DoD Instruction 2000.25

DoD Procedures for Reviewing and Monitoring Transactions Filed with the Committee on Foreign Investment in the United States

Originating Component:	Office of the Under Secretary of Defense for Acquisition and Sustainment
Effective:	December 16, 2021
Change 1 Effective:	May 27, 2022
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 2000.25, "DoD Procedures for Reviewing and Monitoring Transactions Filed with the Committee on Foreign Investment in the United States (CFIUS)," August 5, 2010, as amended
Approved by:	Gregory M. Kausner, Performing the Duties of the Under Secretary of Defense for Acquisition and Sustainment
Change 1 Approved by:	William A. LaPlante, Jr., Under Secretary of Defense for Acquisition and Sustainment

Purpose: In accordance with the authority in DoD Directive (DoDD) 5135.02; Section 4565 of Title 50, United States Code (U.S.C.); and DoDD 5100.01, this issuance establishes policy, assigns responsibilities, and provides procedures for DoD participation on the Committee on Foreign Investment in the United States (CFIUS).

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

1.2. POLICY.

a. In accordance with Section 4565 of Title 50, U.S.C., and as articulated in Subtitle A of Title XVII of Public Law 115-232, also known and referred to in this issuance as the "Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA)," the DoD will maintain a commitment to open investment policies that will welcome and support foreign investments consistent with protecting national security.

b. Department officials shall take steps aimed at ensuring that transactions of or foreign investments in U.S. companies do not present unacceptable risks to national security.

c. The DoD, its Components, and other supporting sub-organizations must provide detailed and substantive assessments regarding CFIUS transactions in accordance with this issuance and Section 4565 of Title 50, U.S.C. as amended.

d. Consistent with inputs from DoD Components and supporting organizations, the DoD will provide an overall assessment of national security implications arising from each CFIUS transaction and declaration. In accordance with this issuance, the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) will submit an integrated DoD recommendation to the Committee based on consensus-based synthesized assessments of the threats, vulnerabilities, and consequences from DoD sub-organizations and Components.

e. If national security concerns exist as a result of a covered transaction, the DoD will, as appropriate, recommend mitigation terms based on input from its interested DoD Components and supporting organizations to resolve national security risks. If the DoD assesses that national security concerns cannot be resolved or that mitigation cannot effectively be supported by the DoD throughout the necessary term, the DoD will advise that the Committee recommend to the President to suspend or prohibit the transaction.

f. The DoD will provide robust and effective compliance monitoring of all DoD CFIUS risk mitigation agreements.

g. The DoD will seek appropriate and timely penalties, damages, and other remedial actions for entities who are subject to and violate CFIUS risk mitigation agreements.

h. The DoD will identify proposed or completed foreign acquisitions of or investments in U.S. companies that pose a risk to national security.

i. CFIUS is the statutorily mandated Executive Branch committee, which legally requires the DoD and its Components to review transactions for national security concerns. DoD Components will resource and staff this DoD responsibility to ensure the successful completion of national security assessments, mitigation planning, and the monitoring of compliance with mitigation agreements between foreign entities, or their U.S. subsidiaries, and the DoD.

1.3. SUMMARY OF CHANGE 1.

The changes to this issuance update organizational titles and references based on:

a. Section 138(b)(6) of Title 10, U.S.C., which establishes the position of the Assistant Secretary of Defense for Industrial Base Policy (ASD(IBP)).

b. The February 10, 2022 Deputy Secretary of Defense Memorandum, which provides guidance on the reporting relationship, duties, and responsibilities of the ASD(IBP) and establishes the Office of the ASD(IBP) (OASD(IBP)).

SECTION 2: RESPONSIBILITIES

2.1. USD(A&S).

The USD(A&S):

a. Represents the Secretary of Defense in CFIUS matters and establishes policies for the DoD's participation in the Committee.

b. Provides:

(1) Direction to DoD Components, ensuring that DoD equities are fully assessed in the review and examination of foreign investment in the United States.

(2) Policy, best practices, and cross-cutting integrated DoD procedures, implemented by the DoD Components, to help identify foreign investment risks as they relate to declarations, national security review, national security investigations, and non-notified processes.

(3) Policies to support effective mitigation of risks and monitoring compliance of subsequent mitigation agreements, where warranted.

2.2. ASD(IBP).

Under the authority, direction, and control of the USD(A&S), the ASD(IBP):

a. Represents the USD(A&S) to the Secretary of the Treasury (CFIUS Chair) representatives and at Committee meetings.

b. Manages the CFIUS process within the DoD, including:

(1) Formulating and synthesizing the consensus-based DoD position on all declarations and notified and non-notified CFIUS transactions in conjunction with other CFIUS executive agencies.

(2) Serving as the DoD's primary point of coordination for DoD internal reviews of declarations and notified and non-notified CFIUS transactions.

(3) Appointing DoD stakeholder(s) with equities affected by a CFIUS transaction as primary equity holder(s) to assist in assessing each CFIUS case.

(4) Assessing the overall level of national security risk each CFIUS transaction poses to the DoD. This includes a synthesized assessment of threats, vulnerabilities, and consequences.

(5) Assessing the criticality of the target U.S. company to the defense industrial base in accordance with Section 4565 of Title 50, U.S.C.

(6) Recommending a DoD position to the USD(A&S) on:

(a) CFIUS transactions, including assessing whether CFIUS risk mitigation agreements can resolve identified national security concerns in the transactions.

(b) Compliance monitoring issues.

(c) Each DoD proposed non-notified transaction that may raise national security considerations, as outlined in Paragraph 3.6.

(7) Recommending DoD's substantive response to congressional inquiries regarding CFIUS matters.

(8) Serving as the Defense CFIUS Coordination Group Chair established in Paragraph 3.7.

2.3. ASSISTANT SECRETARY OF DEFENSE FOR ACQUISITION (ASD(A)); ASSISTANT SECRETARY OF DEFENSE FOR SUSTAINMENT (ASD(S)); ASSISTANT SECRETARY OF DEFENSE FOR NUCLEAR, CHEMICAL, AND BIOLOGICAL DEFENSE PROGRAMS (ASD(NCB)); AND DIRECTOR OF SPECIAL PROGRAMS.

Under the authority, direction, and control of the USD(A&S), the ASD(A), ASD(S), ASD(NCB), and Director of Special Programs determine and assess the vulnerabilities and consequences of CFIUS transactions and declarations related to procurement strategy, policy, acquisition oversight, supply support, and technical and logistic services to the Military Departments, respectively.

2.4. ASD(S).

Under the authority, direction, and control of the USD(A&S) and in addition to the responsibility in Paragraph 2.3., the ASD(S) is the focal point for collaborating declarations and CFIUS transactions subject to energy and energy-related projects evaluation by the DoD Military Aviation and Installation Assurance Siting Clearinghouse in accordance with DoD Instruction 4180.02.

2.5. DIRECTOR OF SPECIAL PROGRAMS.

Under the authority, direction, and control of the USD(A&S) and in addition to the responsibility in Paragraph 2.3., the Director of Special Programs:

a. Coordinates across special access program stakeholders to identify DoD-wide special program equities.

b. Ensures risks are evaluated and mitigated to protect against impacts on existing or future defense capabilities.

c. Develops a coordinated special access program position on cases, as appropriate, to safeguard and preserve critical DoD capabilities.

2.6. DIRECTOR, DEFENSE CONTRACT MANAGEMENT AGENCY (DCMA).

Under the authority, direction, and control of the USD(A&S), the Director, DCMA, as necessary and in conjunction with the ASD(IBP):

a. Assesses defense industrial base criticality of the target U.S. company by leveraging relevant DCMA corporate or defense industrial base assessments.

b. Supports applicable mitigation agreement compliance monitoring activities.

2.7. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING (USD(R&E)).

The USD(R&E) determines and assesses the vulnerability and consequences of CFIUS transactions and declarations on defense research and development programs and their potential effect on future defense capabilities by:

a. Determining whether a target U.S. company is essential for developing critical technologies, defense capabilities, or acquisition programs.

b. When relevant to CFIUS transactions, conducting assessments of trends involving technologies identified in CFIUS filings and documentation.

c. Evaluating CFIUS transactions and declarations to:

(1) Identify their:

(a) Effect on current defense research programs.

(b) Potential effect on future defense capabilities.

(2) Identify whether a target U.S. company is critical to developing vital or emergent technologies or defense capabilities.

(3) Assess their effect on research and development activities due to the foreign acquirer's colocation with, or proximity to, DoD infrastructure.

(4) Assess their effect on emergent technologies.

2.8. DIRECTOR, MISSILE DEFENSE AGENCY (MDA).

Under the authority, direction, and control of USD(R&E), the Director, MDA determines and assesses the vulnerabilities and consequences of CFIUS transactions and declarations on missile defense activities and potential implications on future missile defense technologies.

2.9. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)).

The USD(P) provides policy evaluation and oversight of each CFIUS transaction and declaration under consideration, including assessing:

a. Whether there are current or upcoming DoD functional or regional concerns or applicable policies or strategies regarding technologies or foreign countries or governments involved in a CFIUS transaction or declaration.

b. The impact of a CFIUS transaction or declaration, including vulnerabilities and consequences relevant to functional capabilities, on bilateral and multilateral relationships and regional dynamics.

2.10. DIRECTOR, DEFENSE TECHNOLOGY SECURITY ADMINISTRATION (DTSA).

Under the authority, direction, and control of USD(P), Director, DTSA, is the focal point for providing USD(P)'s position on each CFIUS transaction and declaration, including assessing:

a. Whether the materials, products, technologies, or services of the target U.S. company are export controlled.

b. Whether existing U.S. export controls are adequate to prevent the unauthorized transfer of critical materials, products, technologies, or services possessed by the target U.S. company.

c. National security risks posed by transferring critical materials, products, technologies, or services that could adversely affect U.S. technological competitiveness.

2.11. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)).

The USD(I&S):

a. Addresses the effect of CFIUS transactions or declarations on intelligence and security activities and determines and assesses the vulnerabilities and consequences on intelligence systems and related technologies.

b. Supports DoD compliance monitoring of mitigation agreements when designated by the USD(A&S) as a primary equity holder for Defense Intelligence and Security Enterprise–related matters in conjunction with the OASD(IBP).

c. Informs the ASD(IBP) of the effect of CFIUS transactions or declarations on companies cleared under the National Industrial Security Program (NISP).

d. Evaluates national security concerns of foreign ownership or control of cleared defense contractors that are target U.S. companies in any CFIUS transaction or declaration in accordance

with NISP procedures for government activities relating to foreign ownership, control, or influence (FOCI) in Volume 2 of DoD Manual 5220.32.

e. Assesses CFIUS decision packages addressed to the Deputy Secretary of Defense and CFIUS transaction or declaration decision packages concerning a CFIUS transaction involving Defense Counterintelligence and Security Agency (DCSA) FOCI mitigation, including those recommending both a FOCI and a CFIUS mitigation agreement.

f. Collaborates with the ASD(IBP), as applicable, to support relevant CFIUS mitigation agreement compliance monitoring activities in conjunction with DCSA's annual FOCI action plan review and certification in accordance with NISP procedures in Volume 2 of DoD Manual 5220.32.

g. Oversees Defense Intelligence Component heads in their support to the Defense Intelligence Agency (DIA) threat assessment products listed in Paragraph 2.13.

2.12. DIRECTORS, DIA, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY (NGA), NATIONAL RECONNAISSANCE OFFICE (NRO), AND DCSA AND THE DIRECTOR, NATIONAL SECURITY AGENCY (NSA)/CHIEF, CENTRAL SECURITY SERVICE (DIRNSA/CHCSS).

Under the authority, direction, and control of the USD(I&S), the Directors, DIA, NGA, NRO, and DCSA and the DIRNSA/CHCSS support and assess each CFIUS action that affects their specific area of responsibility, including assessing potential threats associated with DoD CFIUS transactions and declarations.

2.13. DIRECTOR, DIA.

Under the authority, direction, and control of the USD(I&S) and in addition to the responsibility in Paragraph 2.12., the Director, DIA oversees:

a. Technology-transfer risk assessments for CFIUS transactions and declarations in accordance with Section 2537 of Title 10, U.S.C.

b. The production of National Security Threat Assessment (NSTA) supportive threat assessments, including, upon request of the CFIUS Monitoring Agency, a threat reassessment in each CFIUS risk mitigation agreement to which the DoD is a monitoring agency.

2.14. DIRNSA/CHCSS.

Under the authority, direction, and control of the USD(I&S), in addition to the responsibility in Paragraph 2.12.; in coordination with the DoD Chief Information Officer (DoD CIO), as delegated by the Secretary of Defense; and consistent with applicable Office of the Director of National Intelligence (ODNI) guidance, the DIRNSA/CHCSS provides technical support to the

DoD CIO, the USD(I&S), and other U.S. Government officials, as appropriate, in the review of CFIUS actions.

2.15. DIRECTOR, DCSA.

Under the authority, direction, and control of the USD(I&S) and in addition to the responsibility in Paragraph 2.12., the Director, DCSA:

a. Assesses the effect of CFIUS transactions and declarations on NISP-cleared companies.

b. When relevant, recommends CFIUS risk mitigation agreement measures in order to mitigate threats to national security arising from the CFIUS transactions.

c. Provides counterintelligence assessments of CFIUS transactions and support to the CFIUS declarations, mitigation agreement, and monitoring processes.

2.16. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)).

The USD(P&R) assists and coordinates with the USD(A&S), as necessary and requested, with determining and assessing the vulnerability and consequences of identified and relevant CFIUS transactions and declarations on total force readiness by providing:

a. Relevant inputs and assessments on whether a target U.S. company maintains or collects sensitive personal data, including personally identifiable information (PII) and protected health information, about DoD personnel in a manner that may be exploited to threaten national security.

b. Subject matter expertise to support their CFIUS transaction and declaration evaluations, which may either result in the collection of sensitive DoD personal data or impact the readiness, training, and safety of the force.

2.17. GENERAL COUNSEL OF THE DEPARMENT OF DEFENSE.

The General Counsel of the Department of Defense provides:

a. Legal advice and counsel to the DoD regarding CFIUS matters.

b. Legal advice on:

(1) DoD responsibilities and authorities under Section 721 of the Defense Production Act of 1950, as amended; its implementing regulations and directives; and all other law and policy relating to CFIUS.

(2) Proposed legislative updates to assist with, and keep current, the DoD's policy regarding the review of foreign investment in the United States.

2.18. DOD CIO.

The DoD CIO:

a. Identifies national security risks arising from CFIUS transactions and declarations that may expose vulnerabilities in the DoD's information enterprise, including DoD communications.

b. Assesses CFIUS transactions and declarations regarding the electromagnetic spectrum, network policy, and standards for information systems.

c. When required, provides CFIUS case inputs that are consistent with the policies established by Executive Order 13913.

2.19. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA).

Under the authority, direction, and control of the DoD CIO, the Director, DISA evaluates CFIUS transactions and declarations involving information technology equipment and networks operated by the DoD to provide informed and current advice for DoD CFIUS use.

2.20. SECRETARIES OF THE MILITARY DEPARTMENTS.

The Secretaries of the Military Departments:

a. Identify and assess the national security implications of the threats, vulnerabilities, and consequences of a CFIUS transaction relevant to their respective Military Services, including:

(1) The effect on the warfighters' capabilities and technological advantage from the transfer or potential transfer of, or access to, the target U.S. company's products, services, or technologies to the acquiring company.

(2) The effect of the foreign acquirer's colocation with, or proximity to, sensitive military sites and military activities, including training and testing.

(3) Overseeing the Service intelligence centers' and Military Department Counterintelligence Organization's support to the assessment of all threats resulting from each CFIUS transaction.

b. Support mitigation agreement compliance monitoring activities when designated as a primary equity holder.

2.21. CJCS AND COMBATANT COMMANDERS.

The CJCS and Combatant Commanders identify, review, and assess national security implications, including the mission impact of CFIUS transactions that are relevant to their respective areas of concern.

SECTION 3: PROCEDURES

3.1. GENERAL.

a. Background.

(1) The DoD is one of nine agency members of the Committee, which is charged with reviewing transactions involving certain foreign investment in the United States, including foreign real estate transactions, to determine the effect on national security.

(2) The Secretary of the Treasury is the CFIUS Chair and receives, processes, and coordinates notices submitted by the foreign acquirer and target U.S company (referred to in this issuance, collectively and in the context of application of a particular transaction, as "the Parties") to the Committee and coordinates CFIUS actions among Committee members.

(3) Each Committee member evaluates CFIUS actions in several contexts: declarations, national security review, national security investigation, and compliance monitoring—within the FIRRMA statutory timing requirements addressed in this section. CFIUS actions that result from non-notified transactions also utilize these processes.

(4) It is essential that the DoD and its stakeholders employ the procedures in this section to conduct a full, balanced, and detailed examination of CFIUS transactions and provide the USD(A&S) with robust recommendations to reflect the entirety of the DoD's critical equities.

(5) DoD Component head primary equity holders or assigned designees approve their position on risk and national security concerns within the timelines established in this issuance.

b. DoD CFIUS Process Overview.

(1) Declarations.

The 30-day declaration assessment process begins when the Department of the Treasury forwards the short-form transaction summary to the Committee. DoD Components develop risk-based positions informed by the nexus of the facts and transaction circumstances and the Components' equities to determine whether the declaration presents U.S. national security considerations. After consolidating and synthesizing the Components' inputs regarding these national security considerations, the OASD(IBP) develops a risk-based position for the DoD and recommends the CFIUS either:

(a) Takes no action;

(b) Clears the transaction; or

(c) Requests a filing, which could result in a national security review.

(2) National Security Review.

(a) The national security review is a 45-day process to assess whether a covered transaction presents national security concerns.

(b) If the CFIUS Chair determines that a case affects DoD equities, or upon DoD request, the Chair may designate DoD as a CFIUS co-lead. In turn, the OASD(IBP) and DoD stakeholders review the transaction and identify the nexus between DoD stakeholder equities and national security risk.

(c) Based on the specific DoD equities in the case, DoD stakeholder(s) that assess national security risk become equity holder(s). If equity holder(s) identify potential national security concerns, they become primary equity holders and evaluate threat, vulnerabilities, and consequences of the transaction and provide input to the OASD(IBP)'s risk-based analysis (RBA).

(d) If this analysis confirms the existence of national security concerns, OASD(IBP) will recommend a national security investigation to the Committee.

(3) National Security Investigation.

(a) A national security investigation is a 45-day process in which CFIUS investigates the identified national security concerns to determine if the transaction Parties can resolve the concerns through additional due diligence or mitigation measures or if the U.S. Government needs to suspend or prohibit the transaction.

(b) Upon completing an RBA and identifying the resolution of national security concerns through due diligence, OASD(IBP) will recommend clearance of the transaction to the Committee.

(c) Upon completing an RBA and identifying an addressable risk, OASD(IBP) will recommend mitigation terms to the Committee.

(d) Following agreement among the Committee members, the CFIUS imposes terms as part of an order or presents these terms to the Parties of the transactions and negotiates a final agreement. The Committee concludes this phase by either:

1. Certifying to Congress that there are no unresolved national security concerns, which could include signing a mitigation agreement to mitigate national security concerns (Parties sign a national security agreement allowing the DoD to clear the case); or

2. Recommending that the President suspend or prohibit the transaction if concerns persist.

(4) Compliance Monitoring.

If the investigation outcome results in a mitigation agreement between the Parties to the transaction and the Committee, and if the DoD was a CFIUS co-lead during the investigation,

OASD(IBP) and the primary equity holder(s) monitor compliance. If the Parties violate the terms of the agreement, the DoD seeks appropriate and timely penalties, damages, and other remedial actions.

(5) Non-Notified.

(a) Committee members may also identify proposed and completed foreign transactions involving U.S. companies that did not include voluntary notification of the transaction to CFIUS or a mandated declaration, thereby constituting a non-notified transaction.

(b) OASD(IBP) is responsible for exploring potential security risks of non-notified transactions and, if potential risks are identified, submits such transactions to the CFIUS for review.

(c) If the CFIUS concurs that the OASD(IBP) identified transaction presents national security considerations:

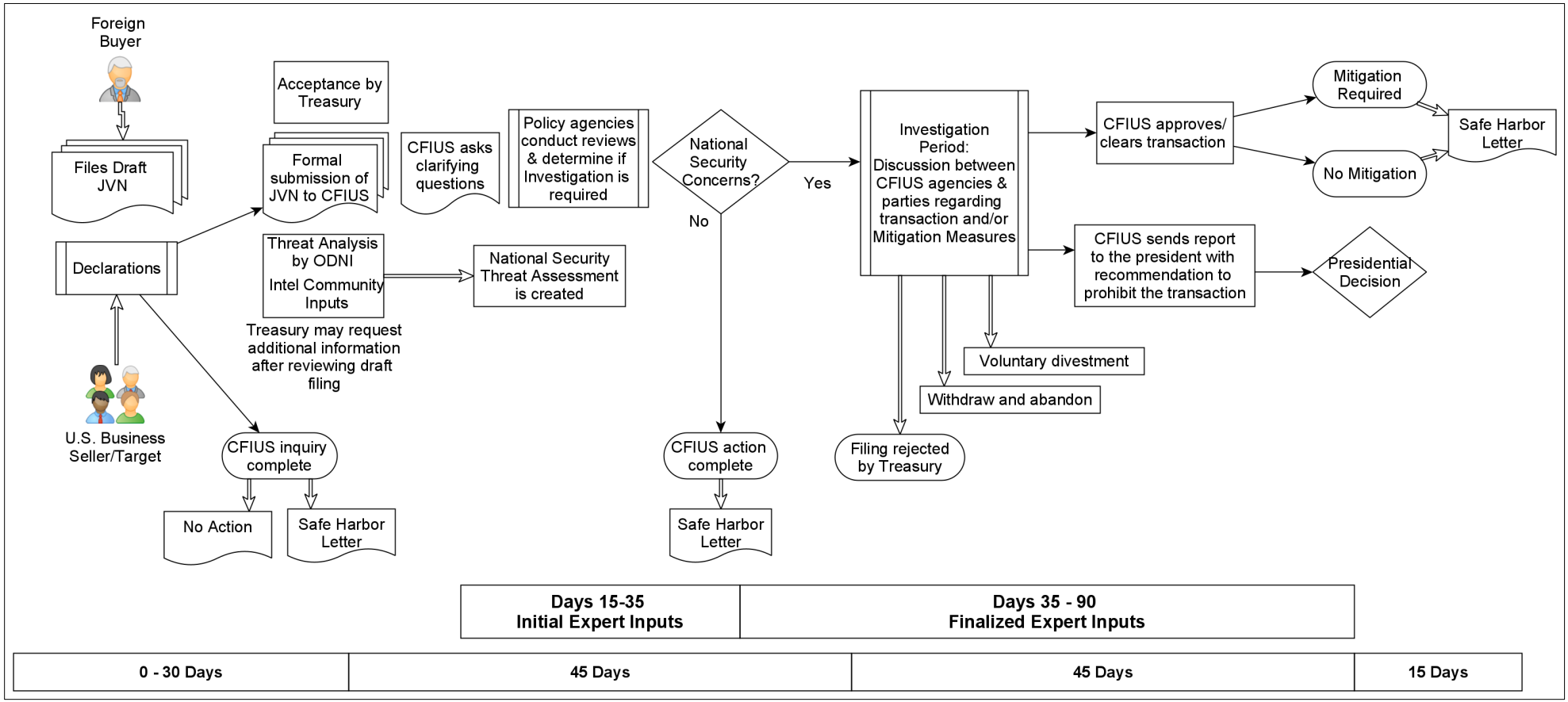
1. The CFIUS Chair may: contact the Parties to request a joint voluntary notification (JVN) to initiate the CFIUS review; or

2. If the Parties refuse to file, the DoD may initiate a unilateral national security review.

(6) DoD's CFIUS Process Depiction.

Figure 1 illustrates the CFIUS process as outlined in Paragraphs 3.2. to 3.4.

Figure 1. CFIUS Process Overview



c. DoD Stakeholders.

DoD positions on national security considerations and concerns in CFIUS cases include, but are not limited to, a risk assessment of the DoD's supply chain relationships with the target U.S. company, proximity to critical infrastructure, impacted mission(s), and sensitive personal data, which are essential aspects of the DoD's national security risk assessment. The analysis and expertise of DoD Component heads are key in assessing the criticality of target U.S. companies.

(1) DoD Components that regularly participate in the CFIUS review process are listed in Table 1. This list is a preliminary set of potential DoD stakeholders who may review the transaction. It is not comprehensive. If a covered transaction involves a DoD Component not listed in Table 1, OASD(IBP) may task it as a DoD stakeholder.

Table 1. DoD Stakeholders

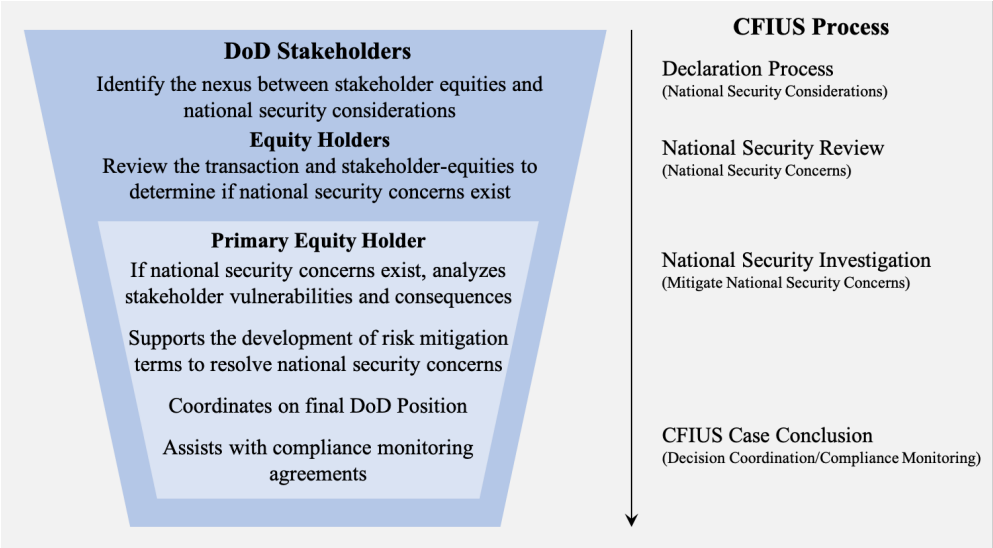
Principal Staff Assistants and Secretaries of the Military Departments	Component
USD(A&S)	Office of the ASD(A) Office of the ASD(S) Office of the ASD(NCB) Office of Special Programs OASD(IBP) Defense Logistics Agency
USD(R&E)	Office of the Director of Defense Research and Engineering (DDRE) for Research and Technology Office of the DDRE for Advanced Capabilities Office of the DDRE for Modernization MDA Defense Advanced Research Projects Agency Space Development Agency DoD Test Resource Management Center
USD(I&S)	NRO NGA NSA/Central Security Service DCSA DIA
USD(P)	DTSA
USD(P&R)	Office of the Assistant Secretary of Defense for Health Affairs
DoD CIO	DISA
Secretary of the Army	U.S. Army - Assistant Secretary of the Army (Acquisition, Logistics and Technology)
Secretary of the Navy	U.S. Navy U.S. Marine Corps
Secretary of the Air Force	U.S. Air Force U.S. Space Force

Table 1. DoD Stakeholders, Continued

Principal Staff Assistants and Secretaries of the Military Departments	Component
CJCS	United States Africa Command United States Central Command United States Cyber Command United States European Command United States Indo-Pacific Command United States Northern Command United States Southern Command United States Space Command United States Special Operations Command United States Strategic Command United States Transportation Command

(2) Figure 2 depicts DoD stakeholder roles during the CFIUS processes. For each CFIUS transaction, a DoD stakeholder can become a primary equity holder if it is determined that national security concerns exist with regard to the DoD stakeholder's equities.

Figure 2. DoD Stakeholder Participation in the CFIUS Process



d. DoD Communication Among Committee Members.

OASD(IBP) is the DoD's primary point of coordination for all DoD CFIUS matters with the CFIUS Chair, Committee members, and Parties. With DoD stakeholder roles in mind, as depicted in Figure 2, this paragraph details how DoD CFIUS case information should flow.

(1) The CFIUS Chair initiates transaction reviews, forwards follow-on transactional information, facilitates questions to the Parties to the transaction, and requests additional information from CFIUS members to facilitate the Committee's review and investigation. The

CFIUS Chair may also allow Parties to the transaction to withdraw a filing at any point in the CFIUS processes.

(2) OASD(IBP) reviews and distributes case materials from the Committee to DoD stakeholders. If the CFIUS staff or other CFIUS member requests information, OASD(IBP) responds to the request with the assistance from the relevant DoD stakeholders.

(3) If DoD stakeholders wish to ask questions of the Parties or to contact a CFIUS member, they establish contact with the Committee and Parties through OASD(IBP).

(a) DoD stakeholders may not contact the Parties, the CFIUS Chair, or the Committee directly regarding the transaction under any circumstances. Specific procedures for formulating questions can be found in the "Foreign Investment Review: CFIUS Question Formulation Instruction Guide for Stakeholders," available on request from USD(A&S).

(b) Some DoD stakeholders have existing authorities outside of CFIUS, such as certain NISP FOCI or export control authorities. Those DoD stakeholders may engage directly with the Parties if the engagement focuses on the transaction as it relates to those existing authorities outside of CFIUS.

(c) If any representative for the Parties to the transaction contacts a DoD Component directly regarding a CFIUS transaction, the DoD Component refers that representative to OASD(IBP).

(4) If any non-DoD Committee member contacts a DoD Component directly regarding a notified CFIUS transaction, the DoD Component refers that Committee member to OASD(IBP).

(5) If DoD is a CFIUS co-lead, OASD(IBP) may coordinate engagements with the Parties of the transaction and the other CFIUS co-lead agencies.

e. CFIUS Communication Within the DoD.

(1) This issuance provides the protocol for communication flow within the DoD throughout the CFIUS processes. OASD(IBP) is the primary point of coordination for all CFIUS matters within DoD. When a DoD stakeholder is notified of a CFIUS transaction and wishes to request the involvement of a DoD Component participant, that request is made through OASD(IBP).

(2) Some DoD stakeholders have existing authorities outside of CFIUS, such as certain NISP FOCI authorities. Those DoD stakeholders may engage directly with applicable DoD Components if the engagement focuses on the transaction as it relates to those existing authorities outside of CFIUS.

(3) Submission timelines and requirements for DoD stakeholders to inform DoD's position on a CFIUS case are as presented here and in Paragraphs 3.2., 3.3., and 3.4. Overarching timelines are dictated by statute (i.e., 30-day declaration process, 45-day national security review, 45-day national security investigation). Case days are calendar days, and the CFIUS staff accounts for weekends and Federal holidays when determining the case initiation

date (day 1) and the statutory deadlines. In accordance with the Section 4565 of Title 50, U.S.C., timelines are suspended in the case of a lapse in appropriations. The other DoD stakeholder timelines in this issuance are intended as guides to facilitate the DoD's ability to meet these statutory time limits.

(a) Upon receipt of case initiation from, and in coordination with OASD(IBP), DoD stakeholders review the case and forward case information to the subordinate offices that are best suited to provide subject matter expert advice to inform DoD stakeholders' inputs to OASD(IBP). The timeline and required DoD stakeholder deliverables for each element of the CFIUS process (declarations, national security review and investigation, monitoring, and non-notified) follow in Paragraphs 3.2., 3.3., and 3.4.

(b) OASD(IBP) coordinates with DoD stakeholders through their designated DoD Component points of contact and does not contact DoD Components' subordinate commands or field offices directly without a process previously approved by the DoD Component point of contact.

(c) DoD stakeholder input includes a statement explaining the reason behind their DoD Component's position on vulnerability and consequences of the covered transaction in terms of national security considerations or concerns.

(d) Due to the short statutory timelines for CFIUS work in accordance with Section 4565 of Title 50, U.S.C., the primary equity holders and equity holders must provide a declaration or covered transaction position approval signature within 5 business days following the request from OASD(IBP).

(e) OASD(IBP) formulates and synthesizes the consensus-based DoD position on all declarations and notified and non-notified CFIUS transactions in conjunction with other CFIUS executive agencies. In the rare event that consensus cannot be reached, a meeting with the ASD(IBP), CFIUS director, and the senior executive service–level representative of the non-concurring DoD Component or supporting organization, with technical support if desired, should be scheduled within 24 hours or as soon as feasible thereafter to attempt to reach consensus together. If consensus cannot then be reached, the ASD(IBP) refers the matter to the USD(A&S) for decision.

(f) Timeline requirements for primary equity holders involved in monitoring agreements are in Paragraph 3.5.

(4) All DoD participants in the CFIUS process use the statement provided in Figure 3 in electronic correspondence pertaining to CFIUS cases. If the correspondence involves DoD deliberations that contain controlled unclassified information or classified information, DoD participants adhere to procedures in DoD Instruction 5200.48 and Volume 2 of DoD Manual 5200.01.

Figure 3. CFIUS Electronic Correspondence Statement

The body of this e-mail or attached documents may contain sensitive information relating to the Committee on Foreign Investment in the United States (CFIUS). Public disclosure of CFIUS information is prohibited in accordance with Section 721(c)(1) of the Defense Production Act of 1950, as amended (50 U.S.C. § 4565(c)(1)), and penalties may apply to disclosures of such information.

3.2. CFIUS DECLARATION PROCESS AND DUE DILIGENCE.

a. Process Overview.

(1) The purpose of the declaration process is to identify national security considerations pertaining to a transaction. Pursuant to Section 4565 of Title 50, U.S.C., the Committee reviews all CFIUS declarations originating from four types of company transactions, which are required to be submitted to the Committee no later than 30 days before closing the transaction. (See Paragraph 3.2.b. for national security considerations.)

(2) OASD(IBP) disseminates declaration case materials to DoD stakeholders on day 1.

(3) DoD stakeholders provide a risk-based position on whether the transaction poses national security considerations that require further analysis to determine whether a transaction threatens or impairs national security.

(4) By day 21, DoD stakeholders complete their review and submit a final risk-based position and recommendations to OASD(IBP), observing:

(a) If OASD(IBP) suspects the existence of potential national security considerations, OASD(IBP) may reach out to DoD stakeholders to inquire about an initial disposition on or about day 11.

(b) If DoD stakeholders identify potential national security considerations before day 21, the DoD stakeholders inform OASD(IBP).

(5) On day 21, OASD(IBP) consolidates final DoD stakeholder recommendations to build DoD's risk-based position.

(6) By day 30, OASD(IBP) receives the basic threat information, produced by the Director of National Intelligence (DNI), through the CFIUS Chair. Upon receipt, OASD(IBP) disseminates the NSTA within 1 day to all DoD stakeholders for review.

(7) By day 30, OASD(IBP) provides DoD's risk-based position to the CFIUS Chair. If DoD is a CFIUS co-lead, a Presidentially appointed, Senate-confirmed (PAS) official will certify clearance, recommending either:

(a) No action—not enough information exists to completely identify a national security risk position.

(b) Safe harbor—there are no CFIUS-identified national security risk considerations. Clear the transaction; or

(c) National security risk considerations exist, prompting:

1. Request that Parties formally file a JVN (making the transaction a CFIUS transaction), leading to an in-depth national security review; or

2. Initiate a unilateral review of the transaction pursuant to Section 800.501(c) of Title 31, Code of Federal Regulations (CFR), leading to a national security review.

b. National Security Considerations.

DoD reviews the following factors that have potential national security considerations, with amplifying information presented in Table 2:

(1) The critical technology, infrastructure, or sensitive personal data described or implicated by the declaration.

(2) The nexus between the target U.S. company and the DoD.

(3) The existence of any proximity risk.

(4) Other information clearly indicating risk to national security.

Table 2. Transactions Requiring CFIUS Declarations

Transaction	Amplifying information in accordance with Parts 800 through 802 of Title 31, CFR
Transactions involving target U.S. companies involved in critical technologies, infrastructure, or sensitive personal data (collectively, U.S. technology, infrastructure, and data (TID) businesses)	Non-controlling rights give a foreign investor one or more of these rights: a. Access to any material, nonpublic technical information. b. Membership or observer rights on the board of directors or equivalent governing body of the U.S. business. c. The right to nominate an individual to a position on the board of directors or equivalent governing body of the U.S. business. d. Any involvement, other than through voting of shares, in or regarding substantive decision making of the U.S. business.
Transactions involving certain foreign government investments in a U.S. TID business	A Non-Excepted Foreign Acquirer: a. Obtains 25 percent or more voting interest in a TID business. b. The Non-Excepted Foreign Acquirer is 49 percent or more owned or controlled by a certain foreign government.
Transactions involving any purchase or lease by, or concession to, real estate in close proximity to military installations or DoD facilities as defined in Part 802 of Title 31, CFR	A Non-Excepted Foreign Real Estate Investor through investment or subsequent change or rights: a. Affords the foreign person at least three of the property rights: 1. To physically access the real estate; 2. To exclude others from physically accessing the real estate; 3. To improve or develop the real estate; or 4. To attach fixed or immovable structures or objects to the real estate.

3.3. NATIONAL SECURITY REVIEW AND DUE DILIGENCE.

a. Process Overview.

(1) The purpose of the national security review process is to identify national security concerns pertaining to the transaction. OASD(IBP) and DoD stakeholders conduct due diligence that considers statutory factors listed in Table 5.

(2) When the CFIUS Chair initiates a review and disseminates the JVN, OASD(IBP) disseminates the case materials to DoD stakeholders observing these milestones:

(a) On day 1, OASD(IBP) disseminates case materials to DoD stakeholders.

(b) By day 1, OASD(IBP) disseminates a one-page case summary to DoD stakeholders that identifies a preliminary list of equity holders whose equities, current or future, may be directly affected by the CFIUS transactions.

(c) If OASD(IBP) determines that the transaction involves DoD equities, OASD(IBP) requests CFIUS co-lead designation from the CFIUS Chair.

(3) By day 21, DoD stakeholders provide a final assessment of national security concerns to OASD(IBP).

(a) If DoD stakeholders with no equity or DoD stakeholders that are equity holders assess that there are no national security concerns, they have an affirmative obligation to send out a statement to OASD(IBP) providing the grounds for this position.

(b) If national security concerns exist, the equity holder(s) provide a statement outlining vulnerabilities and consequences arising from the transaction that includes information gaps or missing details necessary to conduct complete due diligence for the transaction. Each equity holder begins a detailed risk analysis in accordance with Paragraph 3.3.c.

1. If OASD(IBP) suspects the existence of national security concerns, OASD(IBP) may reach out to DoD stakeholders to inquire about an initial disposition on or about day 14.

2. If DoD stakeholders identify potential national security concerns before day 21, they inform OASD(IBP).

(4) By day 21, OASD(IBP) consolidates DoD stakeholder assessments to form the DoD's initial position on risk.

(a) OASD(IBP) designates the equity holders who identified potential national security concerns as primary equity holders. OASD(IBP) may designate more than one primary equity holder. At the time of designation and with the assistance of all primary equity holders, OASD(IBP) begins drafting an RBA.

(b) There are times when OASD(IBP) may assess that national security concerns exist for DoD even when DoD stakeholders do not. This occurs when the aggregation of

separate DoD stakeholder inputs reveals national security concerns. Under this circumstance, OASD(IBP) describes the concerns, consulting and coordinating with the relevant DoD stakeholder(s), as required.

(5) By day 30, OASD(IBP) receives the NSTA, produced by the DNI, through the CFIUS Chair. Upon receipt, OASD(IBP) disseminates the NSTA within 1 day to all DoD stakeholders for review.

(a) The NSTA provides an analysis of any threat that a covered transaction poses to U.S. national security.

(b) Defense Intelligence Components, as discussed in Paragraph 3.3.b., provide the ODNI with threat information for the transaction.

(6) By day 30, primary equity holders provide a final assessment of national security concerns to OASD(IBP).

(7) By day 30, OASD(IBP) consolidates the primary equity holders' RBA input and formulates the DoD's position on the transactions for internal coordination within the DoD.

(8) By day 45, internal DoD coordination concludes whether to proceed to the CFIUS investigation process and OASD(IBP) provides the recommendation to the Committee.

(a) If OASD(IBP) concludes that national security concerns exist, it notifies primary equity holders and equity holders and requests an investigation through the CFIUS Chair.

(b) If OASD(IBP) concludes that national security concerns do not exist, it provides DoD's signed determination, certification, or clearance letter to the CFIUS Chair in accordance with Table 3.

Table 3. Certification or Clearance During National Security Review

Certification or Clearance During National Security Review	DoD Co-Lead*	DoD Not a Co-Lead
Transaction results in Foreign Government Control	Deputy Secretary of Defense and other CFIUS agency co-leads sign a joint certification to Congress that the transaction will not impair national security of the United States.	USD(A&S) or PAS official sends a letter to the CFIUS Chair that the transaction will not impair the U.S. national security.
Transaction does not result in Foreign Government Control	USD(A&S) or PAS official signs joint certification to Congress confirming that there are no unresolved national security concerns.	USD(A&S) or PAS official provides a statement to the CFIUS Chair that the transaction will not impair U.S. national security.
*There are at least two CFIUS agency co-leads assigned to each case, one of which is always the Department of the Treasury.		

b. CFIUS Threat Assessments.

Threat assessment procedures for each CFIUS case are intelligence driven. For this reason, the threat assessment is conducted separately, but also in parallel with the vulnerability and consequence assessments. Pursuant to Section 4565 of Title 50, U.S.C., the DNI conducts an

analysis of any threat to the national security of the United States posed by any covered transaction and delivers that analysis to the Committee. ODNI provides an NSTA to the Committee not later than 30 days after the Department of the Treasury has accepted the case. The NSTA will help inform the CFIUS RBA.

(1) Defense Intelligence Component Inputs to the NSTA.

(a) Table 4 identifies Defense Intelligence Components. Each Component is responsible for providing the ODNI with threat information for filed CFIUS cases.

Table 4. Defense Intelligence Components Providing Input to NSTAs

Defense Intelligence Components
Air Force Office of Special Investigations
DCSA
DIA
Headquarters Department of Army G-2, Army Counterintelligence Center
Headquarters Marine Corps, Deputy Commandant for Information, Intelligence Division
National Air and Space Intelligence Center
National Ground Intelligence Center
Naval Criminal Investigative Service
Naval Intelligence Activity
NGA
NRO
NSA
Office of Naval Intelligence

(b) If the Defense Intelligence Components listed in Table 4 do not have any threat information pertinent to a specific case, each Component provides a written response to the ODNI indicating that it has no pertinent information.

(c) The Defense Intelligence Components in Table 4 engage with the ODNI in accordance with ODNI policies and procedures.

(2) Inputs Other Than Threat Information.

(a) Defense Intelligence Component participants provide the USD(I&S) with relevant inputs related to vulnerabilities and consequences as defined in this issuance.

(b) When Defense Intelligence Components provide vulnerability and consequence inputs to the ODNI, such inputs are included in the ODNI's assessment only to the extent that they illuminate the potential vulnerabilities that the threat actors may intend to exploit.

(3) NSTA Distribution.

(a) Once it receives the NSTA, OASD(IBP), within 1 day, forwards the NSTA to DoD stakeholders as appropriate, based on classification, mission relevancy, and a need-to-know basis.

(b) NSTA recipients may not disseminate or cite NSTA information under any circumstances other than during due diligence and risk analysis of notified CFIUS cases.

c. CFIUS RBA.

CFIUS has a statutory mandate to focus on risks to U.S. national security arising from a transaction. Therefore, OASD(IBP) analyzes the transaction to determine the new or incremental risk that would be realized because, and only because, of the transaction. In its analyses, the DoD uses a transactional risk analysis framework. This risk analysis supports determinations regarding potential mitigation. The transactional RBA framework is as follows:

(1) In accordance with Section 800.102 of Title 31, CFR and CFIUS regulations, an RBA includes credible evidence demonstrating the risk and an assessment of the threat, vulnerabilities, and consequences to national security related to a transaction.

(2) The determination of what constitutes a "threat" is a function of the intent and capability of a foreign entity to take action to impair U.S. national security. OASD(IBP) summarizes threats based on input in the NSTA or additional information provided by a Defense Intelligence Component listed in Table 4.

(3) "Vulnerabilities" refers to the extent to which the nature of the U.S. business presents susceptibility to impairment within the context of national security. OASD(IBP) bases the vulnerability portion of the analysis on:

(a) Subject-matter expertise of relevant DoD Component heads.

(b) All-source research.

(c) Information provided by the Parties to the transaction.

(d) Input from interagency CFIUS partners.

(4) The determination of what constitutes "consequences" to national security pertains to the potential effects that could reasonably result from exploiting the vulnerabilities by the threat actor. OASD(IBP) bases the consequence portion of the analysis primarily on the expertise of relevant DoD Components.

(5) As the DoD CFIUS staff organization, OASD(IBP) uses the result of the threat, vulnerability, and consequence assessments pertaining to one or more risk scenarios to reach a determination of the risks presented by each CFIUS transaction. These scenarios form the basis of a fully informed RBA.

d. Statutory Factors for Consideration.

Table 5 summarizes key RBA factors for consideration in CFIUS cases. Section 4565(f) of Title 50, U.S.C. sets forth the complete list of factors that CFIUS reviewers should consider in assessing the national security risks inherent in a proposed transaction. See Appendix 3A. Statutory factors include those prescribed in Section 4565 of Title 50, U.S.C. and FIRRMA's update with six additional factors that CFIUS may consider. Appendix 3A contains detailed lists of these factors.

Table 5. Factors for Consideration in RBA*

Type of Factors	Factor Details
Congressionally Mandated Risk-Analysis Factor Summary	a. The capability and capacity of domestic production and the industrial base (e.g., human resources, products, technology, and material) needed to meet national defense requirements. b. The effect that foreign control would have on the industrial base's ability to meet national defense requirements. c. The effects of the sale of goods, technology, or equipment that could support terrorism or the proliferation of other threats to the United States. d. The effects of transactions or real estate purchases that potentially expose critical infrastructure, facilities, installations, or properties to threats or foreign surveillance. e. Whether the transaction is a foreign government–controlled transaction and whether it involves a country of special concern that has a demonstrated or declared a strategic goal of acquiring a type of critical technology or critical infrastructure or has a potential for transshipment or diversion of technologies with military applications. f. The potential effects of cumulative control of, or pattern of recent transactions involving, any one type of critical infrastructure, energy asset, critical material, or critical technology by a foreign government or foreign person. g. Whether that foreign entity has a history of complying with U.S. laws and regulations. h. The effects of transactions that could threaten U.S. technological leadership or long-term access to sources of energy and other critical resources and material in areas affecting national security. i. The extent to which a transaction is likely to expose PII, genetic information, or other sensitive data of U.S. citizens to a foreign government or person. j. Whether a transaction is likely to worsen or create new cybersecurity vulnerabilities.
DoD Risk-Analysis Factors (not an all-inclusive list—RBAs should encompass all risks identified within the DoD or identified by DoD stakeholders)	a. Whether the target U.S. company: (1) Is subject to NISP governed by Volume 2 of DoD Manual 5220.32; (2) Produces defense critical technology or unique defense or law enforcement capabilities; (3) Is part of defense critical infrastructure; (4) Produces technology that provides such technological advantage to the United States that no mitigation to prevent technology transfer should even be attempted; or (5) Is a single-source or sole-qualified source supplier for DoD contracts, classified or unclassified, and whether it has technology with military applications. b. Whether this acquisition negatively affects the DoD Mission Assurance defense critical infrastructure line of effort in DoDD 3020.40. c. Existing or pending DoD or U.S. Government policies concerning a foreign country or government involved in the transaction, causing the transaction to pose a potential threat to U.S. interests.
*This list is not exhaustive.	

3.4. NATIONAL SECURITY INVESTIGATION AND DUE DILIGENCE.

a. Process Overview.

(1) The purpose of the national security investigation process is to address national security concerns pertaining to the transaction. Concerns can be resolved through additional due diligence, mitigation measures, and suspension or prohibition of the transaction.

(2) Although the statutory deadline for the investigation process is 45 days, Parties may withdraw and refile before the end of the period for several reasons, including the discovery of material changes to the filing or if national security concerns are not resolved before the statutory deadline.

(a) If the Parties refile, the CFIUS Chair assigns a new CFIUS case number and initiates either a new national security review or new investigation, as appropriate.

(b) OASD(IBP) notifies all DoD stakeholders about the transaction refiling on or before day 1 of the new national security review or investigation process and highlight any material changes to the filing and provide the updated materials to the DoD stakeholders.

(c) OASD(IBP) assumes that all DoD stakeholder inputs pertaining to the previous filing remains valid unless the DoD stakeholders indicate otherwise, in writing, no later than day 7 of the investigation or when additional facts arise from the investigation.

(3) For transactions that enter the investigation process from the review process:

(a) OASD(IBP) and DoD stakeholders continue to conduct due diligence that considers statutory factors listed in Table 5.

(b) Depending on the circumstances of each case, primary equity holders provide OASD(IBP) an outline of an RBA that describes the risk scenario that constitutes the basis for the DoD stakeholders' concerns at the end of the national security review or at the beginning of the national security investigation, in accordance with Paragraph 3.3.c.

(c) Based on the input and with the assistance of primary equity holders, OASD(IBP) develops a fully informed RBA. OASD(IBP):

1. Strives to present the strongest possible analysis on behalf of the DoD stakeholders expressing national security concerns.

2. Exercises final editorial control over each equity holder risk analysis to facilitate the presentation of the DoD's most rigorously supported analysis.

3. Coordinates with primary equity holders on the RBA to ensure that DoD stakeholder concerns and details are accurately represented.

(d) Depending on the circumstances of each case, OASD(IBP) presents DoD's RBA to the CFIUS at the end of the national security review or at the beginning of the national security investigation.

(e) Committee members review and provide written comments on DoD's RBA, and OASD(IBP) addresses those comments. Primary equity holders assist OASD(IBP) in resolving or addressing the Committee members' comments.

(4) Once the Committee reaches consensus on the RBA outcome, that the transactions give rise to DoD-related national security risks, OASD(IBP) presents a mitigation plan to CFIUS addressing all identified risks. Accordingly:

(a) Primary equity holders provide the appropriate subject-matter expertise to assist in determining the necessity, feasibility, appropriateness, and nature of any mitigation option and make recommendations as appropriate and necessary.

(b) OASD(IBP) derives mitigation plans from the RBA, prepared in accordance with Paragraph 3.3.c., and coordinates the plans with primary equity holders.

(c) During mitigation planning, OASD(IBP), primary equity holders, and equity holders ensure that no adequate alternate statutory authority (i.e., other than CFIUS) adequately addresses the identified national security risks, pursuant to Executive Order 11858.

(d) By day 30 of the investigation, OASD(IBP) prepares and forward a final mitigation plan or recommendation for Presidential decision to the CFIUS.

(5) If applicable, OASD(IBP), assisted by the CFIUS Chair and other co-lead agencies, negotiates mitigation terms with subject companies to ensure that the terms are adequate to resolve the national security concerns associated with the transaction.

(a) If national security concerns are resolved during negotiations without the need for implementing mitigation terms, OASD(IBP) provides clearance justification in the DoD's decision package. Primary equity holders provide coordination and identify how their security concerns have been resolved absent CFIUS mitigation.

(b) If the Parties accept the final mitigation terms, primary equity holders provide coordination on the DoD CFIUS decision package affirming that their national concerns have been resolved.

(c) If OASD(IBP) obtains a mitigation agreement to address a primary equity holder's national security concerns, then that primary equity holder becomes a monitoring component for that particular agreement and assists OASD(IBP) in monitoring the Parties' compliance with the agreement.

(d) If the companies involved in a CFIUS transaction do not agree on mitigation terms and refuse to withdraw the case from CFIUS consideration and abandon the transaction, then the CFIUS may:

1. Unilaterally impose mitigation terms on the company; or

2. At its discretion, refer the transaction for Presidential action.

(e) OASD(IBP) provides the DoD's signed certification or clearance letter to the CFIUS Chair in accordance with Table 6.

(6) OASD(IBP) prepares and sends an RBA to the Department of the Treasury and supports the Department of the Treasury's drafting of an interim order to mitigate risks to national security in an expedited manner for transactions that threaten national security and cannot be delayed until the full process in this section is followed. These expedited national security cases may include non-notified transactions whose exposed risk, if exploited, could cause serious national security consequences before the filing or resolution of the CFIUS case.

Table 6. Certification or Clearance During National Security Investigation

Certification or Clearance During National Security Investigation	DoD Co-Lead	DoD Not a Co-Lead
Transaction results in Foreign Government Control	Deputy Secretary of Defense and other CFIUS agency co-leads sign a joint certification to the Congress that there are no unresolved national security concerns.	USD(A&S) or PAS official sends a letter to the CFIUS Chair certifying that the DoD has no unresolved national security concerns.
Transaction does not result in Foreign Government Control	Deputy Secretary of Defense and other CFIUS agency co-leads sign a joint certification to the Congress that there are no unresolved national security concerns.	USD(A&S) or PAS official sends a letter to the CFIUS Chair certifying that the DoD has no unresolved national security concerns.

(7) If the Committee agrees to support the suspension or prohibition of a transaction, OASD(IBP) assists the CFIUS Chair in the preparation of materials for the President's consideration. The Primary equity holder(s) assist OASD(IBP) in this preparation.

(8) In accordance with Section 4565 of Title 50, U.S.C., the President may take such action as the President considers appropriate, including directing the divestment, suspension, or prohibition of the transaction.

b. Mitigation Guide.

(1) OASD(IBP) maintains a CFIUS Mitigation Guide that provides insight and guidance into DoD CFIUS mitigation methods used in CFIUS national security agreements. The CFIUS Mitigation Guide explains the most commonly used CFIUS mitigation concepts and the different terms used to address common risk scenarios presented in CFIUS transactions. Accordingly, the CFIUS Mitigation Guide addresses these national security issues arising from CFIUS transactions, including:

(a) Technology transfer.

(b) Data protection and cybersecurity.

(c) Product integrity.

(d) Co-location.

(e) Supply assurance.

(2) The CFIUS Mitigation Guide is not intended to be an exhaustive list of terms and risk-scenarios facing the DoD; as such, it is updated annually with improved mitigation terms as they are developed in the course of implementing and monitoring mitigation agreements.

3.5. CFIUS COMPLIANCE MONITORING PROCESS.

On behalf of the DoD, in consultation with the Office of General Counsel of the Department of Defense, and in coordination with the primary equity holders and other relevant components, OASD(IBP) monitors compliance for all agreements to which the DoD is a party.

a. The purpose of compliance monitoring is to track and monitor the terms of the national security agreements between the Parties and the Committee through the life of the agreement(s). If the DoD is a co-lead agency for a given case, the ASD(IBP) leads compliance monitoring responsibilities for the DoD.

b. OASD(IBP) performs due diligence to ensure that a Party or Parties to a national security agreement fully comply with the letter and spirit of its terms and conditions and assesses any post-transaction changes that may raise national security considerations.

c. After a final national security agreement is signed, OASD(IBP):

(1) Develops an enforcement regimen that captures the national security concern description and associated mitigation measures.

(2) Designates primary equity holder(s) to support monitoring activities.

(3) Establishes contact with the Parties and their representatives to establish monitoring protocols.

d. With the primary equity holders' support, the ASD(IBP):

(1) Captures the Parties' compliance deliverables.

(2) Reviews each Party's submissions to ensure that submissions comply with the mitigation agreement.

(3) Identifies questions or information gaps that need attention or completion.

(4) Responds to the Parties for the DoD.

(5) Requests agreed-upon deliverables provided by the Parties for both routine and event-driven actions, then establishes scope and timeline for non-routine deliverables.

(6) Submits a formal written reminder to the Parties of their obligations or requests a written update on compliance matters within a specified time.

(7) Takes appropriate actions to address potential material breaches of mitigation obligations.

e. OASD(IBP) creates a plan for site visits and coordinates the schedule with primary equity holders' monitoring components and relevant compliance participants from other CFIUS member agencies, as well as with the Parties to the agreements.

(1) Many risk mitigation agreements include terms enabling the DoD to visit the commercial Parties' facilities to assess the Parties' compliance with their agreement obligations.

(2) Within 1 year of a new agreement's effective date, OASD(IBP) and the primary equity holders' monitoring components conduct a site visit to an appropriate location to make an initial assessment of the Parties' implementation of the mitigation agreement.

(3) Upon completion of a site visit, OASD(IBP) produces a feedback letter that documents the Parties' compliance with ongoing obligations with respect to the national security agreement, as appropriate. OASD(IBP) provides the feedback letter to the Parties, CFIUS, and primary equity holders.

f. OASD(IBP) directs regular reassessments of risk for the DoD's monitoring of active cases. On a regular basis, but no later than every 5 years from the effective date of each agreement, OASD(IBP) and the primary equity holder monitoring component(s) for specific mitigation agreements reassess the risks arising from the transactions, in accordance with Paragraph 3.5. Although these reassessments must be done at least once every 5 years, they may require a greater frequency given the needs of a particular transaction, including, but not limited to, national security concerns. Accordingly:

(1) The Office of the USD(I&S), via the DIA, provides a revised threat assessment of the transaction as input to the risk reassessments.

(2) In addition to the factors for consideration in Paragraph 3.5., reassessments will include the Parties' record of historical compliance with their mitigation agreement(s).

(3) If OASD(IBP) and the monitoring components determine that the risk arising from the transaction has changed, such that the existing mitigation agreement is no longer necessary, then they make a recommendation to the Committee to terminate the agreement.

3.6. CFIUS NON-NOTIFIED TRANSACTION PROCESS.

The purpose of the non-notified process is to identify proposed and completed foreign acquisitions of, or investments in, U.S. businesses for which no voluntary notice has been filed that may be a covered transaction, raise national security considerations, or be a transaction designed or intended to evade CFIUS regulations.

a. Non-notified transactions may become formal CFIUS transactions and thus undergo a national security review by means of either a JVN, submitted by the U.S. companies themselves

after the CFIUS Chair requests one, or as a result of a unilateral agency notice filed by a Committee member without the voluntary participation by the companies.

b. OASD(IBP) identifies CFIUS non-notified transactions that pose national security considerations through various methods including, but not limited to, utilizing various databases, searching through open-source media, and through various outreach programs.

(1) OASD(IBP) collaborates with other CFIUS agencies to identify and review non-notified transactions.

(2) DoD stakeholders are key partners in discovering non-notified transactions and submit any identified non-notified transaction to OASD(IBP) for evaluation to pursue potential CFIUS action.

(3) Non-notified transactions submitted by DoD stakeholders include all known facts of the transaction and a description of the potential national security considerations involved.

c. OASD(IBP) evaluates the non-notified transaction within the transactional risk analysis framework described in Paragraphs 3.3.c. and 3.3.d., using information from equity holder inputs and open, commercial, and classified sources to determine:

(1) Whether the transaction appears to be a "covered transaction" in accordance with Section 4565(a)(4) of Title 50, U.S.C.

(2) The extent to which the DoD has a specific equity to be addressed by CFIUS, including whether the transaction raises the potential for national security considerations for the DoD.

(3) Whether there are additional factors to match those highlighted in Table 5.

d. If there is reason to believe that the transaction is covered and raises potential national security considerations, OASD(IBP) may identify DoD stakeholders to review the transaction to identify whether the transaction may threaten national security. DoD stakeholder responses identify any national security considerations arising from the non-notified transaction affecting their mission and responsibilities.

e. If necessary, throughout the evaluation, OASD(IBP) develops a set of questions to better understand both the transaction and the underlying effects the acquisition may have on U.S. national security.

f. If OASD(IBP) determines that the transaction is a covered transaction that raises potential national security considerations, OASD(IBP) submits the non-notified transaction to the CFIUS Chair for the Committee's consideration. The ASD(IBP) may recommend:

(1) That the CFIUS Chair request the companies involved in a non-notified transaction provide CFIUS with information sufficient to determine whether the transaction is covered. OASD(IBP) forwards the questions developed during OASD(IBP)'s evaluation period to the CFIUS Chair.

(2) That a unilateral agency filing with CFIUS is required to the USD(A&S) or equivalent official. The DoD stakeholder(s) provide input to the unilateral agency filing decision recommendation for the USD(A&S).

g. OASD(IBP) continues to track non-notified transactions submitted to the CFIUS Chair until the Committee determines:

(1) The transaction is not covered;

(2) National security considerations do not exist; or

(3) The transaction enters the declarations or national security review process.

3.7. DEFENSE CFIUS COORDINATION GROUP.

a. Purpose, Membership, and Organization.

(1) The Defense CFIUS Coordination Group convenes at both the DoD Component–leadership level (e.g., general officer/flag officer or senior executive service participants) and senior-staff level (e.g., O-6 or General Schedule-15 participants). These quarterly meetings facilitate training, collaboration, and information sharing among all DoD Components that participate in DoD CFIUS operations.

(2) The purpose of the Defense CFIUS Coordination Group at both levels is to improve executing the DoD's CFIUS mission by virtue of routine, well-planned, and organized meetings at which the members share insights, common goals, and lessons learned to constantly improve the DoD's CFIUS mission.

(3) The ASD(IBP) is the vital group leader and organizer.

(4) DoD stakeholders and Defense Intelligence Components contributing threat information to ODNI are members of the Defense CFIUS Coordination Group.

(5) As appropriate, the Defense CFIUS Coordination Group may also organize itself into working groups, subgroups, or panels as necessary to accomplish its mission.

b. Meetings.

The Defense CFIUS Coordinating Group and any working groups may hold regular and *ad hoc* meetings called by the ASD(IBP) either unilaterally or in response to member suggestions.

APPENDIX 3A. RISK ANALYSIS FACTORS AND CONSIDERATIONS

Table 7. National Security Factors for Inclusion in DoD RBAs When Applicable

	National Security Factors for Inclusion in DoD RBAs When Applicable
1.	The domestic production that would be needed for projected national defense requirements.
2.	The capability and capacity of domestic industries to meet national defense requirements, including the availability of human resources, products, technology, material, and other supplies and services.
3.	The control of domestic industries and commercial activity by foreign citizens as it affects the capability and capacity of the United States to meet the requirements of national security.
4.	The potential effects of the proposed or pending transaction on sales of military goods, equipment, or technology to any country that supports terrorism or any country that is of concern regarding missile, chemical-weapons, or biological-weapons proliferation.
5.	The potential effects of the transaction on potential or pending U.S. international technological leadership in areas affecting U.S. national security.
6.	The potential national security–related effects of the transaction on U.S. critical infrastructure, including major energy assets.
7.	The potential national security–related effects of the transaction on U.S. critical technologies.
8.	Whether the covered transaction is a foreign government–controlled transaction.
9.	Whether the transaction is a foreign government–controlled transaction, namely, whether the acquirer is controlled by, or acting on behalf of, a foreign government.
10.	When appropriate, and particularly with respect to foreign government–controlled transactions requiring further investigation: (1) Adherence of the subject country to nonproliferation control regimes, including treaties and multilateral supply guidelines. (2) The relationship of such a country with the United States, specifically its record on cooperating in counter-terrorism efforts. (3) The potential for transshipment or diversion of technologies with military applications, including an analysis of national export control laws and regulations.
11.	The long-term projection of the United States' requirements for sources of energy and other critical resources and material.
12.	Such other factors as the President or the Committee determine to be appropriate.

Table 8. FIRRMA Risk-Analysis Factors Reflecting the "Sense of Congress"

	FIRMMA Risk-Analysis Factor Reflecting the "Sense of Congress" Details*
1.	Covered transactions that involve 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.
2.	The potential national security–related effects of the cumulative control of, or pattern of recent transactions involving, any one type of critical infrastructure, energy asset, critical material, or critical technology by a foreign government or person.

Table 8. FIRRMA Risk-Analysis Factors Reflecting the "Sense of Congress," Continued

	FIRMMA Risk-Analysis Factor Reflecting the "Sense of Congress" Details
3.	Whether any foreign person engaged in a transaction has a history of complying with U.S. laws and regulations.
4.	Control of U.S. industries and commercial activity that affect U.S. capability and capacity to meet the requirements of national security, including the availability of human resources, products, technology, materials, and other supplies and services.
5.	The extent to which a transaction is likely to expose PII, genetic information, or other sensitive data of U.S. citizens to access by a foreign government or person that may exploit that information to threaten national security.
6.	Whether a transaction is likely to exacerbate or create new cybersecurity vulnerabilities or is likely to result in a foreign government gaining a significant new capability to engage in malicious cyber-enabled activities.
* While the Sense of Congress language in FIRRMA reflects congressional intent and does not have the force and effect of law, these factors have informed DoD RBAs that led to mitigation or positions that recommend prohibition.	

Table 9. DoD Risk Analysis Factors and Considerations

	DoD Risk Analysis Factor and Consideration Details*
1.	Whether the target U.S. company produces a critical technology, a critical infrastructure asset, a law enforcement asset, and/or a unique defense or infrastructure capability.
2.	Whether the target U.S. company produces technology that is unique and would provide such technological advantage to the United States that no mitigation measure to prevent technology transfer should even be attempted. In this case, the acquisition by a foreign entity will be precluded.
3.	Whether the target U.S. company is a single-source or sole-qualified source supplier for DoD contracts, classified or unclassified, and whether it has technology with military applications.
4.	Whether the target U.S. company is part of, or owns, defense critical infrastructure.
5.	Whether this acquisition negatively impacts the DoD Mission Assurance defense critical infrastructure line of effort as established in DoDD 3020.40.
6.	Whether the target U.S. company is subject to the provisions of NISP governed by Volume 2 of DoD Manual 5220.32.
7.	Whether any identified national security concerns posed by the transaction may be eliminated or reduced to tolerable levels by the application of risk mitigation measures under existing DoD issuances, other statutes, or by means of CFIUS mitigation agreements entered into through negotiation with the Parties.
8.	Whether there are current or upcoming DoD functional or regional concerns or applicable policies or strategies regarding any of the foreign countries and/or governments involved in the transaction that might pose a potential regional threat to U.S. interests, and which would therefore require at a minimum an assessment by the OSD regional office director as to whether the country involved means that the transaction needs special and further evaluation to ensure alignment with White House policies and strategies.
*This list is not all inclusive.	

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
ASD(A)	Assistant Secretary of Defense for Acquisition
ASD(IBP)	Assistant Secretary of Defense for Industrial Base Policy
ASD(NCB)	Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs
ASD(S)	Assistant Secretary of Defense for Sustainment
CFIUS	Committee on Foreign Investment in the United States
CFR	Code of Federal Regulations
CJCS	Chairman of the Joint Chiefs of Staff
DCMA	Defense Contract Management Agency
DCSA	Defense Counterintelligence and Security Agency
DDRE	Director of Defense Research and Engineering
DIA	Defense Intelligence Agency
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DISA	Defense Information Systems Agency
DNI	Director of National Intelligence
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DTSA	Defense Technology Security Administration
e-mail	electronic mail
FIRRMA	Foreign Investment Risk Review Modernization Act of 2018
FOCI	foreign ownership, control, or influence
JVN	joint voluntary notification
MDA	Missile Defense Agency
NGA	National Geospatial-Intelligence Agency
NISP	National Industrial Security Program
NRO	National Reconnaissance Office
NSA	National Security Agency
NSTA	national security threat assessment

ACRONYM	MEANING
OASD(IBP)	Office of the Assistant Secretary of Defense for Industrial Base Policy
ODNI	Office of the Director of National Intelligence
PAS	Presidentially appointed, Senate-confirmed
PII	personally identifiable information
RBA	risk-based analysis
TID	technology, infrastructure, and data
U.S.C.	United States Code
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USD(R&E)	Under Secretary of Defense for Research and Engineering

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
agency filing	A filing submitted to the Committee by a CFIUS agency involving a non-notified transaction.
basic threat information	The formal written memorandum that outlines basic threat analysis of a declaration. Basic threat information production is drafted by the National Intelligence Council and is not coordinated within the Intelligence Community. It should not be construed as representing the Intelligence Community's final or authoritative threat judgement regarding the subject transaction.
CFIUS	An interagency committee, statutorily mandated to review transactions that could result in control of a U.S. business or real estate by a foreign person. CFIUS makes determinations as to the effect of such transactions on U.S. national security. The Secretary of the Treasury serves as the Chair of CFIUS.

TERM	DEFINITION
CFIUS non-notified transaction	A transaction for which the Parties have not filed a voluntary notice with CFIUS pursuant to Part 800 of Title 31, CFR.
close proximity	Defined in Section 802.203 of Title 31, CFR.
consequence	A term with statutory significance that pertains to the nature, level, and duration of effects resulting from the exploitation of possible or actual U.S. vulnerabilities affected or caused by assessed threats under the purview of the CFIUS statute and regulations.
country of special concern	In accordance with FIRRMA, a country 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.
covered transaction	Defined in Section 4565(a)(4) of Title 50, U.S.C.
critical infrastructure	Defined in Section 4565(a)(5) of Title 50, U.S.C.
critical technology	Defined in Section 800.215 of Title 31, CFR.
declaration	Abbreviated short-form CFIUS filing.
defense industrial base	Defined in Section 236.2 of Title 32, CFR.
DoD stakeholder	A DoD Component representative having a vested interest in a potential or completed transaction.
due diligence	An investigation, audit, or review performed to confirm the facts of a matter under consideration.
equity holder	A DoD Component representative who potentially has equity in a CFIUS transaction and reviews it to determine if national security concerns exist in accordance with this issuance.
joint certification	A notice or report, prepared by the Department of the Treasury, for certification and transmission to certain Members of Congress pursuant to Section 4565(b)(3) of Title 50, U.S.C. The Chair and the co-lead agency or agencies certify the notice or report.

TERM	DEFINITION
JVN	A written notice provided by companies pursuant to Section 4565 of Title 50, U.S.C. and Section 800.402 of Title 31, CFR, which describes either a proposed or completed transaction.
mitigation agreement	A legally binding agreement entered into between one or more CFIUS members and any Party to a covered transaction in order to mitigate risk to U.S. national security that arises as a result of the covered transaction not resolved under existing statutory authorities.
monitoring component	A DoD Component head primary equity holder who has raised national security concerns regarding a CFIUS case that is the subject of a subsequent mitigation agreement.
national security concerns	Defined on Page 74568 of Volume 73, Federal Register.
national security investigation	The statutorily mandated 45 business day second stage inquiry into a CFIUS transaction pursuant to Section 4565 of Title 50, U.S.C.
national security review	The initial statutorily mandated 45 business day evaluation period of a CFIUS Transaction, pursuant to Section 4565 of Title 50, U.S.C. The period begins on the date of acceptance of a JVN submitted by the company to the CFIUS Chair.
non-excepted foreign acquirer	Foreign investors who are required to file mandatory foreign government declarations and who have not been designated as "excepted" investors by CFIUS.
NSTA	The formal written document that outlines the Intelligence Community wide assessment of threat for each transaction. NSTA production is coordinated by the Investment Security Group of the Economic Security and Financial Intelligence Executive within the ODNI.
parties or party to a transaction	Defined in Section 800.236 of Title 31, CFR.
primary equity holder	A DoD Component head representative who determines that national security concerns exist within its respective area(s) of concern.

TERM	DEFINITION
RBA	An evaluation that the DoD submits to CFIUS providing credible evidence demonstrating a risk; this includes assessments of the threat, vulnerabilities, and consequences to national security issues related to a CFIUS transaction. DoD conducts its RBAs using the transactional risk analysis framework.
risk	The potential for an adverse outcome to national security of the United States assessed as a function of threats, vulnerabilities, and consequences associated with a transaction. Any determination of the CFIUS with respect to a covered transaction to suspend, refer to the President, negotiate, enter into or impose, or enforce any mitigation agreement or condition pursuant to Section 4565 of Title 50, U.S.C. will be based on a RBA of the effects on the CFIUS transaction.
safe harbor	When a transaction can proceed without the possibility of subsequent suspension or prohibition pursuant to Section 4565 of Title 50, U.S.C. A transaction may be granted safe harbor if it was a covered transaction that has been notified to CFIUS, and on which CFIUS has concluded action pursuant to Section 4565 of Title 50, U.S.C., after determining that there were no unresolved national security concerns.
sensitive personal data	Defined in Section 800.241 of Title 31, CFR.
target U.S. company	A U.S. business, including current subsidiaries of foreign companies present in the United States, that is subject to foreign control pursuant to merger, acquisition, or any other transaction with any foreign business.
threat	A risk or danger that is a function of the intent of actors associated with the transaction to take actions detrimental to U.S. national security; the technical and organizational capability of those actors to exploit the vulnerabilities presented by the transaction; and the access those actors have to the acquirer and thus which target the United States through the transaction.
transaction	Defined in Section 800.210–213 of Title 31, CFR and discussed in Section 800.303–304 of Title 31, CFR.

TERM	DEFINITION
transactional risk analysis framework	The methodological approach that the DoD uses in order to assess the likelihood, nature, and magnitude of risks to U.S. national security arising from a given transaction. The transactional risk analysis framework combines threat, vulnerability, and consequences pertaining to one or more risk scenarios.
unilateral national security review	Lacking a voluntary filing, CFIUS can unilaterally initiate a national security review of a covered transaction even if a transaction has closed.
U.S. business	Defined in Section 800.252 of Title 31, CFR.
U.S. TID business	Defined in Section 800.248 of Title 31, CFR.
vulnerabilities	Attributes of the target U.S. company's products, services, intellectual property, market position, business relationships, and operating locations that leave it open or susceptible to exploitation by a controlling entity.

REFERENCES

Code of Federal Regulations, Title 31

Code of Federal Regulations, Title 32, Section 236.2

Deputy Secretary of Defense Memorandum, "Establishment of the Office of the Assistant Secretary of Defense for Industrial Base Policy," February 10, 2022

DoD Directive 3020.40, "Mission Assurance (MA)," November 29, 2016, as amended

DoD Directive 5100.01, "Functions of the Department of Defense and Its Major Components," December 21, 2010, as amended

DoD Directive 5135.02, "Under Secretary of Defense for Acquisition and Sustainment (USD(A&S))," July 15, 2020

DoD Instruction 4180.02, "Implementation and Management of the DoD Mission Compatibility Evaluation Process," March 31, 2016, as amended

DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020

DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of Information," February 24, 2012, as amended

DoD Manual 5220.32, Volume 2, "National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)," April 17, 2014, as amended

Executive Order 11858, "Foreign Investment in the United States," May 7, 1975, as amended

Executive Order 13913, "Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector," April 4, 2020

Federal Register, Volume 73, Page 74568, December 8, 2008

Office of the Deputy Assistant Secretary of Defense for Industrial Policy, "CFIUS Mitigation Guide," September 11, 2020, current edition[1]

Office of the Deputy Assistant Secretary of Defense for Industrial Policy, "Foreign Investment Review: CFIUS Question Formulation Instruction Guide for Stakeholders," June 9, 2020[1]

Public Law 115-232, Title XVII, Subtitle A, "Foreign Investment Risk Review Modernization Act of 2018," August 13, 2018

United States Code, Title 10

United States Code, Title 50

[1] Available on request from the USD(A&S) for Industrial Base Policy Foreign Investment Review.