Buchanan

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

By Daniel B. Pickard, Shareholder, Chair,
International Trade & National Security Practice Group
Keil Ritterpusch, Shareholder
Jordan Yeagley, Counsel
Milton Koch, International Trade Advisor

April 2025

TABLE OF CONTENTS

Charged with addressing the potential national security impacts of foreign direct investment in the United States, the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee") is an interagency committee whose mission is reviewing and addressing U.S. national security risks associated with certain foreign investments while, at the same time, balancing the need for open investment.

Established in 1975, CFIUS was initially charged with monitoring the potential national security impact of foreign investments but had no explicit authority to regulate or block transactions, which the Committee viewed as potentially problematic. In 1988, in response to concerns that U.S. technological leadership could be jeopardized by foreign investment, Congress passed the Exon-Florio Amendment. The Exon-Florio Amendment granted the President authority to suspend or prohibit proposed transactions submitted to CFIUS that, in the view of the Committee and President, posed a threat to U.S. national security.

In 2007, Congress once again expanded the Committee's jurisdiction and scope of review through the passage of the Foreign Investment and National Security Act (FINSA). The new law created additional CFIUS filing requirements and broader review considerations focused primarily on proposed transactions impacting critical infrastructure of the United States and resulting in foreign government control. Then, in 2018, in response to growing concerns over the People's Republic of China's significant investment in high-technology sectors and growing influence over the U.S. supply chain, Congress passed the Foreign Investment Risk Review Modernization Act (FIRRMA). FIRRMA expanded the scope of CFIUS review to include a broader range of foreign investment in the United States, including investment in U.S. real estate transactions, and introduced mandatory filing requirements for parties involved in certain types of proposed transactions.

CFIUS MEMBER AGENCIES

CFIUS Member Agencies

Chaired by the U.S. Department of the Treasury, CFIUS member agencies include:

- Department of Commerce
- Department of Defense
- Department of Energy
- Department of Homeland Security
- Department of Justice
- Department of State
- Office of the U.S. Trade Representative
- Office of Science and Technology Policy, Executive Office of the President
- Department of Labor (Ex-Officio)
- Office of the Director of National Intelligence (Ex-Officio)
- Office of Management and Budget (Observer)
- Council of Economic Advisors (Observer)
- National Security Council (Observer)
- Homeland Security Council (Observer)

In addition to these member agencies, other federal agencies (e.g., Department of Health and Human Services, Department of Transportation) may participate in a CFIUS review of the national security impact of a "covered transaction," as needed. As part of the Consolidated Appropriations Act of 2024, Congress included the Department of Agriculture as a member agency of the Committee on an as needed basis to assist in reviewing certain transactions involving agricultural equities.

CFIUS: DIRECTIVE AND JURISDICTION

In broad terms, CFIUS is charged with reviewing certain "covered transactions" and "covered real estate transactions" involving foreign direct investment in the United States to ensure that the national security interests of the United States are maintained and supported. Where national security risks are identified as they relate to a particular proposed transaction, CFIUS is authorized to institute certain mitigation measures relative to such risks and recommend actions to be taken by the President.

In order to mitigate national security risks arising from foreign direct investment, CFIUS is authorized by FINSA and FIRRMA to review not only those proposed transactions which result in "control" of a U.S. business by a foreign acquirer, but also non-controlling investments in critical technology, critical infrastructure and sensitive personal data. Transactions involving Critical Technology, Critical Infrastructure and U.S. businesses maintaining Sensitive Personal Data are known as "TID transactions."

In addition to expanding the scope of transactions subject to the Committee's jurisdiction, FIRRMA mandated CFIUS filings for two broad categories of transactions, including: (1) transactions involving technologies where "U.S. regulatory authorization" is

required under the U.S. export control laws and (2) transactions involving the acquisition of a "substantial interest" in a U.S. TID business by a foreign person over which a foreign government maintains a "substantial interest."

NATIONAL SECURITY FACTORS CONSIDERED BY CFIUS

Section 721(f) of the Defense Production Act (DPA), as amended by FINSA, provides illustrative examples of the factors to be considered by CFIUS in determining whether a proposed transaction poses a national security risk, including:

- The potential effects of the transaction on the capability and production capacity of domestic industries to meet national defense requirements, including the availability of human resources, products, technology, materials, and other supplies and services;
- 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;
- The potential effects of the proposed or pending transaction on sales of military goods, equipment, or technology;
- The potential national security-related effects on U.S. technological leadership;
- The potential national security-related effects on U.S. critical technology;
- The potential national security-related effects of the transaction on U.S. critical infrastructure, including major energy assets;
- The potential that the transaction presents for transshipment or diversion of technologies with military applications, including an analysis of national export control laws and regulations; and,
- Such other factors as the President or the Committee may determine to be appropriate, either generally or in connection with a specific review or investigation.

FIRRMA further expanded the factors to be considered by CFIUS in determining the national security risks of a proposed transaction, including:

- Whether a covered transaction involves a country of special concern that has a demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure that would affect U.S. leadership in areas related to national security;
- The cumulative control of, or patterns of recent transactions involving, any one type of critical infrastructure, energy asset, critical material, or critical technology by a foreign government or foreign person;
- Whether the control of U.S. industries and commercial activity by foreign persons would

affect the capability or capacity of the United States to meet the requirements of national security, including the continued production in the United States of items that are likely to be acquired by the Department of Defense or other Federal departments or agencies for the advancement of the national security of the United States;

- The extent to which a covered transaction is likely to expose sensitive data of U.S. citizens to access by a foreign government or person that may exploit that information in a manner that threatens national security; and,
- Whether a covered transaction is likely to have the effect of exacerbating or creating new cybersecurity vulnerability in the United States.

Additionally, on September 15, 2022, the Biden administration issued a presidential directive (EO 14083) identifying additional national security factors to be considered by CFIUS in determining the national security risks of any particular transaction, including:

- Whether the proposed transaction would undermine supply chain resiliency efforts and, therefore, national security by making the United States vulnerable to future supply chain disruptions;
- Whether "relevant third-party ties" of the foreign acquirer and/or whether any proposed transaction would or could lead to future advancements in a foreign acquirer's gain in capabilities in technology sectors fundamental to U.S. technological leadership;
- Whether the proposed transaction in the context of the broader industry and whether the cumulative impact of foreign investment in a specific sector could lead to a national security risk for the United States;
- Whether the proposed foreign investment may provide the foreign acquirer or relevant third parties with access to capabilities to conduct cyber intrusions and/or pose malicious cyber security risks;
- Whether the proposed transaction would provide a foreign person with direct or indirect access to capabilities or information databases and systems, including transactions designed to undermine the protection or integrity of data in storage or databases; and
- Whether the proposed transaction would enable the re-identification or de-anonymization of what once was unidentifiable data.

CFIUS REVIEW PROCESS

When submitting a proposed transaction to CFIUS, either pursuant to a mandatory requirement or voluntary disclosure, parties must determine the appropriate and preferred form of filing.

CFIUS Declarations

A CFIUS declaration is a short form filing with the Committee that describes the contours of a proposed transaction in high-level detail. Pursuant to CFIUS regulations, parties must include in a declaration:

- Details of and contact information for the parties to the proposed transaction;
- Details of the underlying proposed transaction, including, but not limited to:
    - Description of the proposed transaction;
    - Percentage of voting and economic interests acquired; and,
    - Total value, status and source of funding for the transaction.
- Resulting interests (voting, decision-making authority, etc.) of the foreign party;
- Ownership, control and influence of any foreign persons and/or governments in the foreign acquirer; and,
- Products and services provided by the U.S. business.

While declarations require an overview of the proposed transaction (including at least the information above), declarations require less detailed information than notices (discussed below) and do not require the parties to pay a filing fee. Moreover, declarations submitted to CFIUS provide for an abbreviated process that could result in an expedited review timeline by the Committee (i.e., a 30-day assessment period, as opposed to 45-days for Notices).

Pursuant to the regulations implementing FIRRMA, certain proposed transactions require the filing of declarations, including those where a foreign government is acquiring a "substantial interest" in certain U.S. businesses and certain covered transactions that involved critical technologies.

While declarations have their advantages, CFIUS may, after reviewing a declaration, ultimately require the parties to file a notice with the Committee. Additionally, the filing of a declaration may result in the issuance of a "no action" outcome from CFIUS, leaving the parties to decide whether to move forward with the proposed transaction without the explicit approval of CFIUS and leave open the possibility of future CFIUS review.

CFIUS Notices

A CFIUS notice requires a more detailed and comprehensive submission with longer "review" and "investigation" periods. Notices submitted to CFIUS provide detailed information on the proposed transaction including, but not limited to:

- The nature of the underlying transaction;
- The parties to the transaction and their ownership/control structure;
- Information on the U.S. business and its industry and activities; and
- The foreign ownership/control of the U.S. business should the transaction be permitted to proceed.

Once it is submitted to and accepted by CFIUS, a formal notice will be distributed to each member agency, which begins the forty-five (45) day review period. Treasury will also assign a "lead agency" to shepherd the filing through its review and, where necessary, request additional information from the parties to the proposed transaction. At any time

during the course of the review, parties to the proposed transaction must respond to any follow-up requests for information from the Committee within three (3) business days.

In certain circumstances, a CFIUS member agency may initiate a subsequent investigation into the proposed transaction following the forty-five (45) day review period. For example, the Committee shall initiate an investigation of any proposed transaction where a member agency "believes that the transaction threatens to impair the national security of the United States and that the threat has not been mitigated." Investigations initiated by CFIUS must be completed within forty-five (45) days, unless extended by fifteen (15) days in "extraordinary circumstances."

Following a CFIUS investigation, the Committee will either: (1) approve the transaction, (2) require a mitigation agreement to approve the transaction, or (3) request the President make a determination with regard to the transaction. If sent to the President, a decision should be announced within fifteen (15) days of CFIUS's completion of its investigation.

Withdrawal of Declaration or Notice

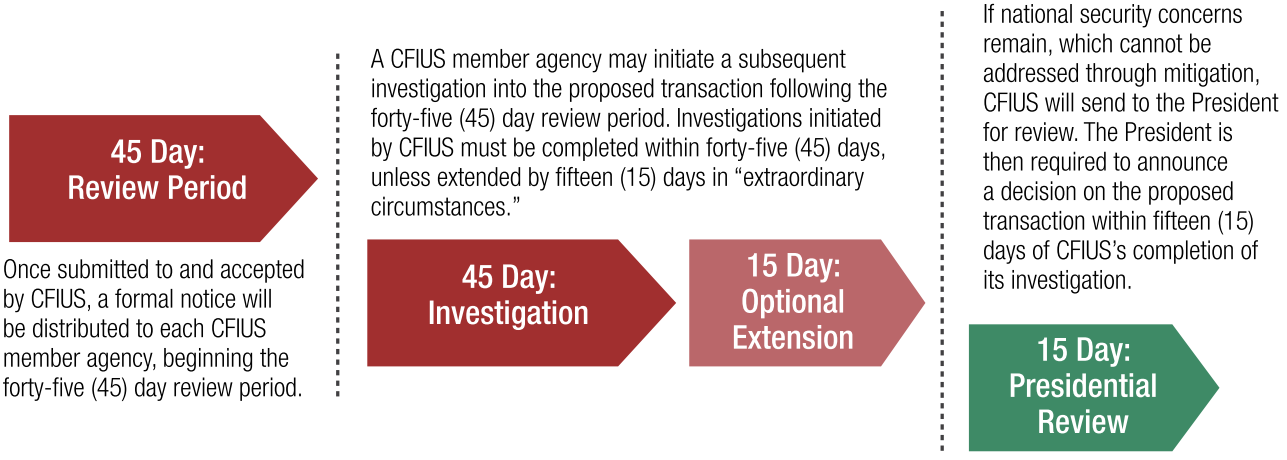
At any time during the review or investigation periods, parties to a proposed transaction may withdraw their notice or declaration. Such a request must be made in writing to CFIUS and is subject to the approval of the Committee.

Note, however, that the withdrawal of a notice or declaration does not absolve the parties of their obligations to CFIUS. The Committee, as a condition of approval of a withdrawal, may place certain conditions on the parties, including requirements that CFIUS be informed of the ongoing status of the underlying transaction and/or that a notice or declaration be re-filed at a later time. To this end, CFIUS tracks withdrawn transactions and may exercise its review obligations or enforce the condition(s) of a withdraw in the future.

Continuing Jurisdiction

CFIUS retains authority to review covered transactions regardless of whether the transaction itself has closed. Moreover, CFIUS can impose mitigation measures (described below), including suspending or blocking the proposed and/or completed transaction. As such, it is critical for parties seeking to engage in a transaction which may implicate U.S. national security to submit a filing with CFIUS prior to the closing of the transaction or risk the possibility that the transaction be unwound. Moreover, failure to file a mandatory CFIUS notice or declaration at least thirty (30) days prior to the closing of the proposed transaction could result in civil penalties up to the value of the transaction.

Timeline for CFIUS Notice



CFIUS REVIEW OF TID TRANSACTIONS

As discussed above, FIRRMA expanded the scope of CFIUS jurisdiction to include foreign investments in U.S. TID businesses, including investments that involve critical technologies, critical infrastructure and/or sensitive personal data. Under FIRRMA and its implementing regulations, CFIUS filings are mandatory for certain foreign investments in TID businesses.

Critical Technology

FIRRMA defines "critical technology" to include:

- Defense articles or services included on the U.S. Munitions List (USML), as set forth in the International Traffic in Arms Regulations (ITAR);
- Certain items included on the Commerce Control List (CCL), as set forth in the Export Administration Regulations (EAR);
- Nuclear equipment, parts and components, materials, software and technology covered by 10 CFR Part 810;
- Nuclear facilities, equipment, and materials covered by 10 CFR Part 110;
- Select agents and toxins covered by 7 CFR Part 331, 9 CFR Part 121 or 42 CFR Part 73; and,
- Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018.

Critical Infrastructure

CFIUS regulations define "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security." Such systems and assets include, but are not limited to, telecommunications, utilities, energy and transportation.

Sensitive Personal Data

"Sensitive personal data" is defined to include numerous categories of data that may be maintained or collected by U.S. businesses. These categories of data include types of financial data, globalization data and health data, among others. Moreover, a U.S. business that maintains or collects these enumerated categories of data on U.S. citizens will only be considered to have sensitive personal data to the extent it:

- Targets or tailors products or services to certain populations, including members of the U.S. military and/or employees of federal agencies with national security responsibilities;

- Collects or maintains such data on at least one million individuals; or,
- Has a demonstrated business objective to maintain or collect such data on greater than one million individuals.

Genetic test information/data is included as a component of "sensitive personal data" regardless of whether it meets the thresholds outlined above.

Notably, the definition of "sensitive personal data" explicitly excludes:

- Data maintained or collected by a U.S. business concerning the employees of that U.S. business, unless the data pertains to employees of U.S. Government contractors who hold U.S. personnel security clearances; or,
- Data that is a matter of public record, such as court records or other government records that are generally available to the public.

CFIUS FILING REQUIREMENTS AND TIMING

CFIUS has jurisdiction to review three categories of foreign investments, including controlling transactions, certain non-controlling investments and certain real estate transactions. CFIUS also maintains mandatory filing requirements for certain transactions involving investments in critical infrastructure and technology as well as transactions resulting in a substantial foreign government interest in a TID business (discussed above).

Covered Control Transactions

Unlike the prior, voluntary practice, FIRRMA now mandates filings for certain transactions that would result in foreign control of a U.S. business—known as "covered control transactions."

"Covered control transactions" are defined as any transaction by or with any foreign person that could result in:

- Foreign control of any U.S. business;
- A foreign person conveying its control of a U.S. business to another foreign person;
- Control by a foreign person of any part of an entity or of assets, if such part of an entity or assets constitutes a U.S. business; or,
- A joint venture in which the parties enter into a contractual or other similar arrangement, but only if one or more of the parties contributes a U.S. business and a foreign person could control that U.S. business by means of the joint venture.

Covered Investments

CFIUS also has jurisdiction over certain non-controlling investments in TID businesses. A "covered investment" is one in which a foreign person or entity invests in a U.S. TID business and, through such investment, obtains certain "rights," including but not limited to:

- Access to material, non-public technical information of the U.S. TID business;
- Membership or observer rights on the board of directors or equivalent governing body of the U.S. TID business; or,
- Any involvement, other than through voting shares, in the substantive decision making of the U.S. TID business.

Covered Real Estate Transactions

In addition to "control transactions" and "covered investments," CFIUS is charged with reviewing certain real estate transactions and investments. Such transactions include those where a foreign person/entity seeks to obtain real estate in and/or around specific, enumerated airports, maritime ports or military installations. Note, CFIUS maintains the authority to review covered real estate transactions even where the transaction does not contemplate the acquisition of a U.S. business.

CFIUS AUTHORITY TO MODIFY OR UNWIND TRANSACTIONS

Following CFIUS review and investigation, the Committee has broad authority to address any potential national security risks which may be posed as a result of the proposed transaction.

"Safe Harbor"

Where CFIUS has completed all actions with respect to a covered transaction and determined that either the transaction does not pose a national security risk or that any risks are adequately mitigated, the Committee will provide written confirmation to the parties that the CFIUS review is complete. Such notice is commonly referred to as a "safe harbor" letter, as the proposed transaction will no longer be subject to further CFIUS review.

Mitigation Measures

If CFIUS identifies certain national security risks, which it believes require additional mitigation, the Committee may require the parties to enter into an agreement (described below) to address these national security concerns. Additionally, and even prior to the completion of the Committee's review, CFIUS may impose interim mitigation measures while conducting its review and investigation.

CFIUS maintains an ongoing role in ensuring that mitigation measures and agreements are being implemented to the satisfaction of the Committee. To this end, CFIUS may impose certain penalties for breach of a mitigation agreement or unilaterally initiate further review of a previously reviewed transaction where a material breach has occurred, regardless of whether the material breach was intentional.

Prohibited Transactions

While CFIUS itself does not have the authority to suspend or prohibit a proposed transaction, the Committee may recommend to the President that a transaction be prohibited as posing a significant risk to the national security interests of the United States which cannot be ameliorated through a mitigation agreement. Notably, the President may also unwind a transaction which has already been completed prior to CFIUS review.

CFIUS MITIGATION AGREEMENTS

Prior to making a determination on a transaction, CFIUS may enter into a mitigation agreement with the parties to address any unresolved national security concerns that emerge during the review process. The goal of a mitigation agreement is to restructure the company/transaction into one that eliminates any national security concerns of CFIUS. Mitigation agreements come in many forms and are negotiated prior to CFIUS approving a transaction. The CFIUS 2023 Annual Report indicates that recent mitigation measures include:

- Divestiture by the foreign acquirer of all or part of the U.S. business;
- Prohibiting or limiting the transfer or sharing of certain intellectual property, trade secrets, assets, or technical information;
- Establishing guidelines and terms for handling existing or future contracts with the U.S. Government or its contractors;
- Ensuring only authorized persons have access to certain technology, systems, facilities, projects, or sensitive information;
- Ensuring that computer networks are segregated;
- Establishing a corporate security committee, proxy agreement, and/or other mechanisms to limit foreign influence and ensure compliance, including the appointment of a U.S. Government-approved security officer, member of the board of directors, or board observer, and requirements for security policies, communications policies, annual reports, and independent audits;
- Notifying customers or relevant U.S. Government parties when there is a change of ownership in the U.S. business;
- Ensuring that businesses notify customers of the identity of ultimate beneficial owners; and/or,
- Assurances of continuity of supply to the U.S. Government for defined periods, notification and consultation prior to making certain business decisions, and reservation of certain rights for the U.S. Government in the event that the company decides to exit a business line.

CFIUS mitigation agreements are not static—typically they are an active process with an ongoing relationship between the companies and the U.S.

government. In recent years, CFIUS has expanded the use and enforcement of mitigation agreements. Since 2019, CFIUS has usually designated Treasury and one other agency as a CFIUS Monitoring Agency (CMA). Mitigation agreements now regularly include various methods to ensure compliance, such as:

- Periodic reporting to CMAs by the companies;
- Required reporting to the CMAs of actual or suspected violations;
- Required responses to CMA requests for information;
- Regular communication with embedded security and compliance personnel and third-party monitors;
- On-site or virtual compliance reviews by CMAs;
- Third-party audits; and/or,
- Investigations and remedial actions if anomalies or breaches are discovered or suspected, including recommending that the Committee impose penalties or unilaterally initiate another review of the covered transaction, where appropriate.

CFIUS's mitigation measures are drawn in large part from agreements used by the Defense Counterintelligence and Security Agency (DCSA).

DCSA is tasked with overseeing cleared facilities of government contractors, including mitigation of concerns connected with foreign ownership, control or influence (FOCI).

Buchanan's International Trade and National Security Practice has significant experience representing clients in a full range of issues before DCSA, including FOCI mitigation measures. Please see Buchanan's DCSA handbook for more information.

CFIUS NON-NOTIFIED TRANSACTIONS

Where no voluntary notice has been filed by pertinent parties to a transaction and no safe harbor has been granted, CFIUS has the ability to take action(s) to determine whether the transaction was, in fact, subject to CFIUS's jurisdiction. Then, CFIUS may take formal steps to initiate a review of the transaction. In particular, if CFIUS determines that a non-notified transaction may be a covered transaction pursuant to 31 C.F.R. Part 800 or a covered real estate transaction under 31 C.F.R. Part 802 and may raise national security considerations, the Department of Treasury, operating on behalf of CFIUS, may contact the transaction parties for additional information.

Transactions that are identified through the non-notified process are often among the most complicated that CFIUS considers. If CFIUS determines that a non-notified transaction is, in fact, a covered transaction that raises national security risks, mitigation measures may be required. In 2018, FIRRMA formalized CFIUS's ability to commence investigations into and reviews of non-notified transactions. Since 2020, the Department of Treasury has dedicated significant resources to non-notification investigations and reviews—measurably increasing CFIUS's ability to identify and assess whether non-notified transactions pose potential national security concerns.

In 2023, CFIUS, including its individual member agencies, identified and considered numerous potential non-notified transactions and investigated the matters to determine which to open as official inquires. Treasury opened non-notified inquiries for 60 transactions and CFIUS formally requested filings for 13 transactions.

CFIUS PENALTY PROCESS

CFIUS may impose monetary penalties and seek other remedies (e.g., directed notices, action plans) for violations of the regulations or mitigation agreements. The U.S. Department of the Treasury, Office of Investment Security (OIS) is responsible for the imposition of such penalties and other remedies.

CFIUS penalties and other remedies are available without prejudice to civil or criminal penalties that may be applicable under other authorities, and CFIUS may refer conduct to other government enforcement authorities where appropriate.

Types of Conduct That May Constitute a Violation of the CFIUS Regulations

The following three categories of acts or omissions may constitute a violation of the CFIUS regulations:

- Failure to File: The failure of a person/entity to timely submit a mandatory declaration or notice, as applicable.
- Non-Compliance with CFIUS Mitigation: Conduct that is prohibited by or otherwise fails to comply with CFIUS mitigation agreements, conditions or orders.
- Material Misstatement, Omission, or False Certification: Material misstatements in or omissions from information filed with CFIUS and false or materially incomplete certifications filed in connection with assessments, reviews, investigations or CFIUS mitigations, including information provided during informal consultations or in response to requests for information (RFIs).

Not all violations of the regulations lead to penalties, as CFIUS exercises discretion in determining when a penalty is appropriate, including by considering applicable aggravating and mitigating factors.

Evaluation of Facts and Circumstances by CFIUS in Determining if a Violation Occurred

CFIUS has the ability to evaluate information from an array of different sources to independently determine a person's or entity's compliance with the regulations. CFIUS receives actionable information from other U.S. government agencies, publicly available information, third-party service providers (e.g., auditors and monitors), tips, transaction parties and filing parties.

- RFIs: CFIUS often requests information to support its monitoring of compliance with mitigation requirements, as well as to investigate whether a violation of the regulations has occurred and what enforcement action, if any, should be taken. If CFIUS determines that a violation occurred, it will consider the cooperation in response to requests for information in determining what action, and the extent of any, to take. In addition to providing the requested information, parties may choose to provide any

exculpatory evidence, as well as any defense, justification, mitigating factors or explanation for the conduct at issue.

- Self-Disclosures: CFIUS, as with other U.S. Government agencies involved with international trade, strongly encourages any person who believes they may have violated the regulations to submit a voluntary self-disclosure regarding the potential violation. Self-disclosures are written notifications to CFIUS describing pertinent facts and circumstances that may constitute violations.

  Self-disclosures will only be treated by CFIUS as a mitigating factor if the self-disclosure is filed before the U.S. Government has initiated an investigation.

- Tips: CFIUS encourages any person with knowledge or reason to believe that another person has committed a violation of the CFIUS regulations to submit a tip, referral or other relevant information to the CFIUS tips line found on the CFIUS Monitoring & Enforcement website.

- Subpoena Authority: CFIUS has the ability to gather information through the issuance of subpoenas.

Penalty Process

The process for considering and imposing penalties is:

- Notice of Penalty: CFIUS sends a notice of penalty, including a written explanation of the conduct to be penalized and the amount of any monetary penalty to be imposed. The notice will state the legal basis for concluding that the conduct constitutes a violation of the regulations and may set forth any aggravating and mitigating factors that the Committee considered.

- Petition for Reconsideration: A company may, within 15 business days of receipt of a notice of penalty, submit a petition for reconsideration to the CFIUS Staff Chairperson, including any defense, justification, mitigating factors or explanation. Upon a showing of good cause, this period may be extended by the Staff Chairperson.

  If a petition for reconsideration is timely received, CFIUS will consider it within 15 business days of receipt of the petition, which may be extended by the Staff Chairperson, before issuing a final penalty determination.

Aggravating and Mitigating Factors

When determining any appropriate penalty in response to a violation, CFIUS engages in a fact-based analysis in which it weighs aggravating and mitigating factors. Factors that are relevant in the context of one violation will not necessarily be relevant in the context of another. Some factors that CFIUS may consider aggravating or mitigating in determining an appropriate response to a violation include the following:

- Accountability and Future Compliance

The impact of the enforcement action on protecting national security and ensuring that the company is held accountable for its conduct and incentivized to ensure compliance.

- Harm

The extent to which the conduct impaired or threatened to impair U.S. national security.

- Negligence, Awareness, and Intent
    - The extent to which the conduct was the result of simple negligence, gross negligence, intentional action or willfulness.
    - Any effort to conceal or delay the sharing of relevant information with CFIUS.
    - The seniority of personnel within the entity that knew or should have known about the conduct.
- Persistence and Timing
    - The length of time that elapsed after the company became aware, or had reason to become aware, of the conduct, and before CFIUS became aware of the conduct and/or its remediation.
    - The frequency and duration of the conduct.
    - In the case of a violation of a CFIUS mitigation agreement, the length of time since the CFIUS mitigation agreement was issued or became effective.
    - In the case of a Failure to File, the date of the transaction at issue.

- Response and Remediation
  - Whether the company submitted a self-disclosure, including the timeliness, nature and scope of information reported to CFIUS.
  - Whether the company cooperated completely in the investigation of the matter (e.g., providing timely and detailed responses).
  - The promptness of complete and appropriate remediation of the conduct, including the remedial steps taken upon learning of a violation.
  - Whether there was an internal review of the nature, extent, origins and consequences of the conduct to prevent its reoccurrence.
- Sophistication and Record of Compliance
  - The history and familiarity with CFIUS and, if applicable, past compliance with CFIUS mitigation agreements.
  - Internal and external resources dedicated to compliance with applicable legal obligations (e.g., legal counsel, consultants, auditors and monitors).
  - Policies, training and procedures in place to prevent the conduct and the reason for the failure of such measures.
  - Variation in the consistency of compliance, both horizontally across the entity, and vertically from directors and officers to supporting staff.
  - The compliance culture that exists within the company (e.g., demonstrated commitment to compliance with applicable legal obligations).
  - The experience of other federal, state, local or foreign authorities with knowledge of the assessment of the quality and sufficiency of compliance with applicable legal obligations.
  - In the case of a violation of CFIUS mitigation agreement, the extent to which written compliance policies or training on the terms of the relevant mitigation agreement were communicated and implemented across the entity.
  - In the case of a violation of a mitigation agreement, the extent to which the authority, role, access and independence of any security officer were sufficient and in compliance with the terms of the mitigation agreement.

Notice of Proposed Rulemaking to Expand Enforcement and Mitigation Regulations

On April 11, 2024, CFIUS published a Notice of Proposed Rulemaking (NPRM) in the Federal Register proposing to amend its enforcement and mitigation regulations, marking the first substantive update to CFIUS's mitigation and enforcement provisions since the enactment of FIRRMA in 2018. The NPRM proposed the following revisions:

- Expand the types of information that CFIUS can request from parties to non-notified transactions (i.e., transactions over which CFIUS has jurisdiction but for which the parties did not submit a notice to CFIUS seeking review);

- Institute a three (3) day timeline within which parties to a transaction must respond to CFIUS's mitigation proposals (the timeline could be extended by mutual agreement);
- Increase the maximum civil penalties from $250,000 to $5 million per violation for material misstatements and omissions, violations of CFIUS mitigation agreements or orders, or failure to submit mandatory filings (control/investment transactions only); and
- Expand CFIUS's subpoena authority to request additional information from parties to non-notified transactions and from third persons regarding notified transactions.

On November 18, 2024, the Department of Treasury, as Chair of CFIUS, issued a Final Rule consistent with the proposals included in the NPRM, with one exception. The Final Rule does not implement the automatic three-day response deadline but, instead, authorizes the Staff Chairperson to exercise discretion to impose a deadline for responding to mitigation proposals that is no less than three (3) business days.

STATES ENACT "MINI"-CFIUS LEGISLATION

In addition to the requirements of CFIUS (discussed above), various states have begun enacting legislation to require reporting and/or approval obligations at the state-level as it relates to forms of foreign investment. Such legislation is often referred to as "mini"-CFIUS.

By way of illustrative example, on May 8, 2023, Governor Ron DeSantis signed into law SB-264, which restricts Florida's government entities from contracting or providing economic development incentives to entities of foreign countries of concern. Additionally, SB-264 imposes restrictions on purchases of real estate within Florida, prohibiting the People's Republic of China, the Chinese Communist Party, and any other political party or member of a political party in the People's Republic of China, from purchasing or acquiring real property in this state.

SB-264 also includes restrictions on other foreign countries of concern purchasing property within ten miles of a military installation or critical infrastructure (i.e., airports, powerplants, etc.). Foreign countries of concern listed in SB-264 are: China, Russia, Iran, North Korea, Cuba, the Maduro Regime of Venezuela, and Syria.

In May 2023, a group of Chinese citizens residing in Florida filed a lawsuit challenging SB264 as amounting to housing discrimination in violation of both the Constitution and the Fair Housing Act and that SB-264 was preempted by FIRRMA's authorization of CFIUS with respect to real estate transactions. On February 1, 2024, the Eleventh Circuit Court of Appeals temporarily halted enforcement of SB264 while the case proceeds.

OUTBOUND CFIUS

On August 9, 2023, President Biden issued Executive Order 14105 requiring Treasury to "establish a program to prohibit or require notification of certain types of outbound investments," which includes "semiconductors and microelectronics, quantum information technologies, and artificial intelligence." EO 14105 also identifies China (including Hong Kong and Macau) as a country of concern.

To this end, on October 28, 2024, Treasury released the final rule implementing EO 14105 (the "Outbound CFIUS Rule"), which imposes additional due diligence responsibilities, notification requirements, and limitations on U.S. persons engaging in certain transactions with foreign persons in "countries of concern." Currently, the Outbound CFIUS Rule defines "covered foreign persons" to include any person or entity that engages in a covered activity and is:

- A citizen or permanent resident of China and not a U.S. citizen;
- An entity headquartered or with its principal place of business in China;
- An entity incorporated under Chinese law;
- A Chinese government party; or,
- Any entity, wherever located, where 50% or greater voting interests, board interests or equity interests are held by one of the categories of persons or entities described above.

Where a "covered foreign person" is engaged in certain activities, the Outbound CFIUS Rule requires both notification obligations and prohibits certain categories of transactions, including:

- Treasury must be notified of a proposed transaction where a covered foreign person engages in: (1) designing or fabricating integrated circuits (ICs), or (2) developing AI systems which are designed for military or mass surveillance uses, intended to be used in cybersecurity applications, or trained using certain thresholds of computing power.
- Transactions are prohibited if they involve sensitive activities, including: (1) certain advanced technologies or military end uses, or (2) certain technologies related to ICs, semiconductors, or quantum computing.

While the Outbound CFIUS Rule does not, itself, establish penalties, penalty amounts under the International Emergency Economic Powers Act may be applicable to any violations. These include civil penalties of the greater of either $250,000 (adjusted for inflation) or twice the value of the transaction, and criminal penalties of up to $1 million and imprisonment for up to 20 years.

The Outbound CFIUS Rule became effective on January 2, 2025. As such, covered transactions with a completion date on or after January 2, 2025, are subject to the prohibition and notification requirements of the Outbound CFIUS Rule.

On January 20, 2025, the Trump administration issued an "America First Trade Policy Memorandum" which calls for, inter alia, the Secretary of Treasury, in consultation with the Secretary of Commerce, to

review EO 14105 and the implementing Outbound CFIUS Rule to determine whether "sufficient controls" exist to "address national security threats" of outbound investments. Upon review, the Secretary of Treasury is to make recommendations to the President, "including potential modifications to the Outbound Investment Security Program."

AMERICA FIRST INVESTMENT POLICY

On February 21, 2025, President Trump outlined the Administration's approach to foreign investment controls in a memorandum entitled "America First Investment Policy." Stating that "[w]elcoming foreign investment and strengthening the United States' world-leading private and public capital markets will be a key part of America's Golden Age," the Policy, in broad terms, seeks to facilitate inbound investment from U.S. allies while placing greater restrictions on foreign investment for "foreign adversaries," including the Peoples Republic of China (PRC), Hong Kong, Macau, Cuba, Iran, North Korea, Russia, and the regime of Venezuelan politician Nicolás Maduro.

To expedite foreign investment in the United States by "specified allied and partner sources," the Trump administration will create a "fast-track" process, including expedited reviews. Participation in the currently undefined "fast-track" process will "allow for increased foreign investment subject to appropriate security provisions, including requirements that the specified foreign investors avoid partnering with United States foreign adversaries."

As it relates to investments from "foreign adversaries," the Policy states that the "United States will establish new rules to stop United States companies and investors from investing in industries that advance the PRC's national Military-Civil Fusion strategy and stop PRC-affiliated persons from buying up critical American businesses and assets…" Additionally, the Policy states that the Administration will "cease the use of overly bureaucratic, complex, and open-ended 'mitigation' agreements for United States investments from foreign adversary countries," instead favoring "concrete actions that companies can complete within a specific time, rather than perpetual and expensive compliance obligations."

Further, the Policy alludes to the potential expansion of CFIUS jurisdiction by seeking, in consultation with Congress, to "strengthen CFIUS authority over 'greenfield' investment, to restrict foreign adversary access to United States talent and operations in sensitive technologies (especially artificial intelligence), and to expand the remit of 'emerging and foundational' technologies addressable by CFIUS." In this way, the Policy appears to allow for, among other things, new technologies to be deemed "emerging and foundational," which could result in additional transactions being subject to mandatory CFIUS filings and review.

Agencies given directives under the new Policy, including Treasury's assessment of whether current outbound investment regulations include "sufficient controls to address national security threats," are to deliver recommendations on potential modifications to the program by April 1, 2025.

BUCHANAN'S EXPERIENCE WITH CFIUS

For individuals and entities considering transactions that may fall within the jurisdiction of CFIUS, having a team of experienced lawyers is a necessity. Buchanan Ingersoll & Rooney's National Security practice group members are intimately familiar with these regimes and remain abreast of the latest development and enforcement actions. Buchanan stands ready to guide individuals and entities through these continually evolving matters.

Daniel B. Pickard

Chair, Shareholder, International Trade & National Security Practice Group

Email: daniel.pickard@bipc.com

Phone: (202) 452-7936

In his specialty practice, Dan has extensive experience in regard to the intersection of international business and national security matters such as U.S. economic sanctions, export controls (including the International Traffic in Arms Regulations (ITAR)), antiboycott measures, and the Foreign Corrupt Practices Act (FCPA). Dan provides comprehensive international trade law compliance guidance, including to U.S. and international clients that provide goods and services that may be regulated due to national security reasons. He develops customized and specialized corporate compliance programs related to the FCPA, ITAR, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and the National Industrial Security Program (NISP) and mitigating Foreign Ownership, Control, or Influence (FOCI) issues. In cases of non-compliance and potential violations, Dan conducts internal investigations and represents clients before the relevant agencies in connection with investigations, voluntary self-disclosures, licensing, and enforcement actions. In addition, clients also often look to Dan for guidance pertaining to the Foreign Agents Registration Act (FARA).

Keil Ritterpusch

Shareholder

Email: keil.ritterpusch@bipc.com

Phone: (202) 452-7304

Keil represents clients in international trade, national security, and corporate/government investigation matters. With more than 20 years of experience, he focuses his practice on all matters related to the U.S. export control and economic and trade sanctions laws and regulations. Keil's clients come from the defense, aerospace, technology, encryption, computer, electronic device, software, medical, and private equity industries. He provides export compliance counsel in the context of acquisitions, investments, and divestitures involving foreign companies and export-regulated technologies, economic embargoes and sanctions, and supply chain security and compliance.

Jordan Yeagley

Counsel

Email: jordan.yeagley@bipc.com

Phone: (202) 452-7900

Jordan focuses his practice on advising and representing clients from across a wide range of heavily regulated industries in complex litigation, national security and compliance matters. Jordan also has extensive experience advising clients on national security matters such as U.S. economic sanctions administered by the Office of Foreign Assets Control (OFAC), export controls (including the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR)), the Foreign Corrupt Practices Act (FCPA), the Bank Secrecy Act (BSA) and the Foreign Agents Registration Act (FARA). He helps U.S. and international organizations to navigate these complex national security regimes and mitigate potential legal and regulatory risks inherent in doing business in the global economy. Where issues of potential non-compliance arise, Jordan guides clients through internal investigations and, where necessary, voluntary self-disclosures and enforcement actions.

Milton Koch

International Trade Advisor

Email: milton.koch@bipc.com

Phone: (202) 452-7937

Milton provides analysis to domestic producers in trade remedy litigation, with a particular emphasis on antidumping investigations before the U.S. Department of Commerce. As a Certified Public Accountant and a former analyst at the U.S. Department of Commerce, Milton Koch supports trade litigation clients by developing legal strategies based on in-depth analysis of complex financial data. He has taken a primary role in numerous trade cases providing creative and novel legal solutions to address issues ranging from the business structure of multinational companies to unique subsidy schemes of foreign governments. He serves as an analyst in cases across a number of industries, including manufacturing, finance and investing. He also assists clients in research matters relating to economic sanctions, national security, and litigation.

NOTES:

Buchanan