day. Most recently, the Committee's focus has been mostly on foreign investment in U.S. businesses involved with sensitive personal data, critical technologies or critical infrastructure.

Keywords: CFIUS, FDI, FIRRMA, national security, TID U.S. business.

1 Introduction

The Committee on Foreign Investment in the United States (CFIUS or the Committee) is the United States' foremost inward foreign direct investment (FDI) regulator. Chaired by the U.S. Department of the Treasury, CFIUS is an interagency committee comprising leaders from eight other executive departments and offices (Department of Justice, Department of Homeland Security, Department of Commerce, Department of Defense, Department of State, Department of Energy, Office of the U.S. Trade Representative, and Office of Science & Technology Policy). Five White House offices (Office of Management & Budget, Council of Economic Advisors, National Security Council, National Economic Council, and Homeland Security Council) and two *ex officio* members (Director of National Intelligence and the Secretary of Labor) also currently participate on CFIUS on a non-voting basis and the President or the Committee may appoint or consult other heads of a department, agency, or office on an *ad hoc* basis if a case comes within their equities.[1] Once a small advisory body shrouded in obscurity, it has assumed a large and prominent role in the U.S. Government over the last two decades.

CFIUS is now a significant factor in cross-border transaction structuring and planning, as well as a well-utilised instrument in the United States' foreign investment policy tool belt. The Committee's stated policy goal is to promote open investment in the United States (which it sees as necessary to fuel innovation and growth in a globalised economy), while warding against risks to national security posed by investments that may have non-commercial motivations. Indeed, the Committee has the authority to recommend the U.S. President suspend or prohibit transactions that 'threaten to impair the national security of the United States',[2] an authorisation from which CFIUS draws much, if not all, of its influence. How and to what extent a transaction is determined to threaten to impair 'national security' is largely left to the Committee's discretion. The laws and regulations giving rise to CFIUS's authority and procedures do not clearly define the term.[3] Consequently, the Committee enjoys almost complete free reign to define it for itself and respond in real time to a shifting national security landscape. This constantly shifting definition of national security can – and has – caused much heartburn for industry (that is, those parties to transactions that must interface with CFIUS) and its advisors as they attempt to keep up with the Committee. Unsurprising,

* Farhad Jalinous is a Partner at White & Case LLP in Washington, DC. He is the Global Head of the firm's Foreign Direct Investment (FDI) Reviews & US National Security/CFIUS practice. Timothy Sensenig is an associate at White & Case LLP in Washington, DC and also member of the firm's FDI Reviews & US National Security/CFIUS practice. He owes gratitude to colleagues Farhad Jalinous, Karalyn Mildorf, and Keith Schomig for helpful discussions and tutelage. Any views expressed in this publication are strictly those of the authors and should not be attributed in any way to White & Case LLP.

1 50 U.S.C. § 4565(k); U.S. Department of the Treasury, *CFIUS Overview*, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-overview (last accessed March 20, 2023).

2 50 U.S.C. § 4565(d)(1) (emphasis added). Not all transactions fall within CFIUS's jurisdiction, as will be discussed further in the following text. CFIUS also has the authority to implement mitigation of a transaction, rather than recommend a prohibition. *Id.* at § 4565(l)(3).

3 For the sake of completeness, the modern statute and regulations under which CFIUS operates directs CFIUS to make a 'risk-based analysis' (RBA) with respect to determining national security, which 'shall include an assessment of the threat, vulnerabilities, and consequences to national security related to the transaction'. *Id.* at § 4565(l)(4)(A). As CFIUS can still decide for itself what is a 'threat' and 'vulnerability', and the regulations circularly define both these words in terms of their implications to national security, practically, this RBA is as ill-defined as 'national security'. This article, therefore, will refer to both the concept and the RBA calculation collectively as 'national security'. *See also* 31 C.F.R. § 800.102.

 doi: 10.5553/ELR.000242

the definition is informed by political and economic dynamics of the day, punctuated by legislation, presidential executive orders and the Committee's own regulations and 'keeping up' requires charting trends and closely monitoring the Committee's every move. Today, that means CFIUS's deepening concern over sensitive personal data, including where it is stored and who can access it; its objective both to protect U.S. technologies and to maintain the nation's competitive advantage; and the Committee's close eye on potential adversaries. This article will examine, from the practitioner's perspective, the evolution of this definition of 'national security' with the goal of both understanding the current environment and predicting future developments. Section 2 examines the history of CFIUS, starting with its early years as a mostly irrelevant body, wherein 'national security' was barely a consideration. Section 3 details the rapid changes to the Committee during the Trump Administration and, in particular, the expansive growth under the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which granted CFIUS its broadest jurisdiction and review authority to date and exemplified the current expansive view of 'national security'. Section 4 explores the future of CFIUS and how 'national security' is likely to be construed in the future.

2 CFIUS's History

To understand the current situation, it is helpful to examine CFIUS's historical arc. The Committee's origins and growing pains are well documented, as are the theories seeking to explain this history.[4] These accounts, along with published laws and public record, depict a clear trend of how the U.S. Government has conceptualised 'national security' in the foreign investment context, slowly but surely delegating broader discretion to CFIUS to give meaning to the term.

2.1 Pre-CFIUS and the 1975 Executive Order

The U.S. policy towards FDI following World War II was largely receptive, with few restrictions except for those on certain investments originating in communist or hostile states.[5] This policy began to shift with political and public opinion in the 1970s, when the United States experienced an uptick in investment from nations party to the Organization of Petroleum Exporting Countries (OPEC) and general economic turmoil.[6] By 1975, President Gerald Ford established CFIUS by executive order.[7] President Ford's order was relatively short (occupying only two pages in the Federal Register) and sparse on details. It delegated general authority to CFIUS to 'monitor' the impact of investment in the United States and to 'coordinate' policy on such investment.[8] It made no mention of 'national security', though the executive order granted CFIUS the authority to 'review investments in the United States which … might have major implications for … United States' *national interests*'.[9] It did not specify any procedures for effecting these responsibilities and did not explicitly empower the Committee to pursue mitigation or remedies.

As such, it is commonly interpreted that the order was issued to release political pressure resulting from the economic throes of the 1970s while preserving general free-market principles more than it was related to any specific policy initiative.[10] A memorandum circulated through the Department of the Treasury at the time purported that the reason for the executive order was to 'dissuade Congress from enacting new restrictions' on inbound investment, a real possibility given congressional concerns that some of the OPEC investments were driven by political, rather than commercial, factors, as well as a general alarm among the American public regarding the new FDI.[11] As the order's text evinces, however, it effectively established an advisory body with no formal powers.[12] Ford's executive order created CFIUS, but gave it little direction or purpose and the Committee only held ten meetings in its first five years.[13]

2.2 Exon-Florio and Byrd Amendments

The next chapter in CFIUS's history began when Congress amended, and President Reagan signed, the Exon-Florio Amendment to the Defense Production Act (DPA) as a part of the Omnibus Trade and Competitiveness Act of 1988.[14] Reports about the Amendment suggest it became law at a time when the United States was, again, particularly concerned with the impact of foreign investment on the economy, in addition to new anxiety about threats to the United States' development of computers, robotics, and related technologies.[15] Particularly, the sale of Fairchild Semiconductor Co. by its French parent to a Japanese buyer 'generated intense concern in Congress in part because of general difficulties in trade relations with Japan at the time and because some

4 *See, e.g.*, K. Eichensehr and C. Hwang, 'National Security Creep in Corporate Transactions', 123 Columbia Law Review 549 (2023); M. Baltz, 'Institutionalizing Neoliberalism: CFIUS and the Governance of Inward Foreign Direct Investment in the United States since 1975', 24 Review of International Political Economy 859 (1975); C.S. Eliot Kang, 'U.S. Politics and Greater Regulation of Inward Foreign Direct Investment', 51 International Organization 301 (1997).

5 Kang, above n. 4, at 302.

6 U.S. Congress. House Committee on Government Operations Subcommittee on Commerce, Consumer, and Monetary Affairs. *The Operations of Federal Agencies in Monitoring, Reporting on, and Analyzing Foreign Investments in the United States. Hearings. 96th Congress, 1st Session, Part 3, July 30, 1979*. Washington: GPO, 1979: 334-35, *cited in* Congressional Research Service, *The Committee on Foreign Investment in the United States (CFIUS)* 1, 3 July 2018; Baltz, above n. 4, at 861.

7 Executive Order 11858, 40 F.R. 20263 (7 May 1975).

8 *Id.*, at 20263.

9 *Id.* (emphasis added).

10 Kang, above n. 4, at 315. *See also*, Baltz, above n. 4, at 868.

11 CSR Report on CFIUS, above n. 6, at 334-35; Kang, above n. 4, at 302.

12 Baltz, above n. 4, at 862, 869.

13 *Id.*, at 870.

14 P.L. 100-418, 23 August, 1988, 102 Stat. 1425.

15 CSR Report on CFIUS, above n. 6, at 5; *see also* Eichensehr and Hwang, above n. 4, at 4.

Americans felt that the United States was declining as an international … power'.[16]

The Exon-Florio Amendment granted the President, or a designee, the authority to suspend or prohibit foreign acquisitions of U.S. companies that may threaten to 'impair the national security of the United States', thus giving rise to the standard under which CFIUS operates its reviews to this day.[17] Interestingly, the original text of the bill also granted the President authority to block transactions that threatened to impair 'essential commerce', but the Reagan Administration rejected this version of the bill as too broad and not sufficiently focused on defence and military concerns.[18] Instead, the final text of the Exon-Florio Amendment stated three factors the President should take into account in investment reviews:

(1) domestic production needed for projected *national defence requirements*; (2) the capability and capacity of domestic industries to meet *national defence requirements*, including the availability of human resources, products, technology, materials, and other supplies and services; and (3) the control of domestic industries and commercial activity by foreign citizens as it affects the capability and capacity of the United States to meet the requirements of *national security*.[19]

This final text – as well as the negotiated exclusion of 'essential commerce' from the Amendment – is telling. First, there is a clear pivot from the vague 'national interest' language referenced in the 1975 Ford Executive Order to a more concrete standard. Such pivot marks a milestone in CFIUS's history as the first expansion of its duties and authority. No longer a committee in name only, the Amendment gave the President, but ultimately CFIUS, its first serious marching orders regarding investment security. Second, this standard is inextricably tied to what is often considered 'traditional' notions of national security rooted in protecting the defence industrial base. All three factors focused on domestic production and capacity necessary for national security, rather than economic considerations. As such, the Exon-Florio Amendment indicates the U.S. vulnerabilities CFIUS was instructed to protect at this time, but noticeably does not define 'national security'.

To further add colour to this evolving notion of national security at this time, shortly after Congress enacted the Exon-Florio Amendment, President George H. W. Bush signed another amendment, the 'Byrd Amendment' to the DPA, into law in 1992. It directed the President, or again, a designee, to investigate specifically investments by foreign-government-controlled acquirers, further indicating perceived sources of national security risk, though this time from a threat, rather than vulnerability, perspective.[20]

The authority and factors provided under the Exon-Florio Amendment and the Byrd Amendment started to transform the Committee from a mere advisory body to a player in U.S. foreign investment policy. These amendments also signalled to transaction parties that 'national security' was linked likely in some way to vulnerabilities in the defence industrial base and threats from foreign governments thereto, while at the same time leaving CFIUS discretion to determine the meaning of the term in practice. The difference between the text of the amendments and the level of discretion afforded CFIUS likely led to significant market uncertainty and explains the initial spike in CFIUS filings following the enactment of the Exon-Florio Amendment. Filings from 1989 to 1992 averaged 189.25 annually, but eventually dropped off in subsequent years.[21] It is clear that despite these periodic enhancements in legislation, CFIUS remained relatively obscure during its earliest years.[22]

2.3 FINSA

Following the attacks on September 11, 2001, Congress again turned its focus to foreign investment and set out to establish what closely resembles the modern-day Committee. Starting in 2005, public and congressional outcry ensued when the then-British-owned Peninsular and Oriental Steam Navigation Company (P&O), which had commercial port operations in six U.S. ports, was sold to an Emirati company based in Dubai.[23] Following the outcry, the Emirati investor announced the sale of P&O's U.S. operations to a New York-based financial investor.[24] During the same time period, over twenty-five bills were introduced in the 109th Congress regarding numerous aspects of FDI.[25] By 2007, Congress passed, and President George W. Bush signed, the Foreign Investment and National Security Act (FINSA).[26]

FINSA fundamentally transformed CFIUS. Its preamble stated CFIUS's modern policy objective: ' [t]o ensure the national security while promoting foreign investment and the creation and maintenance of jobs', as well as indicated key reforms, including 'the process by which such investments are examined for any effect they may have on national security', and 'to establish the Committee on Foreign Investment in the United States.'[27] To this end, FINSA codified the Committee in statute, as compared to presidential fiat, and defined its jurisdiction over so-called 'covered transactions'; made Committee membership permanent and expanded member-

16 CSR Report on CFIUS, above n. 6, at 5. The Fairchild Semiconductor transaction was the first transaction CFIUS ever reviewed. Eichensehr and Hwang, above n. 4, at 4. *See also* Kang, above n. 4, at 316-26.

17 Pub. L. 100-418, 23 August 1988, 102 Stat. 1425. President Reagan later formally delegated this authority to the then-existing CFIUS panel by executive order in 1988. Exec. Order No. 12,661, 54 Fed. Reg. 779, 780 (27 December 1988).

18 CSR Report on CFIUS, above n. 6, at 6.

19 102 Stat. at 1426 (emphasis added).

20 Pub. L. 102-484, Oct. 23, 1992, 106 Stat. 2463-2465.

21 From 1993 to 2007, there was an average of 77.2 filings per year. These calculations are based on data shared by CFIUS with the authors regarding CFIUS filings from 1988 to 2011.

22 For example, only 2% of filings resulted in a formal CFIUS investigation between 1989 and 2007. *Id*. *See also* Baltz, above n. 4, at 875.

23 CSR Report on CFIUS, above n. 6, at 1.

24 *Id.*

25 *Id*., at 2.

26 Foreign Investment and National Security Act of 2007, Pub. L. 110-49, 121 Stat. 246.

27 *Id.*

doi: 10.5553/ELR.000242

ship generally; provided procedures and timelines for filing notifications, including that each notified transaction must be approved by a presidentially appointed and Senate-approved government official; required the Secretary of the Treasury to designate a lead agency for review of each transaction; and increased the number of factors the President should consider when conducting a national security review.[28] On this last point specifically, FINSA again did not define 'national security', but the list provided was the most instructive to date:

i. domestic production needed for projected national defene requirements;
ii. the capability and capacity of domestic industries to meet national defense requirements, including the availability of human resources, products, technology, materials, and other supplies and services;
iii. the control of domestic industries and commercial activity by foreign citizens as it affects the capability and capacity of the United States to meet the requirements of national security;
iv. the potential effects of the proposed or pending transaction on sales of military goods, equipment, or technology to any country identified by the U.S. Secretary of State as a country that supports terrorism or as a country of concern regarding specific considerations;
v. the potential effects of the proposed or pending transaction on U.S. international technological leadership in areas affecting U.S. national security;
vi. the potential national security-related effects on U.S. critical infrastructure, including major energy assets;
vii. the potential national security-related effects on U.S. critical technologies;
viii. whether the covered transaction is a foreign government-controlled transaction;
ix. the subject country's record of adhering to nonproliferation control regimes; cooperating in counter-terrorism efforts; and the potential for transshipment or diversion of technologies with military applications, including an analysis of national export control laws and regulations;
x. the long-term projection of U.S. requirements for sources of energy and other critical resources and material; and
xi. such other factors as the President or the Committee may determine to be appropriate, generally or in connection with a specific review or investigation (collectively the 'FINSA Factors').[29]

FINSA also loosely defined 'critical technology' and 'critical infrastructure' (by reference to their importance to national security and defence) and instituted mandatory formal investigations (rather than initial review) into transactions by foreign governments (if notified to CFIUS).[30] As such, the definition of 'national security' begins to take on new meaning under FINSA: implicating important infrastructure and general resource supply, as well as the prior notions of critical technology and the defence industrial base. Nonetheless, 'national security' remained undefined and the last of the FINSA Factors indicates the list of national security considerations provided in the act is non-exhaustive. FINSA, however, was not the last statute to define CFIUS's role in U.S. foreign investment policy.

Today, CFIUS is governed by FINSA's successor, FIRRMA,[31] and both the regulations promulgated by the authority granted to CFIUS thereunder[32] and a recent executive order from President Biden.[33] As will be examined more closely in the following text, similar to its predecessors, FIRRMA was enacted at a time of increased economic and geopolitical tension. These legal instruments, *inter alia*, collectively expanded CFIUS's jurisdiction beyond FINSA, provided additional insight into what the Committee should consider a national security risk, and instituted the first-ever mandatory filing requirement. While the policy objective of CFIUS remains focused on open investment, keeping up with the definition of 'national security' is increasingly challenging as new legislation grants CFIUS's broader authority.

3 FIRRMA and Its Progeny

FIRRMA was signed into law by President Donald Trump on 13 August 2018. The Trump Administration and its allies were consistent in their messaging that FIRRMA was meant to address 'exploited gaps' between the transactions that CFIUS was able to review under FINSA and transactions it currently cannot review (despite them raising similar national security concerns).[34] Those 'gaps' largely pertained to particular investment trends from potential adversaries : (i) real estate acquisitions in sensitive areas; (ii) minority investments (particularly through private equity-type structures) that might not be controlling, but that nonetheless provide access to sensitive data or technology of the target U.S. business; (iii) the increasing use of joint ventures into which U.S.-origin technology is transferred; and (iv) concerns that deals were being structured to circumvent CFIUS.

FIRRMA provided the general contours for CFIUS reform, but not the specifics. Later in 2020, CFIUS released final regulations implementing FIRRMA.[35] Together,

28 *Id.*, at 246-60; *see also* CSR Report on CFIUS, above n. 6, at 9-10.
29 Pub. L. 110-49, 121 Stat. 253.
30 *Id.*, at 258.
31 Pub. L. 115-232, 23 August 2018, 132 Stat. 2173, 50 U.S.C. § 4565.
32 31 C.F.R. §§ 800-802.
33 Exec. Order No. 14,083, 87 Fed. Reg. 57369 (15 September, 2022).
34 *See*, *e.g.*, Remarks by President Trump at a Roundtable on the Foreign Investment Risk Review Modernization Act (FIRRMA), *The White House* 23 August 2018, available at https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-roundtable-foreign-investment-risk-review-modernization-act-firrma/ (last accessed March 20, 2023).
35 31 C.F.R. §§ 800-802. FIRRMA instructed CFIUS to implement various administrative regulations to supplement the text of the statute with specific substantive and procedural details. *See*, *e.g.*, 50 U.S.C. § 4565(a)(4)(D)(iii). Delegation of such rulemaking authority to the Executive Branch is a

FIRRMA and these regulations brought CFIUS into a whole new era. As before, the definition of 'national security' evolved too, and is the most expansive yet. An examination of these legislative and regulatory changes reveal the Committee is aggressively focused on sensitive personal data and critical technologies, while committed to maintaining its steady protections of traditional notions of national security as it pertains to the defence industrial base.

3.1 FIRRMA's Mandatory Filing Requirements

Perhaps most relevant to defining 'national security' is FIRRMA's new mandatory filing requirement. The upshot of FIRRMA and its regulations is that CFIUS remains primarily a voluntary process, as it was since 1975. Since the Exon-Florio Amendment, CFIUS had jurisdiction to review certain transactions and pursue prohibition or mitigation of a transaction that threatened to impair the U.S. national security; however, the Committee could not enforce penalties against parties for not filing. Pursuant to this jurisdiction, CFIUS could (and still can) call in a 'non-notified' transaction but it does require a filing in a narrow set of circumstances. Unless a transaction falls within either of two specific categories, the parties may decide for themselves whether to submit the transaction for CFIUS review. (Though, importantly, CFIUS retains the right to initiate reviews of, or encourage parties to submit voluntarily for review, non-notified transactions and FIRRMA allocated historic financial resources to CFIUS's non-notified team to increase hiring and general ability to research transactions.[36]) The first category applies to investments by *any investor* (subject to certain narrow exemptions) in businesses dealing in *critical technologies*.[37] The second pertains to covered transactions by foreign investors with *substantial (generally defined as 49% or more) foreign government ownership* (subject to certain narrow exemptions) in *any* U.S. business dealing in critical technology, critical infrastructure, and sensitive personal data that results in the investor holding 25% or more of the voting interest in that business, whether direct or indirect.[38] Penalties for failing to make a mandatory filing include civil fines up to $250,000 dollars or the value of the transaction, whichever is greater. These two special categories for a mandatory filing signal to transaction parties and practitioners what is perhaps most central to CFIUS's view of 'national security'. Notably, they align with Committee trends dating back to the Exon-Florio and Byrd Amendments: critical technologies and investments by foreign states and their agents. Regardless of other expansions and nuances under FIRRMA, the legislation and its regulations demonstrate a clear recommitment to these traditional notions of national security.

3.2 CFIUS's Expanded Jurisdiction under FIRRMA

Expansions to CFIUS's jurisdiction under FIRRMA further demonstrate the modern view of 'national security'. Prior to FIRRMA, CFIUS's jurisdiction was limited to what was originally outlined in the Exon-Florio Amendment (and later re-affirmed in FINSA): transactions that could result in foreign control of a U.S. business. As a result, the jurisdictional analysis was largely legal in nature: did the investor's ownership structure make it a 'foreign person'; could the investor's governance rights result in 'control'; and did the target company or assets constitute a 'U.S. business'? There was little, if any, need to consider the substantive national security vulnerabilities of the target to complete the jurisdictional analysis. Historically, the substantive assessment would typically be considered in assessing whether to make a voluntary filing and potential risks relating to such a decision where jurisdiction was clear or presumed.

FIRRMA retained CFIUS's jurisdiction over such transactions (referred to now as 'covered control transactions') but gave CFIUS two new bases for jurisdiction: (i) *non-controlling*, yet *non-passive*, investments (known as 'covered investments')[39] in certain U.S. businesses involved with critical technology, critical infrastructure, or sensitive personal data (known as 'TID U.S. businesses' for technology, infrastructure and data); (ii) incremental acquisitions of interest that result in control or non-passive investments in TID U.S. business; and (iii) certain real estate transactions.[40] The regulations further provide detailed criteria of a U.S. business's operations or the real estate assets, as applicable, that would cause a transaction to fall within these new bases for jurisdiction.[41] As a result, under the new legal framework created by FIRRMA and the regulations, the jurisdictional analysis for non-controlling transactions re-

core principal of American administrative law and the source of most federal agencies' rulemaking authority. *See, e.g.*, *Chevron U.S.A., Inc.* v. *NRDC*, 467 U.S. 837 (1984).

36 50 U.S.C. § 4565(b)(1)(H). Since the Exon-Florio Amendment, CFIUS retains *jurisdiction* to review certain transactions and pursue prohibition or mitigation of a transaction that threatens to impair the U.S. national security; however, the Committee could not previously enforce penalties against parties for not submitting a filing. Parties to transactions subject to CFIUS's jurisdiction—but who chose not to notify CFIUS of the transaction—risk the possibility that CFIUS learns of the transaction and requests a filing from the parties (called a 'non-notified' transaction). Accordingly, parties who believe their transaction is likely to present substantive national security issues, whether or not subject to filing requirements, may choose to file voluntarily to avoid unexpected requests and possible remediation from CFIUS.

37 *Id.*, at § 4565(b)(1)(C)(v)(IV)(cc); 31 C.F.R. § 800.401(b)(2). Note that the investment must also generally be subject to CFIUS's expanded jurisdiction, i.e. a covered control transaction or a covered investment. As described further in the following text, these businesses must also be a 'TID U.S. business'.

38 50 U.S.C. § 4565(b)(1)(C)(v)(IV)(bb); 31 C.F.R. § 800.401(b)(1). The regulations stipulate a substantial foreign government ownership is one in which a national or subnational government from a single foreign state holds 49% or more of the voting interest, whether direct or indirect. As described further in the following text, these businesses are called 'TID U.S. businesses'.

39 *See infra* Part II(b)(i).

40 50 U.S.C. § 4565(4)(B)-(D) (describing what constitutes a 'covered transaction').

41 31 C.F.R. §§ 800.214-215, 241; *id.*, at § 802.211.

doi: 10.5553/ELR.000242

quires a substantive assessment of the target business against these detailed criteria.

3.2.1 Covered Investments

CFIUS's jurisdiction to review certain non-controlling, yet non-passive investments is based on both the nature of the investment and the nature of the target U.S. business. FIRRMA supplied the first half of the test: the nature of the investment must afford a foreign person[42] one or more of the following:

- access to any material non-public technical information in the possession of the TID U.S. business;
- membership or observer rights on the board of directors (or equivalent) of the TID U.S. business or the right to nominate an individual to a position thereto; or
- any involvement, other than through voting of shares, in substantive decision-making of the TID U.S. business regarding critical technology, critical infrastructure, or sensitive personal data.[43]

The regulations supply the second half of the test by defining with more particularity what is required to be a 'TID U.S. business'. The three categories of TID U.S. businesses are as follows:

Critical Technology

As indicated earlier, the first of the three TID U.S. business types relates to a traditional national security concern of CFIUS's. A U.S. business that produces, designs, tests, manufactures, fabricates, or develops one or more 'critical technologies' is considered a 'TID U.S. business'.[44] The regulations maintain without change or additions to the definition of 'critical technology' in FIRRMA, which includes: defence articles and services included on the United States Munitions List (USML); certain items included on the Commerce Control List (CCL); certain nuclear-related facilities, equipment, parts and components, materials, software, and technology; select agents and toxins; and emerging and foundational technologies controlled for export pursuant to section 1758 of the Export Control Reform Act of 2018 (ECRA).[45]

Sensitive Personal Data

Despite FIRRMA's recommitment to historical concerns about critical technologies, FIRRMA directly addresses a new perceived risk to national security only relevant in the modern age: data. FIRRMA contains no definitions or delineating principles with respect to 'sensitive personal data', other than that it refers to data that may be exploited in a manner that threatens national security.[46] To address this ambiguity, the regulations create two classes of sensitive personal data. First, sensitive personal data includes 'identifiable data', which is defined as data that can be used to distinguish or trace an individual's identity, but only if the following category and collection requirements are satisfied:

- Categories: the identifiable data falls within one of ten identified categories, which range from financial data that could be used to determine an individual's financial distress or hardship to geolocation data.
- Collection: the U.S. business that maintains or collects the identifiable data over certain thresholds.

And second, the results of an individual's genetic tests, including any related genetic sequencing data, whenever such results constitute 'identifiable data' – regardless of the amount of such data or the population on which it is collected.[47] The summary chart[48] is illustrative (see Table 1 below).

Any U.S. business that maintains or collects either class of 'sensitive personal data', with limited exceptions (e.g. such data on the employees of the U.S. business or available in the public domain), is considered a 'TID U.S. business'.

Critical Infrastructure

Finally, the third TID U.S. business category maintains commitments initiated under FINSA to protect important U.S. infrastructure. FIRRMA instructs CFIUS to limit its jurisdiction over covered investments in 'critical infrastructure' to a subset of infrastructure (referred to in the regulations as 'covered investment critical infrastructure') that is likely to be of particular importance to U.S. national security. The regulations define this subset with precise bright lines in a detailed appendix that identifies twenty-eight types of infrastructure.[49] These include telecoms, power, oil and gas, water supply, financial institutions, the defence industrial base, and ports. The appendix also assigns one or more of five specified functions (own, operate, supply, service, or manufacture) to each of the twenty-eight types of infrastructure.[50] A U.S. business that performs at least one of the functions assigned to the corresponding type of covered investment critical infrastructure is considered a 'TID U.S. business'.

42 Oher than a foreign person that meets a detailed list of criteria, referred to as an 'excepted investor'. 31 C.F.R. § 800.219.
43 50 U.S.C. § 4565(a)(4)(D).
44 31 C.F.R. § 800.215.
45 50 U.S.C. § 4565(a)(6).
46 *Id.*, at § 4565(a)(4)(B)(iii)(III).
47 31 C.F.R. § 800.241. This definition excludes data derived from databases maintained by the U.S. Government and routinely provided to private parties for purposes of research.
48 This chart was designed by the authors based on the CFIUS regulations. *Id.*
49 50 U.S.C. § 4565(a)(4)(B)(ii)(I); *id.*, at § 4565(a)(5).
50 31 C.F.R. § 800, Appendix A.

Table 1

Type of Data	Threshold
Identifiable data collected or maintained by a U.S. business that:	
Targets or tailors products or services to any **U.S. executive branch agency or military department** with intelligence, national security, or homeland security responsibilities, or to personnel and contractors thereof.	No minimum.
Has maintained or collected any identifiable data within **one or more categories**: i. financial data ii. consumer report data iii. health insurance data iv. health/medical data v. non-public electronic communications data vi. geolocation data collected via positioning systems vii. biometric enrolment data viii. government ID data ix. U.S. government personnel security clearance status data x. sets of data used to apply for a personnel security clearance or employment in a position of public trust	Greater than **one million individuals** in the 12 months preceding the transaction.
Has a demonstrated **business objective** to collect any of the aforementioned10 forms of data now or in the future.	Greater than **one million individuals**.
Genetic data	
The results of an individual's genetic tests, including any related genetic sequencing data, whenever such results constitute identifiable data. Such results shall not include data derived from databases maintained by the U.S. Government and routinely provided to private parties for purposes of research.	No minimum.

3.2.2 Covered Real Estate Transactions

In addition to TID U.S. businesses, FIRRMA also gave CFIUS jurisdiction to review the purchase or lease by, or concession to a foreign person of certain real estate (i) located within or functioning as part of an air or maritime port or (ii) that is in close proximity to, or that provides the foreign person the ability to collect intelligence on or surveil national security activities at U.S. military installations or other sensitive U.S. Government facilities or property.[51] The regulations implement this new basis for jurisdiction through the concept of a 'covered real estate transaction'.[52] Specifically, unless any of the eight enumerated exceptions applies, CFIUS has the authority to review any purchase or lease by, or concession to, a foreign person of 'covered real estate' either directly or indirectly, that affords the foreign person at least three of four 'property rights'.[53]

With respect to CFIUS's constantly shifting view of 'national security', this expanded jurisdiction under FIRRMA and its regulations is illustrative for two reasons. First, most obviously, CFIUS jurisdiction is expanded from FINSA. This demonstrates the Committee's ability to exercise an aggressive regulatory approach and it is now motivated and authorised to review more transactions than it could previously. Consequently, CFIUS can now also mitigate or prohibit more transactions than before, overall increasing its role in U.S. foreign investment policy and making it a gatekeeping consideration for many transactions. Second, the criteria for subjecting transactions to CFIUS's expanded jurisdiction – TID U.S. businesses and certain real estate – reflect the types of U.S. businesses or assets that the U.S. Government views as an essential component to 'national security' (in addition to maintaining the traditional integrity and reliability of the defence industrial base under the Exon-Florio Amendment). What is more, FIRRMA and the regulations, while not perfect, lay out in great detail the TID U.S. business and real estate requirements. While CFIUS maintains its discretion under the original FINSA Factors to pursue other national security considera-

51 50 U.S.C. § 4565(a)(4)(C).

52 31 C.F.R. § 802.212.

53 These are the right to: (i) physically access the real estate; (ii) exclude others from physically accessing the real estate; (iii) improve or develop the real estate; or (iv) attach fixed or immovable structures or objects to the real estate.

doi: 10.5553/ELR.000242

tions,[54] this level of detail is the most illustrative definition of 'national security' in CFIUS's history.

3.3 Executive Order 14083 and Guidelines

As close as FIRRMA and its regulations come to painting a clear(er) national security picture for transaction parties and practitioners, President Joseph Biden recently signed Executive Order 14083 (the EO)[55] identifying the national security factors that the Committee *must* now consider when reviewing covered transactions. The EO marks the first time in CFIUS's nearly fifty-year history when the President expressly publicly directed CFIUS to consider certain specific sets of factors in its review of national security risks arising from covered transactions. In particular, the EO expands on two FINSA Factors and directs CFIUS to consider three additional factors in its reviews, focusing on five areas: (i) supply chain resilience; (ii) impact on U.S. technological leadership; (iii) assessment of aggregate investment trends in industries; (iv) cybersecurity risks; and (v) sensitive data. While nothing precluded CFIUS from considering such issues prior to the EO – indeed, most of the points covered in the EO track with areas of CFIUS focus since FIRRMA and the FINSA Factors always included a catch-all provision for the Committee's discretion[56] – it does direct CFIUS publicly to consider these new factors in reviews. Accordingly, the EO reflects a clear policy priority by the Biden Administration as the U.S. Government continues to try to adapt CFIUS to the ever-evolving national security landscape.

These five factors are as follows:

1 A given transaction's effect on the resilience of critical U.S. supply chains that may have national security implications, including those outside of the defence industrial base

Following more than two years of supply chain disruptions in the United States and globally,[57] the EO's directive begins by emphasising the United States' need to ensure supply chain resiliency. In expanding on the issues to be considered under FINSA's third factor noted earlier (related to control of domestic industries and commercial activity),[58] the EO states that supply chain disruptions are a vulnerability to U.S. national security if they occur in certain manufacturing capabilities, services, critical mineral resources or technologies fundamental to U.S. national security. Notably, the EO emphasises that supply chain resilience considerations are not limited to the defence industrial base. The EO specifically references microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy (such as battery storage and hydrogen), climate adaptation technologies, critical materials (such as lithium and rare earth elements), and elements of the agriculture base that have implications for food security as examples of such areas fundamental to national security.[59] In assessing supply chain considerations, the EO directs that the Committee must consider, as appropriate (i) the United States' domestic capacity to meet national security requirements of supply chains; (ii) the degree of involvement in the supply chain by a foreign person party to the transaction that might take actions to threaten or impair national security or has relevant third-party ties that might cause the transaction to pose such a threat; (iii) the degree of diversification through alternative suppliers, including those located in allied or partnered economies; (iv) whether the U.S. business party to the transaction supplies, directly or indirectly, the USG, the energy sector industrial base, or the defence industrial base; and (v) the concentration of ownership or control by the foreign person in the given supply chain.

2 A given transaction's effect on U.S. technological leadership in areas affecting U.S. national security, including microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies

The EO acknowledges the long-held CFIUS policy that foreign investment can foster domestic innovation, but re-iterates the similarly long-held belief that it is important to protect U.S. technological leadership via CFIUS reviews. Accordingly, in expanding on the fifth FINSA Factor (relating to U.S. technological leadership),[60] the EO requires CFIUS to consider, as appropriate, whether a covered transaction involves certain manufacturing capabilities, services, critical mineral resources, or technologies fundamental to U.S. technological leadership, which it notes include microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies.[61] In addition to considering whether the foreign person party to the transaction or its relevant third-party ties create risks to national security, the EO directs CFIUS to consider whether a covered transaction could reasonably result in future advancements and applications in such technologies that could undermine national security. As discussed earlier, starting with FINSA and continued under FIRRMA, maintaining technological leadership has long been a factor that CFIUS is specifically instructed to consider in reviews, but the EO identifies *specific industries* in which CFIUS must analyse this consideration. The EO also directs the Office of Science and Technology Policy to 'periodically' publish a list of technology sectors, in addition to those identified in the EO, that are fundamental to U.S. technological leadership in areas relevant to na-

54 50 U.S.C. § 4565(f)(11) (in describing the factors the Committee and President should consider in determining national security: 'such other factors as the President or the Committee may determine to be appropriate, generally or in connection with a specific review or investigation').

55 Exec. Order No. 14,083, 87 Fed. Reg. 57369 (15 September 2022).

56 50 U.S.C. § 4565(f)(11).

57 *See*, e.g., *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth*, The White House (June 2021).

58 50 U.S.C. § 4565(f)(3).

59 Exec. Order No. 14,083, 87 Fed. Reg. 57369 (15 September 2022).

60 50 U.S.C. § 4565(f)(5).

61 Exec. Order No. 14,083, 87 Fed. Reg. 57369 (15 September 2022).

tional security. Accordingly, the EO contemplates the list of industries CFIUS considers with respect to technology leadership issues evolving over time.

3 Industry investment trends that may have consequences for a given transaction's impact on U.S. national security when considered in the aggregate

Although CFIUS reviews each covered transaction on a case-by-case basis, the EO directs CFIUS to look *beyond* the specific transaction before it in assessing its impact on U.S. national security and to consider the *aggregate* impact of foreign investments in the same or related industries.[62] This approach is not necessarily new. However, it arguably denotes a subtle shift in CFIUS's long-held public stance that it reviews each case based on the facts of the particular transaction before it. While FIRRMA and its implementing regulations generally direct the Committee and the President to review the risk arising from the particular transaction before it in assessing the national security risks arising from the transaction, the EO makes clear that such reviews should not occur in isolation, and should instead consider industry investment trends. The White House Fact Sheet released with the EO notes that

> there may be a comparatively low threat associated with a foreign company or country acquiring a single firm in a sector, but a much higher threat associated with a foreign company or country acquiring multiple firms within the sector.[63]

This emphasis on considering incremental investments over time in the same or related industries will likely add a layer of uncertainty when parties assess the potential risks arising from their transactions. This is because it is often difficult to assess both general investment trends within an industry and whether a particular transaction will be the tipping point within an industry trend that the Committee finds problematic.

4 Risks to U.S. persons' sensitive data

Consistent with ongoing heightened national security interest in data security that began under FIRRMA's introduction of TID U.S. businesses, the EO instructs CFIUS to consider a number of factors relating to sensitive data of individuals.[64] The EO further instructs CFIUS to consider the risks to national security of foreign investments in U.S. businesses that have access to or that store personal data of U.S. persons. Notably, whereas the TID U.S. business standard in the CFIUS regulations refers to U.S. businesses that *collect or maintain* sensitive personal data, the EO directs CFIUS to consider U.S. businesses that have *access* to sensitive data, which is a broader standard. The EO also goes well beyond data considerations under the TID U.S. business standard by using the term 'sensitive data', which is distinct from – and more expansive than – the defined term 'sensitive personal data' under the CFIUS regulations. Significantly, the EO notes that sensitive data includes U.S. persons'

> health, digital identity, or other biological data and *any data that could be identifiable or de-anonymized*, that could be exploited to distinguish or trace an individual's identity in a manner that threatens national security.[65]

The EO also notes that 'advances in technology, combined with access to large data sets, increasingly enable the re-identification or de-anonymisation of what was once identifiable data'.[66] Practitioners can attest that CFIUS can be reluctant to exempt anonymised or aggregated data from requirements in mitigation agreements relating to data concerns, and the EO confirms the Biden Administration's concerns in this area.

5 Cybersecurity risks that threaten to impair national security

Related to the sensitivities around personal data, the EO provides that CFIUS shall consider whether a covered transaction might provide a foreign person, or third-parties to which it has ties, with direct or indirect access to capabilities or information databases and systems through which they could conduct cyber intrusions or other malicious cyber-enabled activity.[67] The EO highlights as relevant national security considerations cyber activities that can impact (i) the outcome of elections; (ii) the operation of U.S. critical infrastructure, including critical energy infrastructure and smart grids; (iii) the confidentiality, integrity or availability of U.S. communications; and (iv) the protection or integrity of data in storage or databases or systems housing sensitive data. The EO also instructs CFIUS to consider the cybersecurity posture, practices, capabilities, and access of both the foreign person and the U.S. business involved in the transaction that could enable malicious cyber activities. The EO's emphasis on cybersecurity is neither new nor surprising given ongoing concerns about cyber vulnerabilities. More and more in recent years, CFIUS practitioners have certainly seen the Committee address concerns relating to cybersecurity issues in covered transactions, including potential third-party vulnerabilities.

All said, the EO provides a useful – but not definitive – guide for considering how CFIUS defines 'national security', but it does not fundamentally change the CFIUS process or authorities. Building on FIRRMA and its regulations, CFIUS is demonstrably concerned with tradi-

62 *Id.*

63 FACT SHEET: President Biden Signs Executive Order to Ensure Robust Reviews of Evolving National Security Risks by the Committee on Foreign Investment in the United States, The White House (15 September 2022) www.whitehouse.gov/briefing-room/statements-releases/2022/09/15/fact-sheet-president-biden-signs-executive-order-to-ensure-robust-reviews-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states (last accessed on March 20, 2023).

64 *Id.*

65 Exec. Order No. 14,083, 87 Fed. Reg. 57369 (15 September 2022) (emphasis added).

66 *Id.*

67 *Id.*; *see also* 50 U.S.C. § 4565(a)(4)(B)(iii)(III).

doi: 10.5553/ELR.000242

tional notions of national security, such as critical technologies and integrity of supply (albeit adapted for modern contexts), but continues its mounting efforts to monitor and secure data. Factor (iii) regarding aggregate industry trends, similar to FIRRMA's expanded jurisdiction, also indicates the U.S. Government will continue to maximise CFIUS's statutory authority. For those keeping up with CFIUS's approach to national security, the FIRRMA era is perhaps the broadest in the concept's history.

4 Potential Changes to Come

From President Ford's original 1975 executive order through President Biden's in 2022, both CFIUS's authority and its definition – however nebulous – of 'national security' has expanded considerably. How this growth continues in the future, as it has before, will likely track political and economic trends, but it is doubtful it will ever reverse itself. As CFIUS becomes an ever more important tool in implementation of U.S. foreign investment policy, the executive and legislative branches, also informed by classified reports from CFIUS that the public cannot access,[68] are prone to push CFIUS's boundaries further and further. As such, one need only look at the recent proposals in Congress, particularly those from last spring, for indications of how CFIUS may expand in the future. The focus on critical technology and securing the defence industrial base are certain to continue, as are the newer concerns with sensitive data. However, geo-political tensions may drive expansions into higher education, agriculture, real estate, and genetic data.[69]

4.1 Higher Education

Higher education has often been discussed as a possible area for CFIUS intervention. On June 8, 2021, the U.S. Senate passed by a large majority (68-32 vote) the U.S. Innovation and Competition Act of 2021.[70] Among other provisions, this bill included the Strategic Competition Act (SCA). The SCA would amend the Higher Education Act and the DPA to expand CFIUS's jurisdiction and reporting requirements for institutions of higher education.[71] Specifically, it would add certain gifts to 'institutions of higher education' to CFIUS's jurisdiction.[72]

To accommodate this expansion, the SCA would amend the definition of a 'covered transaction' to include 'any gift to an institution of higher education from a foreign person, or the entry into a contract by such an institution with a foreign person'[73] if the following requirements are met:

- *One of the following*: **(1)** The 'value of the gift or contract equals or exceeds $1,000,000'; **or (2)** 'the institution receives, directly or indirectly, more than one gift from or enters into more than one contract, directly or indirectly, with the same foreign person for the same purpose the aggregate value of which, during the period of two consecutive calendar years, equals or exceeds $1,000,000'; **and**
- *One of the following*: The gift or contract **(1)** 'relates to research, development, or production of critical technologies and provides the foreign person potential access to any material nonpublic technical information', **or (2)** 'is a restricted or conditional gift or contract that establishes control'.[74]
- Further, the SCA would define 'Institution of Higher Education' (IHE) to mean 'any institution, public or private, or, if a multicampus institution, any single campus of such institution, in any State' that meets the following four criteria:
- It 'is legally authorized within such State to provide a program of education beyond secondary school'(i.e. beyond 12th grade);
- It 'provides a program for which the institution awards a bachelor's degree (or provides at least a 2-year program which is acceptable for full credit toward such a degree) or a more advanced degree';
- It 'is accredited by a nationally recognized accrediting agency or association'; **and**
- It is an institution 'to which the Federal Government extends Federal financial assistance (directly or indirectly through another entity or person), or that receives support from the extension of Federal financial assistance to any of the institution's subunits.'[75]

Under the SCA, a mandatory declaration would be required with respect to the gift or contract that relates to research, development, or production of critical technologies and provides the foreign person potential access to any material non-public technical information.[76] Further, 'Academic freedom at institutions of higher education in the United States' would be added running list of FINSA Factors,[77] and in the case of a covered

68 50 U.S.C. § 4565(m)(1).

69 Some bills, such as the America Creating Opportunities for Manufacturing Pre-Eminence in Technology, and Economic Strength Act (America COMPETES Act), also sought to regulate *outbound* investment; however, this authority would not be vested in CFIUS, but a new, sister committee. *See, e.g.*, Inu Manak, *Outbound Investment Screening Waits in the Wings*, Council on Foreign Relations (15 August 2022), available at www.cfr.org/blog/outbound-investment-screening-waits-wings (last accessed March 20, 2023); K. O'Keeffe et al., 'Lawmakers Make Bipartisan Push for New Government Powers to Block U.S. Investments in China', *Wall Street Journal* (14 June 2022). The America COMPETES Act went through numerous amendments and reviews by both houses of Congress and was ultimately passed as the CHIPS and Science Act of 2022 without the outbound screening mechanism. Pub. L. 117-167 (9 August 2022).

70 S. 1260, 117th Congress, available at www.congress.gov/bill/117th-congress/senate-bill/1260/text (last accessed March 20, 2023).

71 The SCA would also amend a single section of the Higher Education Act of 1965 (20 U.S.C. § 1011f) to include the Secretary of the Treasury, as chair of CFIUS, to the list of recipients of higher education disclosures relating to foreign gifts and ownership.

72 S. 1260, 117th Congress § 3138 (2021).

73 *Id.*, at § 3138(a)(1)(B).

74 *Id.*

75 *Id.*

76 *Id.*, at § 3138(a)(2).

77 *Id.*, at § 3138(a)(3).

transaction involving an IHE, proposed earlier, the Secretary of Education would be included on CFIUS.[78]
When reviewing the SCA for indications of what a future CFIUS may look like, three trends emerge. First, no different from FIRRMA, FINSA, or any of their related executive orders and regulations, the draft SCA takes a broad approach to capturing national security concerns. However, attenuated to higher education, it proposes, for example, an arguably expansive IHE definition. It also further expands the list of national security factors beyond the original FINSA Factors. Second, a dual approach with respect to investment from potential adversaries is likely to continue. The dual thresholds for what qualifies as a 'gift' – (i) a general threshold (i.e. $1,000,00) to capture presumably high-impact donations and (ii) a second threshold defined not by dollar amount, but the nature of the investment – is nearly identical to the expansions to CFIUS jurisdiction under FIRRMA's. The TID U.S. businesses and covered investments provisions similarly maintained broad jurisdiction over traditional covered control transactions, but stretched CFIUS jurisdiction to covered smaller investments that despite small economic impact could nonetheless be sensitive to the U.S. Government. Third, and finally, the mandatory filing requirement remains an attractive tool to Congress for promoting disclosure to CFIUS and generally shape foreign investment policy by granting CFIUS additional police powers.

4.2 Agriculture

Seasoned practitioners know well that agriculture has often been a topic of conversation in CFIUS circles. In the last two years, at least five bills concerning CFIUS and agriculture were introduced in Congress, including, but not limited to: the Security and Oversight of International Landholdings (SOIL) Act of 2022,[79] the Promoting Agriculture Safeguards and Security (PASS) Act of 2022,[80] the Food Security is National Security Act of 2021,[81] the Foreign Adversary Risk Management (FARM) Act of 2021,[82] and the Agriculture Security Risk Review Act of 2021.[83] Each of these bills would amend the DPA to, among other things, install the U.S. Secretary of Agriculture on CFIUS. Some would amend the definition of 'critical infrastructure' to include 'agricultural supply chains' and expand CFIUS's jurisdiction to review 'any [covered] transaction … that could result in control of any United States business that is engaged in agriculture and uses agriculture products'.[84] Others expand CFIUS jurisdiction over or outright block transactions regarding agricultural land from China, Russia, Iran, South Korea (or some alternative definition of 'nonmarket economy country' or those designed by the Director of National Intelligence as a threat to U.S. national security).[85] One simply adds to the list of FINSA Factors:

> the potential effects of the proposed or pending transaction on the security of the food and agriculture systems of the United States, including any effects on the availability of, access to, or safety and quality of food.[86]

Given the flurry of legislative activity around agriculture and CFIUS, it is expected to remain a topic for national security consideration in the future, especially given there are currently no federal or state prohibitions on such ownership.[87] However, the bills may lose traction because of a potentially low perceived threat and the relative flexibility under current law to review agriculture cases. Interestingly, the bills focus mainly on transactions resulting in control of agricultural lands. According to the Congressional Research Service, only 2.7% of all privately owned agricultural land in the United States is currently held by foreign persons.[88] As such, the threat posed by additional foreign persons buying agricultural lands may not be as serious as those obtaining critical technologies or sensitive personal data. Further, the bills risk redundancy with current law. Under FIRRMA and its regulations, for example, the President and CFIUS may already consider national security factors as they see fit, which could include food supply chains and agricultural land if the Committee so desired.[89] Additionally, should a specific case require it, the President – or the Committee acting as his or her delegee – could appoint the U.S. Secretary of Agricultural to the Committee under FIRRMA.[90] Indeed, CFIUS has brought in the Secretary Agriculture to review matters that fall under the Department of Agriculture's equities.[91] Nonetheless, there is clearly congressional interest in the topic and it could in the future become an enumerated component of 'national security' for CFIUS.

4.3 Real Estate

It is possible that a future CFIUS will also be increasingly focused on real estate transactions as a means of protecting the defence industrial base. On April 21, 2021, the U.S. Senate referred to the Senate Committee on Banking, Housing, and Urban Affairs (Senate Banking Committee) the Protecting Military Installations and Ranges Act of 2021 (PMIRA).[92] This bill would expand CFIUS's jurisdiction by amending 'covered transaction'

78 *Id.*, at § 3138(a)(4).
79 S. 4821, 117th Congress § 1 (2022).
80 H.R. 8274, 117th Congress § 1 (2022).
81 S. 3089, 117th Congress § 1 (2021).
82 S. 2931, 117th Congress § 1 (2021).
83 H.R. 8274, 117th Congress § 1 (2021).
84 S. 2931, 117th Congress § 3(c) (2021).
85 S. 4821, 117th Congress § 2 (2022); H.R. 8274, 117th Congress § 2 (2022).
86 S. 3089, 117th Congress § 2 (2021).
87 Congressional Research Service, *Foreign Farmland Ownership in the United States* (November 18, 2021), at 1.
88 *Id.*, at 2.
89 50 U.S.C. § 4565(f)(11).
90 *Id.*, at § 4565(k)(2)(J).
91 *See, e.g.*, Fufeng 'Looks Forward' to Building GF Plant after CFIUS Says it Has 'No Jurisdiction', *Knox News Radio* (December 13, 2022), available at https://knoxradio.com/2022/12/13/fufeng-looks-forward-to-building-gf-plant-after-cfius-says-it-has-no-jurisdiction/ (last accessed March 20, 2023).
92 S. 1278, 117th Congress (2021), available at www.congress.gov/bill/117th-congress/senate-bill/1278/text?r=29&s=1 (last accessed March 20, 2023).

doi: 10.5553/ELR.000242

under the DPA to include land transactions *by certain foreign governments* (which is not currently specified under FIRRMA or the subsequent CFIUS regulations). This amendment would require 'unilateral mandatory review' of transactions meeting the three following requirements:

- The transaction in question is the purchase, lease, or concession of land in the United States;
- The acquirer is the Russian Federation, the People's Republic of China, the Islamic Republic of Iran, **or** the Democratic People's Republic of Korea; **and**
- The land in question meets certain proximity thresholds to various sensitive U.S. Government land.[93]

As proposed in PMIRA, the new 'unilateral mandatory review' would direct CFIUS to review every transaction meeting these three requirements.[94] It is unclear from the draft how CFIUS would know about these transactions, and thus, the pre-existing notice and declaration requirements likely still apply. While PMIRA is underdeveloped, its introduction in the Senate reveals an ongoing concern in Congress – and possibly, through classified reports, in CFIUS – regarding government land and investments from non-allied nations in that land.

4.4 Genetic Data

On May 20, 2021, the U.S. Senate referred to the Senate Banking Committee the Genomics Expenditures and National Security Enhancement Act of 2021 (GENE Act).[95] The GENE Act would not expand CFIUS's jurisdiction in the way the SCA or PMIRA would, but it does broaden the category of transactions that require a mandatory filing. Under the GENE Act, when a covered transaction (as defined by the current law) involves a U.S. business that 'maintains or collects information about genetic tests of United States citizens, including any such information relating to genomic sequencing' a mandatory filing would be triggered.[96] Similar to the Secretary of Education's addition to CFIUS under the proposed SCA, the GENE Act would add the Secretary of Health and Human Services to CFIUS when a business involving genetic material is implicated.[97]

Although under FIRRMA and its regulations, genetic data is already included in the definition of TID U.S. business and a mandatory filing is already required for certain investments in these types of businesses, the GENE Act is notable because it would require a mandatory filing for all covered transactions involving genetic data, not just those by foreign governments and their entities. Similar to FIRRMA's mandatory filing requirements for all covered transactions in critical technology, the GENE Act suggests genetic data in particular is sensitive to national security and therefore requires CFIUS review in all circumstances. Given the latest EO and general concerns about data, it would not be surprising to see more legislation tinkering with sensitive personal data.

5 Conclusion

This article explored the growth of CFIUS as well as the parallel evolution of 'national security' as a concept in the United States' foreign investment policy throughout history. When CFIUS was first organised pursuant to an executive order by President Ford in 1975, 'national security' was barely a consideration and CFIUS was rarely involved in regulating transactions. Today, however, it is part and parcel of the Committee's identity and the Committee is a first-string strategy consideration in most cross-border transactions. The interceding legislative renditions reveal that 'national security' is a politically salient concept in the United States, but it is more and more CFIUS's responsibility to define this term. The Exon-Florio Amendment, FINSA, and FIRRMA each appear to provide more structure and direction to CFIUS, but each also provided significant deference to the Committee, with FIRRMA providing the Committee's broadest jurisdiction and authority in history, while granting few checks on CFIUS's discretion.

It is important to underscore that both CFIUS and its interpretation of 'national security' continue to evolve. In 1975, there was a 'national interest' in controlling investment from OPEC countries; tomorrow, gifts to IHEs may pose a threat to 'national security'; but today, technology, infrastructure, data, and a competitive global geopolitical landscape are the key concerns occupying the Committee. This offers optimism to transactional parties who feel the current regime unnecessary frustrates their transaction objectives that are not motivated by non-commercial factors. However volatile national security trends may seem, with careful attention to statutes, regulations, and other sources of law as well as close monitoring of political and economic developments, and – of course – adept counsel, it is possible to keep up with CFIUS.

93 S. 1278, 117th Congress § 2(a)(2).
94 *Id.*, at § 2(b)(4).
95 S. 1745, 117th Congress (2021), available at www.congress.gov/bill/117th-congress/senate-bill/1745/text (last accessed March 20, 2023).
96 S. 1745, 117th Congress § 2(a) (2021).
97 *Id.*, at §2(b).