wiley

The Committee on Foreign Investment in the United States (CFIUS) Handbook

wiley.law

TABLE OF CONTENTS

wiley

Introduction

The Committee on Foreign Investment in the United States (CFIUS or the Committee) is an interagency committee that reviews transactions involving certain foreign investments in U.S. businesses and real estate for potential national security risks. CFIUS's mission is to address U.S. national security considerations while simultaneously ensuring that the United States maintains an open investment policy.

The Committee was originally established in 1975 by Executive Order 11858 in response to concerns that investments from the Middle East into the United States were unchecked and had the potential to pose national security risks. At that time, CFIUS was charged with monitoring the impact of foreign investments but had no explicit power to regulate or block those transactions.

CFIUS's mission is to address U.S. national security considerations while simultaneously ensuring that the United States maintains an open investment policy.

Subsequently in 1988, in response to concerns that the United States was losing critical technologies as a result of a series of Japanese foreign direct investment transactions, Congress passed the Exon-Florio Amendment as part of the Defense Production Act of 1950. The Exon-Florio Amendment expanded the Committee's jurisdiction by granting the President express authority to suspend or prohibit CFIUS transactions that pose a threat to the national security of the United States. Twenty years later, in 2007, following controversy surrounding the sale of management operations at certain U.S. seaports to a state-owned company from the United Arab Emirates, Congress passed the Foreign Investment and National Security Act of 2007 (FINSA), resulting in a more formalized process, including additional CFIUS filing requirements for parties and broader national security review considerations, particularly with respect to transactions involving certain critical infrastructure and foreign government control. Most recently, in 2018, in response to growing concerns over investments from the People's Republic of China in high-technology sectors and other market segments that pose significant risks to U.S. national security and important supply chains, Congress significantly expanded CFIUS's jurisdiction and operational mandate by passing the Foreign Investment Risk Review Modernization Act (FIRRMA). FIRRMA was constructed to reach a broader range of foreign direct investments and real estate transactions and introduced mandatory filing requirements for certain types of transactions.

Composition of CFIUS

CFIUS is chaired by the U.S. Department of the Treasury (Treasury). Additional members include the Departments of Commerce, Defense, Energy, Homeland Security, Justice, Labor, and State; and the Offices of the Director of National Intelligence (DNI), the U.S. Trade Representative, and Science and Technology Policy.[1]

[1] The DNI and the Secretary of Labor are ex-officio, non-voting members of CFIUS.

In addition, the Council of Economic Advisors, National Security Council, National Economic Council, Homeland Security Council, and Office of Management and Budget observe and, where appropriate, participate in CFIUS review activities. CFIUS may consult other agencies with appropriate expertise, as necessary.

What Does CFIUS Do?

CFIUS reviews "covered transactions" and "covered real estate transactions" to determine whether they pose risks to the national security interests of the United States. CFIUS is also authorized to mitigate risks that arise from such transactions and recommend action by the President.

Under FIRRMA's predecessor FINSA, the scope of CFIUS review was limited to investments that could result in "control" of a U.S. business[2] by a foreign person, i.e., the foreign acquirer. FIRRMA, however, expanded CFIUS's jurisdiction to include certain non-controlling, non-passive investments in Critical **T**echnology, Critical **I**nfrastructure, and Sensitive Personal **D**ata (TID) U.S. businesses, as well as certain real estate transactions.

FIRRMA further provided for mandatory CFIUS filings that are now required for two broad categories of transactions: (1) covered transactions involving critical technologies if a "U.S. regulatory authorization" under export control laws is required to export, reexport, transfer (in-country), or retransfer the TID U.S. business's technologies to the foreign acquirer, and (2) covered transactions involving the acquisition of a "substantial interest" in a TID U.S. business by a foreign person in which a foreign government holds a "substantial interest."

CFIUS now has authority to review certain non-controlling investments in Technology, Infrastructure, and Data businesses and certain real estate transactions.

Mandatory filings are now required for certain investments in critical technology businesses as well as certain transactions involving foreign government ownership.

What Does the U.S. Government Consider National Security?

CFIUS focuses on addressing "national security" issues when reviewing proposed transactions. While the CFIUS regulations do not define the term "national security" and CFIUS reviews can span transactions across a broad range of industries, there are certain legal and policy factors that CFIUS considers in evaluating whether a proposed foreign investment could affect U.S. national security interests. The Committee's analysis includes the assessment of

[2] CFIUS defines "U.S. business" as "any entity, irrespective of the nationality of the persons that control it, engaged in interstate commerce in the United States."

the following non-exhaustive factors when evaluating national security risks:

- Domestic production (including supply chains) needed for national defense;
- U.S. critical and emerging technologies;
- Long-term requirements for energy and other critical resources;
- Critical infrastructure, such as major energy assets; and
- Control of a U.S. business by a foreign government.

Many CFIUS cases also involve other factors considered relevant to national security, including:

- Classified defense or homeland security-related contracts;
- Sole-source contracts with federal, state, or local governments; and
- Export control restrictions.

Most recently, FIRRMA instructed CFIUS to consider:

- Involvement of a country of special concern;
- Patterns of acquisitions by a foreign country or person in particular assets or technologies;
- Parties' history of compliance with U.S. laws and regulations;
- Control of U.S. industries as it affects the capacity of the United States to meet the requirements of national security;
- Access to sensitive personal data of U.S. citizens, which includes certain "identifiable data" and genetic information;
- Acquisition of certain rights with respect to real estate in close proximity to sensitive U.S. government (USG) facilities; and
- Cybersecurity vulnerabilities.

CFIUS has reviewed transactions in the following industries, among many others:

- Aerospace and Defense
- Chemicals
- Energy
- Engineering
- Health care, medical services
- Information and Advanced Technologies
- Insurance and Financial Services
- Logistics
- Social Media and Mobile Applications
- Software
- Telecommunications
- Travel and Tourism

Expanded Jurisdiction for TID Investments

As noted above, FIRRMA expanded CFIUS's jurisdiction over transactions that involve TID U.S. business investments – i.e., investments that involve critical technologies, critical infrastructure and/or sensitive personal data. Under the regulations implementing FIRRMA, CFIUS filings are mandatory for certain investments involving TID U.S. businesses.

Critical Technologies

FIRRMA defines "critical technologies" to include:

- **Defense articles or services included on the United States Munitions List (USML)** set forth in the International Traffic in Arms Regulations (ITAR);
- **Certain items included on the Commerce Control List (CCL)** set forth in the Export Administration Regulations (EAR), including emerging and foundational technologies controlled pursuant to Section 1758 of the Export Control Reform Act of 2018 (ECRA);
- **Nuclear equipment,** parts and components, materials, software, and technology covered by 10 CFR Part 810 (relating to assistance to foreign atomic energy activities);

- **Nuclear facilities,** equipment, and material covered by 10 CFR Part 110 (relating to export and import of nuclear equipment and material); and
- **Select agents and toxins** covered by 7 CFR Part 331, 9 CFR Part 121, or 42 CFR Part 73.

Critical Infrastructure

The CFIUS regulations define "critical infrastructure" as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security." Such assets include the following:

- IP networks;
- Telecommunications and information services;
- Submarine cable systems and facilities;
- Electricity, oil, and gas facilities;
- Data centers;
- Satellite systems; and
- Airports and maritime ports.

Sensitive Personal Data

The regulations implementing FIRRMA define "sensitive personal data" to include certain identifiable data and genetic information. "Identifiable data" refers to "data that can be used to distinguish or trace an individual's identity," and is treated as "sensitive personal data," for example, when it is maintained or collected by a U.S. business that targets or tailors products or services to any U.S. Executive branch agency or the U.S. business has maintained or collected data on more than 1 million individuals. The regulations identify 10 categories of identifiable data that may be sensitive personal data, including:

- Financial data that could be used to analyze or determine an individual's financial distress;
- Data in an application for health insurance;
- Non-public electronic communications;
- Geolocation data; and
- Biometric enrollment data, including facial, voice, retina/iris, and palm/fingerprint templates.

How Does the CFIUS Review Process Work?

The CFIUS review process typically begins when the parties to a transaction file either a **notice** or a **declaration** with Treasury. Declarations require less information and are subject to a relatively shorter assessment period as compared to notices, but they frequently do not provide the parties with as much deal certainty as would be obtained through filing a more comprehensive notice. In some cases, a declaration may not provide CFIUS with enough information to enable the Committee to fully evaluate the transaction. In other cases, CFIUS may need additional time to review the transaction, consider potential mitigation, or assess other appropriate actions to address national security concerns. In these cases, CFIUS may not be able to clear the transaction through the declaration process.

Notices

A notice provides more detailed information regarding the nature of the transaction, the parties to the transaction, the U.S. business and activities at issue, and the subsequent foreign ownership/control of the U.S. business. Prior to filing a formal notice with CFIUS, parties to a transaction have the option of submitting a draft or "pre-filed" notice, which enables the Committee to review the specific details of the transaction before initiating the formal review period. While the submission of a pre-filed notice is voluntary, doing so has become standard practice as it allows parties to address upfront questions or concerns from CFIUS prior to filing a formal notice.

Once a formal filing is submitted to CFIUS, Treasury determines whether the filing contains

all of the required information and, if so, the agency circulates the filing to other CFIUS members, beginning a **45-day national security review** period. During this period, Treasury assigns a "lead agency" (or agencies) to the case and may request additional information from the filing parties. The parties are generally required to provide requested information within three business days. On day 30 of a review, the DNI provides CFIUS agencies with a threat assessment identifying issues that could pose a threat to the national security of the United States as a result of the transaction.

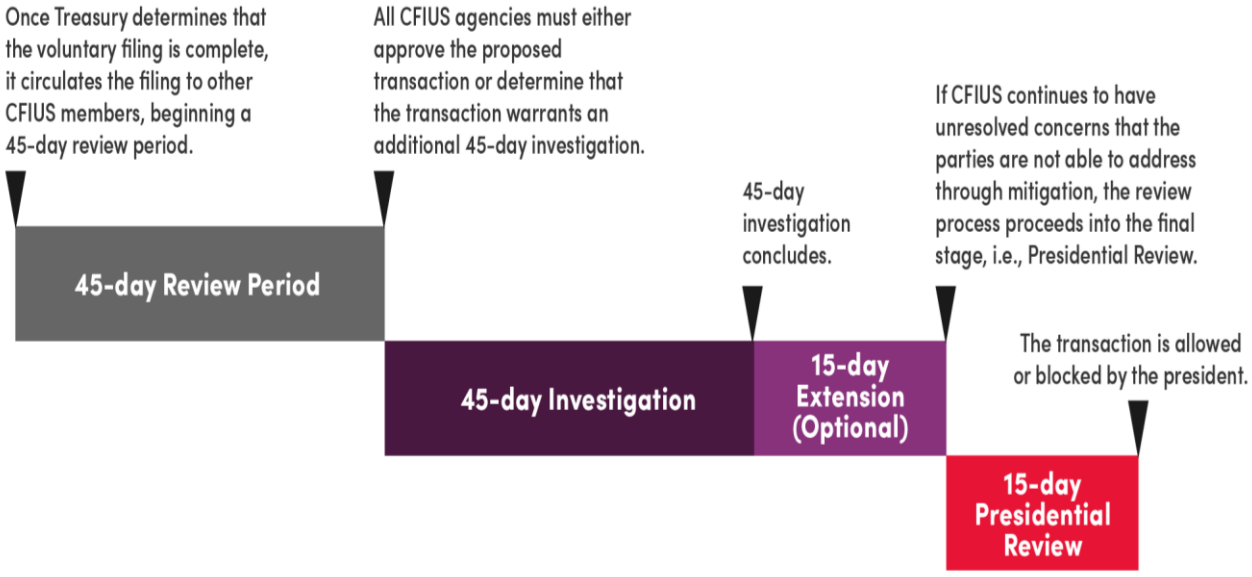
After the 45-day review period, CFIUS member agencies must either approve the proposed transaction or determine that the transaction warrants an additional 45-day period for an investigation. Any CFIUS member agency may request an investigation. Although some transactions receive approval within the review period, more complicated transactions and those involving foreign government control, critical infrastructure, critical technology, or sensitive personal data typically proceed to the 45-day investigation period. In "extraordinary circumstances," CFIUS may extend an investigation by 15 days.

If, after the 45-day investigation period, CFIUS has concerns that have not been or cannot be mitigated (see below), the process proceeds to the final stage, i.e., **Presidential Review**, in which CFIUS sends a report of the transaction and associated national security risks to the President for consideration. Within 15 days, the President must decide whether to allow the transaction to proceed, block the transaction from going forward, or take other action.

If CFIUS requires additional time to complete its review, the Committee may allow the parties to withdraw their notice prior to a final decision and subsequently refile. CFIUS allows for withdrawals and refilings to afford the Committee additional time to review the transaction and, if necessary, mitigate concerns over national security or allow the parties time to provide additional information or restructure the problematic elements of the proposed transaction. The withdrawal and refiling of a notice starts a new CFIUS review clock.

Declarations

In lieu of filing a detailed written notice with the Committee, parties may opt instead to submit a short-form **declaration**, which provides basic



information regarding the transaction and the parties involved.

Within 30 days of accepting a declaration, CFIUS will either: (1) request that the parties file a written notice; (2) inform the parties that the Committee is unable to complete action with respect to the transaction on the basis of the declaration alone; (3) unilaterally initiate a review of the transaction; or (4) notify the parties in writing that the Committee has completed all action with respect to the transaction.

The primary advantages of filing a declaration in lieu of a notice are that a declaration is less burdensome to prepare, does not require payment of a filing fee, and is subject to a comparatively shorter assessment period by CFIUS. The primary disadvantages of filing a declaration are that CFIUS is not required to make a final determination on a declaration, and this could delay the closing of the transaction if a notice turns out to be required or necessary to obtain USG approval for the transaction.

It is important to note that all information submitted to CFIUS is confidential. Confidentiality covers information submitted to CFIUS when parties engage in pre-filing consultations (even if a final notice is not ultimately submitted) and continues after CFIUS concludes its review/investigation process. Information and documentary material filed with CFIUS are also exempt from disclosure under the Freedom of Information Act (FOIA). However, CFIUS now permits the disclosure of certain confidential information to allied foreign governments for national security purposes.

Who Should File and When?

CFIUS has jurisdiction to review foreign investments across three categories of transactions: controlling transactions; certain non-controlling, non-passive investments; and certain real estate transactions. As noted above, CFIUS filings are also mandatory for certain investments in critical technology firms and transactions resulting in a substantial foreign government interest in a TID U.S. business.

Covered Control Transactions. Prior to FIRRMA, CFIUS was essentially a voluntary process[3] and the Committee's authority was limited to reviewing transactions that could result in foreign control of a U.S. business. Under FIRRMA, CFIUS retains its traditional authority to review transactions within the foreign control category, but the process is no longer voluntary for parties to certain control transactions. "Covered control transaction" is defined as any transaction by or with any foreign person that could result in foreign control of any U.S. business, including such a transaction carried out through a joint venture.

Covered Investments. The Committee also has jurisdiction over certain non-controlling, non-passive investments in TID U.S. businesses. Non-controlling foreign investments in TID U.S. businesses covered under the FIRRMA-implementing regulations include those in which the foreign investor acquires an equity interest that also affords the foreign person any of the following rights:

- Access to any material nonpublic technical information in the possession of the TID U.S. business;
- Membership or observer rights on the board of directors or equivalent governing body of the TID U.S. business, or the right to nominate an individual to a position on the board of directors or equivalent governing body; or
- Any involvement, other than through voting of shares, in substantive decision-making of the TID U.S. business regarding:
  - The use, development, acquisition, safekeeping, or release of sensitive personal

[3] CFIUS had and still has the ability to request that parties file or unilaterally initiate a case on its own motion.

data of U.S. citizens maintained or collected by the TID U.S. business;

- The use, development, acquisition, or release of critical technologies; or
- The management, operation, manufacture, or supply of certain critical infrastructure.

"TID U.S. businesses" subject to these provisions include the following:

- Any U.S. business that produces, designs, tests, manufactures, fabricates, or develops one or more critical technologies;
- Any U.S. business that owns, operates, manufactures, supplies, or services certain critical infrastructure; and
- Any U.S. business that maintains or collects, directly or indirectly, sensitive personal data of U.S. citizens.

The regulations clarify that an indirect investment by a foreign person in a TID U.S. business through an **investment fund** that affords the foreign person membership as a limited partner or equivalent on an advisory board or a committee of the fund will not be considered a covered investment with respect to the foreign person if the following criteria are met:

- The fund is managed exclusively by a general partner, a managing member, or an equivalent;
- The general partner, managing member, or equivalent of the fund is not a foreign person;
- The advisory board or committee does not have the ability to approve, disapprove, or otherwise control:
  - (i) investment decisions of the investment fund; or
  - (ii) decisions made by the general partner, managing member, or equivalent related to entities in which the investment fund is invested;
- The foreign person does not otherwise have the ability to control the investment fund, including, without limitation, the authority:
  - to approve, disapprove, or otherwise control investment decisions of the investment fund;
  - to approve, disapprove, or otherwise control decisions made by the general partner, managing member, or equivalent related to entities in which the investment fund is invested; or
  - to unilaterally dismiss, prevent the dismissal of, select, or determine the compensation of the general partner, managing member, or equivalent;
- The foreign person does not have access to material nonpublic technical information as a result of its participation on the advisory board or committee; **and**
- The investment does not afford the foreign person any of the access, rights, or involvement specified in the definition of "covered investment."

Mandatory Declarations. Subject to certain exceptions, covered transactions involving U.S. critical technology companies and covered transactions that involve foreign government acquisitions of a "substantial interest" in a TID U.S. business are subject to mandatory filing requirements.

CFIUS filings are required for covered transactions involving critical technologies if a "U.S. regulatory authorization" would be required to export, reexport, transfer (in-country), or retransfer the TID U.S. business's critical technologies to the foreign person involved in the transaction or to certain foreign persons in the ownership chain.

The regulations implementing FIRRMA also establish a mandatory filing requirement for certain investments involving the acquisition of a "substantial interest" in a TID U.S. business (defined as a direct or indirect voting interest of at least 25%) by a foreign person in which a

foreign government holds a "substantial interest" (defined as a direct or indirect voting interest of at least 49%).

Additionally, the regulations clarify that in determining whether a foreign government holds a "substantial interest" in an **investment fund** context, the Committee will look only at a foreign government's interest in the general partner (or equivalent) because that is the entity typically responsible for the day-to-day decision-making of the investment fund.

Real Estate Transactions. In addition to covered transactions involving U.S. businesses, CFIUS also has jurisdiction to review certain real estate transactions involving foreign persons when the U.S. real estate is either (1) located within, or will function as part of, an airport or maritime port, or (2) located in close proximity to a U.S. military installation or another USG facility or property that is sensitive for reasons relating to national security. The transaction must afford the foreign person certain property rights in order to be covered.

Although CFIUS had previously reviewed and blocked certain transactions involving real estate even prior to the enactment of FIRRMA, those transactions also involved the acquisition of foreign control over an existing U.S. business. In contrast, FIRRMA expanded the Committee's jurisdiction to allow CFIUS to review real estate transactions even when they do not also involve a foreign investment in a U.S. business. This is another noteworthy example of FIRRMA's broader reach.

Timing. CFIUS has the authority to review a covered transaction at any time, even after the transaction has concluded. CFIUS can also impose mitigation remedies, including (in rare cases) suspending a proposed or pending transaction. Thus, parties to a covered transaction with the potential to raise national security concerns are generally advised to submit a filing with CFIUS prior to closing the transaction. Parties to such transactions often make CFIUS clearance a condition to closing in the deal documents. Failure to file either a short-form declaration or a full CFIUS notice at least **30 days prior to closing** a transaction, when the transaction is subject to a mandatory CFIUS filing requirement, could also result in civil monetary penalties up to the value of the transaction.

What Actions May CFIUS Take?

CFIUS can take several actions after it reviews a filing. First, CFIUS may reject a filing if (1) it is incomplete; (2) the parties do not provide additional information when requested to do so; (3) there is a material change in the transaction; or (4) CFIUS learns information that contradicts information provided in the filing. This leaves parties with no safe harbor for completing the transaction, and CFIUS may recommend that the President prohibit or unwind the transaction if it determines that an unmitigable risk to national security exists.

Second, to the extent that the proposed transaction does not pose a national security risk, or if CFIUS believes that other U.S. laws are able to adequately address such risks, CFIUS will provide the parties with written confirmation that it has concluded all action with respect to the transaction (i.e., its examination and any mitigation measures). The transaction will obtain safe harbor from further CFIUS review but may nevertheless be subject to other U.S. legal authorities that regulate the activities of the business or parties.

Third, in the course of its review or investigation, CFIUS may require that the parties enter into a mitigation agreement with the government to address any national security concerns posed by the transaction. Mitigation measures may include, but are not limited to, any of the following:

- Establishing a corporate security committee, security officers, and/or other mechanisms to ensure compliance with required actions,

including annual reports and independent audits;

- Ensuring compliance with established guidelines and terms for handling existing or future U.S. government (USG) contracts and USG customer information;
- Requiring that only U.S. persons handle certain products and services, and ensuring that certain activities and products are located only in the United States;
- Limiting foreign access to certain corporate information or technology;
- Notifying relevant USG entities in advance of foreign national visits to the U.S. business;
- Notifying relevant USG parties of any material introduction, modification, or discontinuation of a product or service, as well as any awareness of any vulnerability or security incidents;
- Ensuring continued production of certain products for relevant USG parties for specified periods; and
- Requiring a proxy entity to perform certain functions and activities of the U.S. business.

CFIUS may impose interim mitigation measures and may even suspend a transaction while conducting its review. Whenever mitigation measures are imposed, the Committee must formulate plans to monitor parties' compliance with the terms of the mitigation agreement.

Finally, CFIUS may recommend that the President prohibit (or block) a transaction that poses a national security risk when the risk cannot be resolved through mitigation or other existing U.S. laws, and when parties will not agree to abandon the transaction. The President also has the authority to unwind a transaction that has been completed prior to CFIUS review. CFIUS may also recommend that the President take other action to address national security risks.

After the review process concludes, CFIUS maintains an ongoing role in supervising parties' compliance with any mitigation agreement. FIRRMA also allows CFIUS to enter into and impose mitigation and conditions in cases where parties to a covered transaction have voluntarily chosen to abandon the transaction and in cases where a transaction has already been completed. Furthermore, CFIUS has recently imposed penalties for breach of mitigation terms and maintains the authority to unilaterally initiate a review of a previously reviewed transaction if the parties materially breach a mitigation agreement or condition, regardless of whether the breach was intentional.

What Are the Key Considerations for Navigating a CFIUS Review?

Early Engagement. CFIUS encourages parties to begin informal consultations and submit a draft filing before officially requesting a review. Early engagement gives parties a clearer sense of whether their transaction would fall under CFIUS's jurisdiction, and it gives parties a better understanding of the information CFIUS needs and any concerns it may have prior to filing a case. Doing so also provides CFIUS with additional time to work through issues, which may allow an otherwise complicated transaction to be cleared expeditiously.

Preparation. Because CFIUS reviews are focused on national security considerations, parties should be well-prepared to address all potential national security issues that could arise as a result of a transaction, including threats posed by the foreign investor and vulnerabilities associated with the U.S. business being acquired by a foreign entity.

Mitigation. As discussed in greater detail above, CFIUS is authorized to impose and enforce agreements or conditions to mitigate any national security risks posed by a transaction. As a result, parties entering the

CFIUS process should be prepared for the possibility of mitigation measures and consider the impact of mitigation agreements on their businesses going forward. As a result, it is generally prudent for parties to include provisions in their deal documents addressing the handling of potential mitigation measures.

Filing Fees. In July 2020, pursuant to FIRRMA, Treasury issued a final rule establishing a fee schedule for parties filing a formal written notice of a transaction for review by CFIUS. The fee amount is based on the value of the transaction and generally must be paid before CFIUS will initiate a review. The current fees are set as follows:

Transaction Value	Fee Amount
$0 to $499,999.99	$0
$500,000 to $4,999,999.99	$750
$5,000,000 to $49,999,999.99	$7,500
$50,000,000 to $249,999,999.99	$75,000
$250,000,000 to $749,999,999.99	$150,000
$750,000,000 +	$300,000

Filing fees are not required for declarations.

Mandatory Filings. As discussed above, parties are required to submit a CFIUS filing (declaration or notice) for certain transactions. These include certain investments in critical technology companies where the target U.S. company would need U.S. regulatory authorization (e.g., EAR export license) to export its technology to certain transaction parties, or certain investments resulting in a foreign government acquiring a substantial interest in a TID U.S. business.

Excepted Investors. Investments by certain foreign persons are excluded from the definition of "covered investment" and therefore may not be subject to the mandatory filing requirements depending on the facts and circumstances of the particular case. Excepted investors include nationals of and other foreign persons with strong ties to an "excepted foreign state." "Excepted foreign states" include any foreign state that the Committee has determined "has established and is effectively utilizing a robust process to analyze foreign investments for national security risks and to facilitate coordination with the United States on matters relating to investment security." At present, the excepted foreign states are Australia, Canada, and the United Kingdom. CFIUS may identify additional countries as excepted foreign states in the future.

Foreign Government Control. The CFIUS-authorizing statute presumes a 45-day investigation period for all acquisitions resulting in foreign government control of a U.S. business, such as investments by state-owned entities and sovereign wealth funds. However, such cases may close during the preceding 45-day review period with express approval from the Secretary or Deputy Secretary of the Treasury and the "lead agency" (or agencies) on the case.

Public Affairs and Press Strategy. It is important to underscore that CFIUS filings and the identity of parties are not public information. Nevertheless, parties may wish to make certain details of their transaction public. Alternatively, in certain cases, information about transactions will be made public out of necessity or a legal proceeding (e.g., a transaction involving a publicly traded company or a bankruptcy proceeding). In these cases, even though CFIUS conducts its examination of transactions without public input or participation, public opinion may play an important role in determining the fate of a proposed transaction. Particularly in high-profile cases, it may be important for parties to a transaction to maintain and execute a public affairs and press strategy that includes media, public, and congressional outreach.

What Is the Role of Congress?

CFIUS laws and regulations provide a limited oversight role for Congress. Although Congress does not participate in the CFIUS review process, specific congressional committees have some oversight role and may require CFIUS to provide certain details or statistics on transactions to Congress, including information regarding the parties, all of which must be protected by Congress. Further, CFIUS reports certain transactions that it reviews to members of Congress through a congressional notification or certification process, which relays the outcome of the case. However, for certain transactions that have political implications, it may be prudent for the parties to brief Members of Congress on the proposed deal before or during the CFIUS review process.

Recent CFIUS Activity

The White House and Congress have sought to heighten scrutiny of various types of foreign investments to address a range of national security concerns. CFIUS plays a leading role in this effort as it regulates the types of foreign investments described here. The most recent publicly available data indicate that the Committee received 231 notices in 2019, and we understand that CFIUS likely received over 130 declarations and nearly 200 notices in 2020. With the introduction of mandatory declarations and notices under FIRRMA, these numbers are likely to increase in the coming years.

It is important that companies be prepared to successfully navigate the CFIUS process. Complications resulting from CFIUS reviews have caused parties to walk away from dozens of investments, and Presidents have formally blocked or unwound seven foreign investments – five of them since 2016 alone.

Recent decisions following Presidential Review include:

- **August 14, 2020:** President Trump ordered ByteDance to divest all interests and rights in any tangible or intangible assets or property used to enable or support ByteDance's operation of the TikTok app in the United States as well as any data obtained or derived from TikTok app users in the United States. The divestiture order is currently being litigated, and President Biden may ultimately adopt alternative means for addressing U.S. national security concerns in connection with ByteDance's operation of the TikTok app.
- **March 6, 2020:** President Trump ordered Beijing Shiji Information Technology Co. to unwind its 2018 acquisition of the American hotel property management software company StayNTouch, Inc. In addition, the Executive Order directed Shiji and its affiliates to immediately refrain from accessing StayNTouch's hotel guest data.
- **March 12, 2018:** President Trump blocked Broadcom Ltd., a then-Singapore-based company in the process of re-domiciling in the United States, from pursuing a hostile takeover of Qualcomm Inc. over concerns related to the development of 5G mobile communications technology.
- **September 13, 2017:** President Trump halted the acquisition of Lattice Semiconductor Corporation, a U.S. chipmaker, by Canyon Bridge Capital Partners, a U.S. private equity firm with a Chinese state-owned limited partner.
- **December 2, 2016:** President Obama blocked the acquisition of Aixtron SE, a German semiconductor chip supplier with a California-based subsidiary, by Fujian Grand Chip Investment Fund LP, a Chinese investor, citing national security risks.
- **September 28, 2012:** President Obama blocked a transaction involving the acquisition of wind farm project firms by Chinese-owned Ralls Corporation, due in

part to the proximity of the wind towers to a sensitive U.S. military installation. As a result, Ralls was forced to divest its ownership interest in the project.

The Committee normally directs parties to abandon or unwind a transaction before reaching the Presidential Review stage. A recent high-profile example of this is CFIUS's recommendation that Chinese gaming company Kunlun Tech Co., Ltd. sell Grindr LLC, a social networking app company. Kunlun became Grindr's majority stakeholder in 2016 and then acquired the remaining stake in 2018. Kunlun did not seek CFIUS approval for either transaction. In March 2019, CFIUS directed Kunlun to sell Grindr based on national security risks posed by Kunlun's access to sensitive personal data.

Another example is CFIUS's August 2018 request that the Chinese conglomerate HNA Group Co., Ltd., sell its ownership stake in a Manhattan skyscraper. HNA Group indicated that the U.S. national security concerns arose due to the location of the property. The property's tenants included a New York Police Department precinct responsible for security at the nearby Trump Tower. At the Committee's direction, HNA Group transferred its stake in the building to a blind trust with an independent board of directors with the assets ultimately sold to U.S. purchasers.

CFIUS Overview for Government Contractors

Federal government contractors have an increased risk of being subject to CFIUS review because they may be involved in work that is considered particularly sensitive and more likely to raise potential national security concerns. CFIUS has historically noted that a significant number of transactions reviewed by CFIUS presenting national security considerations "involve foreign control of U.S businesses that provide products and services – either as prime contractors or as subcontractors or suppliers to prime contractors – to agencies of the U.S. government and state and local authorities, including, but not limited to, sole-source arrangements." This, of course, includes any federal contracts that support national security activities, homeland security, public health and safety, critical infrastructure, or technologies that are considered essential for maintaining or increasing U.S. leadership.

What Does the CFIUS Review Process Entail for Government Contractors? If a transaction involving a federal contractor is subject to CFIUS review, the Committee will assess potential risks to national security by examining, among other factors: (1) the background and business dealings of the foreign party and the contractor (which may include sensitive information about each entity's management structure and executive leadership), (2) the foreign party's interest in acquiring or investing in the U.S.-based contractor, in particular, whether the foreign party will be able to exercise control over the U.S. company (which may include not only the ownership share, but also rights and authorities of minority shareholders), (3) the federal contracts that the company has previously performed and any current contracts, including the federal agencies that awarded or were otherwise involved with the contracts, and (4) whether the federal contracts are priority-rated, classified, or subject to export controls.

Government Contractor CFIUS Business Planning. Companies performing under USG contracts should note that potential foreign investments could be subject to CFIUS jurisdiction, even when the investments originate from allied countries. Of primary concern for CFIUS is the degree of control a foreign party may have over a U.S.-based contractor and the nature of the products or services the contractor provides to the USG.

Several issues should be factored into the structure of any deal that involves foreign investments in a business that serves as a federal government contractor. More specifically, measures imposed by CFIUS on the business, including through mitigation agreements, have the potential to impact a contractor's day-to-day operations, and could result in additional costs to the business. Contractors should also keep in mind that many government contracts have notice requirements that require the business to notify the agency of any material change in operations and seek the contracting agency's authorization to ensure that the business is able to fully perform under its contract.

What Is Wiley's CFIUS Experience?

Wiley has unparalleled experience counseling clients in transactions that involve every industry sector subject to CFIUS review. We have substantial expertise assisting parties with transactions that involve sophisticated technology and classified information. Our work includes the negotiation of national security, proxy, and special security agreements. We advise clients on strategies to mitigate national security risks and to address political and public relations issues at the national and local levels.

Our attorneys and consultants have served in nearly every CFIUS department, including the U.S. Departments of Treasury, Homeland Security, Justice, Defense, Commerce, and State, as well as the National Security Council. The firm has long-standing relationships with Members of Congress and Executive branch officials, and we have worked directly with congressional committee staff and Members of Congress to review and explain potentially sensitive transactions.

Our team of legal and policy experts includes several former government professionals who understand the inner workings of CFIUS – including a unanimously Senate confirmed Assistant Secretary for Industry and Analysis at the U.S. Department of Commerce's International Trade Administration, and the former U.S. Treasury Deputy Assistant Secretary for Investment Security and Policy.

Senior Public Policy Advisor **Nova J. Daly** joined Wiley after serving as the Deputy Assistant Secretary for Investment Security and Policy at Treasury from 2006 to 2009. In that capacity, he ran the CFIUS process, oversaw the reviews of over 350 cases, negotiated new CFIUS law, and was responsible for the development, coordination, and implementation of new CFIUS regulations. He also worked closely with the Trump Administration and Congress on new CFIUS law provisions in FIRRMA.

Partner **Hon. Nazak Nikakhtar**, Co-Chair of the National Security practice, is a CFIUS and national security law expert and served as the U.S. Department of Commerce's lead in the government's review of CFIUS transactions from 2018 through 2021, overseeing the implementation of FIRRMA and leading the decision-making on approximately 700 cases, including non-notified transactions and complex mitigation agreements.

Partner **Kendra P. Norwood** represents government contractors, subcontractors, and grant recipients on a range of legal issues and handles bid protests before multiple federal government agencies. Prior to joining Wiley, Kendra spent more than ten years at the National Aeronautics and Space Administration (NASA).

Of Counsel **Daniel P. Brooks** represents clients before CFIUS, the Federal Communications Commission, and the U.S. Treasury, State, Commerce, and Defense Departments on a wide range of national security, telecommunications, economic sanctions, and export control issues.

Wiley's CFIUS and National Security Practice is complemented by the expertise of attorneys, advisors, and economists throughout Wiley's other practice groups including Government

Contracts, Export Controls, Telecommunications, Cybersecurity, Digital Trade, Economic Sanctions/Office of Foreign Assets Control, Foreign Corrupt Practices Act, and Corporate – and is further bolstered by a host of specialized practice experience in defense, telecommunications, satellite technology, and other sectors.

Contact Us

Nova J. Daly
Co-Lead, CFIUS
202.719.3282
NDaly@wiley.law

Hon. Nazak Nikakhtar Co-Chair, National Security
202.719.3380
NNikakhtar@wiley.law

Kendra P. Norwood
Partner, Government Contracts
202.719.7069
KNorwood@wiley.law

Daniel P. Brooks
Of Counsel, National Security
202.719.4183
DBrooks@wiley.law

wiley.law