



Department of Defense INSTRUCTION

NUMBER 2000.25

August 5, 2010

Incorporating Change 1, August 31, 2018

USD(A&S)

SUBJECT: DoD Procedures for Reviewing and Monitoring Transactions Filed with the Committee on Foreign Investment in the United States (CFIUS)

References: See Enclosure 1

1. PURPOSE. This Instruction establishes policy, assigns responsibilities, and provides instructions in accordance with the authority provided in DoD Directive (DoDD) 5111.1 (Reference (a)) for DoD CFIUS reviews required by section 2170 of title 50, United States Code (U.S.C.) (Reference (b)), which determine the effects on national security of foreign acquisitions of U.S. companies. It also establishes the DoD CFIUS Monitoring Committee and prescribes procedures for establishing and monitoring mitigation agreements that are negotiated to permit the conclusion of specific CFIUS acquisitions.

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

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. Foreign acquisitions of U.S. companies that do not pose an unacceptable level of risk to U.S. national security interests, as manifested in DoD programs, assets, or future technological superiority, are acceptable to the Department of Defense.

b. The DoD CFIUS process should, to the extent possible, be a transparent process.

c. The potential implications for relevant DoD programs, assets, and future technological superiority resulting from a foreign acquisition involving a defense supplier, defense-related technologies, and infrastructure critical for DoD missions shall be based on:

(1) The impact to U.S. national security interests, technologies, and infrastructures critical to DoD missions, the defense industrial base, the presence of any classified operations within the company being purchased, and any other concerns that a transaction poses.

(2) At a minimum, but are not limited to, the factors found in Enclosure 4 of this Instruction.

d. The risk to DoD interests in each CFIUS case will be assessed pursuant to Enclosure 5 of this Instruction.

e. Information or documentary material filed with CFIUS shall be exempt from disclosure pursuant to section 552 of title 5, U.S.C. (also known and hereafter referred to as “The Freedom of Information Act, as amended” (FOIA) (Reference (c)) and will not be made public due to the statutory protections in Reference (a).

f. The Department of Defense shall monitor company compliance with CFIUS mitigation agreements signed with the Department of Defense as described in Enclosure 6.

g. Adequate resources, in terms of staff and budget, should be provided to the DoD Components for monitoring and ensuring compliance to mitigation agreements with the Department of Defense to protect national security interests.

h. DoD Components that are members of the Intelligence Community will also fulfill their alternate role in providing additional support and information to the Office of the Director of National Intelligence (ODNI) as required pursuant to Reference (a).

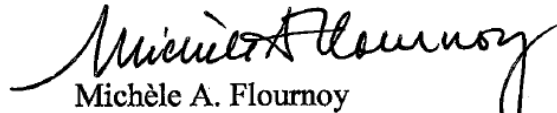
5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. DoD procedures for reviewing CFIUS transactions to determine any national security concerns following their receipt from the Department of the Treasury are found in Enclosure 3.

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

8. SUMMARY OF CHANGE 1. This change reassigns the office of primary responsibility for this instruction to the Under Secretary of Defense for Acquisition and Sustainment in accordance with the July 13, 2018 Deputy Secretary of Defense Memorandum (Reference (d)).

9. EFFECTIVE DATE. This Instruction is effective immediately.


Michèle A. Flournoy
Under Secretary of Defense for Policy

Enclosures

1. References
 2. Responsibilities
 3. Procedures
 4. DoD CFIUS Security Assessment Strategy
 5. DoD CFIUS Mitigation Review Methodology
 6. DoD CFIUS Monitoring Strategy and Responsibility and Role of DoD CFIUS Monitoring Committee
 7. DoD CFIUS Review Procedure Diagram
- Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....6

ENCLOSURE 2: RESPONSIBILITIES.....7

 UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)).....7

 DIRECTOR, DEFENSE TECHNOLOGY SECURITY ADMINISTRATION (DTSA)7

 DUSD(PI&CoS)8

 DEPUTY UNDER SECRETARY OF DEFENSE FOR STRATEGY, PLANS, AND
 FORCE DEVELOPMENT8

 ASSISTANT SECRETARY OF DEFENSE FOR INTERNATIONAL SECURITY
 AFFAIRS8

 ASSISTANT SECRETARY OF DEFENSE FOR ASIAN AND PACIFIC SECURITY
 AFFAIRS (ASD(A&PSA))8

 ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND
 AMERICAS’ SECURITY AFFAIRS (ASD(HD&ASA))9

 DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR WESTERN HEMISPHERE
 AFFAIRS9

 ASSISTANT SECRETARY OF DEFENSE FOR GLOBAL STRATEGIC AFFAIRS
 (ASD(GSA))9

 USD(AT&L).....9

 DIRECTOR, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY10

 DIRECTOR, SPECIAL PROGRAMS10

 DIRECTOR, DEFENSE LOGISTICS AGENCY10

 DIRECTOR, MISSILE DEFENSE AGENCY10

 UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)).....10

 DIRECTOR, NATIONAL SECURITY AGENCY (NSA)11

 DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA)11

 DIRECTOR, NATIONAL RECONNAISSANCE OFFICE (NRO)11

 ASD(NII)/DoD CIO.....11

 DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA)12

 GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE12

 HEADS OF THE DoD COMPONENTS12

 SECRETARIES OF THE MILITARY DEPARTMENTS.....14

 CHAIRMAN OF THE JOINT CHIEFS OF STAFF14

 COMMANDERS OF THE COMBATANT COMMANDS15

ENCLOSURE 3: PROCEDURES.....16

ENCLOSURE 4: DoD CFIUS SECURITY ASSESSMENT STRATEGY21

ENCLOSURE 5: DoD CFIUS RISK AND MITIGATION METHODOLOGY24

ENCLOSURE 6: DoD CFIUS MONITORING STRATEGY AND RESPONSIBILITY AND
 ROLE OF DoD CFIUS MONITORING COMMITTEE26

GLOSSARY30

 ABBREVIATIONS AND ACRONYMS30

 DEFINITIONS.....30

TABLE

 DoD CFIUS Reviewers.....29

FIGURE

 DoD CFIUS Review Process28

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5111.1, “Under Secretary of Defense for Policy (USD(P)),” December 8, 1999
- (b) Section 2170 of title 50, United States Code
- (c) Section 552 of title 5, United States Code (also known as “The Freedom of Information Act, as amended”)
- (d) Deputy Secretary of Defense Memorandum, “Establishment of the Office of the Under Secretary of Defense for Research and Engineering and the Office of the Under Secretary of Defense for Acquisition and Sustainment,” July 13, 2018
- (e) DoD Directive 5105.72, “Defense Technology Security Administration (DTSA),” July 28, 2005
- (f) DoD Directive 3020.40, “DoD Policy and Responsibilities for Critical Infrastructure,” January 14, 2010
- (g) DoD 5220.22-R, “Industrial Security Regulation,” December 4, 1985
- (h) Executive Order 11858, “Foreign Investment in the United States,” January 23, 2008
- (i) Part 800 of title 31, Code of Federal Regulations
- (j) Parts 120.6, 120.9, and 121.1 of title 22, Code of Federal Regulations
- (k) Part 774 of title 15, Code of Federal Regulations
- (l) Part 110 of title 10, Code of Federal Regulations
- (m) Part 331 of title 7, Code of Federal Regulations
- (n) Part 121 of title 9, Code of Federal Regulations
- (o) Part 73 of title 42, Code of Federal Regulations

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) shall oversee and establish policies for DoD's participation in CFIUS national security reviews and for monitoring transactions filed with CFIUS.

2. DIRECTOR, DEFENSE TECHNOLOGY SECURITY ADMINISTRATION (DTSA). The Director, DTSA, under the authority, direction, and control of the USD (P), and pursuant to its responsibilities under DoD Directive (DoDD) 5105.72 (Reference (e)), shall in addition to the responsibilities in section 22 of this enclosure:

a. Develop DoD policies and procedures for reviewing and monitoring transactions filed with the CFIUS.

b. Represent the Department of Defense on CFIUS issues that are not raised to the Deputy Under Secretary of Defense for Policy Integration and Chief of Staff (DUSD(PI&COS)).

c. Serve as the primary DoD point of contact for the CFIUS Chair for all issues to include: forwarding queries to the companies filing with CFIUS; attending interagency meetings regarding CFIUS filings; and deciding procedural CFIUS issues involving CFIUS filings such as appointment of the Department of Defense as a co-lead agency or final outcome of CFIUS deliberations.

d. Serve as the primary DoD point of contact with the Joint Chiefs of Staff for CFIUS matters.

e. Determine, after consultation with DoD Components, which DoD Components will perform specific functions during review of CFIUS transactions on a case-by-case basis. Determine which reviewers should augment a CFIUS review to ensure a robust and thorough review.

f. Identify specific issues that relevant DoD Components should review in CFIUS filings to ensure a robust and thorough review.

g. Chair the CFIUS Monitoring Committee.

h. Determine, in cooperation with DoD Components, any proposals for enhancing the effectiveness of the CFIUS review process.

i. Ensure that adequate staff and budget resources are available to monitor and ensure that foreign entities or their U.S. subsidiaries are complying with mitigation agreements concluded with the Department of Defense.

3. DUSD(PI&CoS). The DUSD(PI&CoS), under the authority, direction, and control of the Principal Deputy Under Secretary of Defense for Policy, shall:

- a. Serve as the DoD representative to the CFIUS.
- b. Provide the USD(P) weekly status of pending CFIUS acquisitions.
- c. Provide senior leadership summaries of all CFIUS acquisitions that affect national security interests.
- d. Recommend to USD(P) and/or Deputy Secretary of Defense which CFIUS acquisitions should be approved or subjected to an additional 45-day period of investigation.
- e. Forward any CFIUS filings or actions to the Deputy Secretary of Defense for action when appropriate.

(1) CFIUS filings forwarded to the Deputy Secretary of Defense will include, but are not limited to, acquisitions involving foreign-government-controlled transactions and critical infrastructure transactions, for which the Department of Defense has been designated a co-lead agency.

(2) CFIUS actions forwarded to the Deputy Secretary of Defense will also include, but are not limited to, approvals of requests for second-stage investigations, approvals of filings involving mitigation agreements, and approvals of CFIUS reports to the President of the United States when the Department of Defense is a co-lead agency.

4. DEPUTY UNDER SECRETARY OF DEFENSE FOR STRATEGY, PLANS, AND FORCE DEVELOPMENT. The Deputy Under Secretary of Defense for Strategy, Plans, and Force Development, under the authority, direction, and control of the USD(P), shall review CFIUS filings for sensitive policy issues and prepare assessments, as necessary, regarding force development for conventional capabilities that may impact or be impacted by a CFIUS transaction.

5. ASSISTANT SECRETARY OF DEFENSE FOR INTERNATIONAL SECURITY AFFAIRS. The Assistant Secretary of Defense for International Security Affairs, under the authority, direction, and control of the USD(P), shall review CFIUS filings for sensitive policy issues and prepare assessments, as necessary, regarding regional or bilateral issues that may impact or be impacted by a CFIUS transaction.

6. ASSISTANT SECRETARY OF DEFENSE FOR ASIAN AND PACIFIC SECURITY AFFAIRS (ASD(A&PSA)). The ASD(A&PSA), under the authority, direction, and control of the USD(P), shall review CFIUS filings for sensitive policy issues and prepare assessments, as

necessary, regarding regional or bi-lateral issues that may impact or be impacted by a CFIUS transaction.

7. ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND AMERICAS' SECURITY AFFAIRS (ASD(HD&ASA)). The ASD(HD&ASA), under the authority, direction, and control of the USD(P), shall:

- a. Evaluate CFIUS filings for their potential impact on the U.S. defense critical infrastructure in accordance with DoDD 3020.40 (Reference (f)).
- b. Coordinate with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) regarding the need for any further industrial capability assessments.
- c. Coordinate with the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) on transactions that impact critical telecommunications infrastructure.

8. DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR WESTERN HEMISPHERE AFFAIRS. The Deputy Assistant Secretary of Defense for Western Hemisphere Affairs, under the authority, direction, and control of the ASD(HD&ASA), shall review CFIUS filings for sensitive policy issues and prepare assessments, as necessary, regarding regional or bi-lateral issues that may impact or be impacted by a CFIUS transaction.

9. ASSISTANT SECRETARY OF DEFENSE FOR GLOBAL STRATEGIC AFFAIRS (ASD(GSA)). The ASD(GSA), under the authority, direction, and control of the USD(P), shall review CFIUS filings for sensitive policy issues and prepare assessments, as necessary, regarding space and cyber security issues that may impact or be impacted by a CFIUS transaction.

10. USD(AT&L). The USD(AT&L) shall:

- a. Identify any effect on national security of a proposed CFIUS foreign acquisition of a U.S. defense, or potential defense supplier, in areas for which the USD(AT&L) has responsibility, including the defense-related industrial base; research and development; defense cooperation relationships with foreign partners; defense procurement and logistics; and small business programs, specifically addressing whether the firm being acquired possesses critical defense technology under development or is otherwise important to the defense industrial and technological bases.
- b. Assess whether the U.S. firm possesses any critical technologies, as defined in the Glossary of this Instruction.

c. Assess the likelihood and national security impact of any supply disruption based on availability of alternative sources and the strategic objectives and economic viability of the acquiring firm.

d. Ensure adequate resources, in terms of staff and budget, are available for statutorily required monitoring and ensuring yearly compliance by foreign entities or their U.S. subsidiaries party to mitigation agreements with the Department of Defense for which USD(AT&L) is primarily responsible.

11. DIRECTOR, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY. The Director, Defense Advanced Research Projects Agency, under the authority, direction, and control of the USD(AT&L), through the Director, Defense Research and Evaluation, shall, in addition to the responsibilities in section 22 of this enclosure, evaluate CFIUS transactions for their effect on defense research programs and their potential effect on future defense capabilities.

12. DIRECTOR, SPECIAL PROGRAMS. The Director, Special Programs, under the authority, direction, and control of the USD(AT&L), shall identify DoD-wide Special Program interests; evaluate the CFIUS transactions for their affect on these programs as well as their potential affect on existing or future defense capabilities; and develop a coordinated position on each of these filings with respect to these issues.

13. DIRECTOR, DEFENSE LOGISTICS AGENCY. The Director, Defense Logistics Agency, under the authority, direction, and control of the USD(AT&L), through the Assistant Secretary of Defense for Logistics and Material Readiness, shall, in addition to the responsibilities in section 22 of this enclosure, assess the effect of CFIUS transactions on defense procurement and planning related to supply support and technical and logistic services to the Military Departments.

14. DIRECTOR, MISSILE DEFENSE AGENCY. The Director, Missile Defense Agency, under the authority, direction, and control of the USD(AT&L), shall, in addition to the responsibilities in section 22 of this enclosure, evaluate CFIUS transactions to determine their impact on missile defense activities and potential implications on future missile defense-related technologies.

15. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I) shall:

a. Evaluate CFIUS transactions for their impact on intelligence and security activities; assess whether the policies in DoD 5220.22-R (Reference (g)) are adequate to mitigate potential national security concerns of foreign ownership of cleared defense contractors; and so inform DoD CFIUS participants.

b. Ensure adequate resources, in terms of staff and budget, are available for statutorily required monitoring and ensuring yearly compliance by foreign entities or their U.S. subsidiaries party to mitigation agreements with the Department of Defense for which USD(I) is primarily responsible.

c. Forward all relevant information received from the Director of the Defense Security Service regarding the impact of proposed transactions on companies cleared under the National Industrial Security Program, including any recommended measures to mitigate foreign ownership, control, or influence.

d. Ensure the Defense Intelligence Components support the ODNI in accordance with the requirements of Reference (b), including the National Security Threat Assessment process, as required.

16. DIRECTOR, NATIONAL SECURITY AGENCY (NSA). The Director, NSA, under the relevant authority, direction, and control of the USD(I) and ASD(NII)/DoD CIO, as delegated by the Secretary of Defense, and consistent with ODNI authority, shall, in addition to the responsibilities in section 22 of this enclosure:

a. Evaluate CFIUS transactions to determine their impact on NSA's Signals Intelligence and Information Assurance missions and their potential effect on future NSA capabilities.

b. Provide signals intelligence and information assurance technical support to ASD(NII)/DoD CIO, USD(I), and other U.S. Government officials, as appropriate, to support review of CFIUS filings and monitoring of compliance with mitigation agreements in those circumstances where the Director, NSA, has relevant information or technical expertise.

c. Ensure that adequate resources, in terms of staff and budget, are available for statutorily required monitoring and ensuring yearly compliance by foreign entities or their U.S. subsidiaries party to mitigation agreements with the Department of Defense and for which the Director, NSA, is primarily responsible.

17. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). The Director, DIA, under the authority, direction, and control of the USD(I), shall, in addition to the responsibilities in section 22 of this enclosure, prepare assessments that analyze the technology transfer and diversion risks of CFIUS transactions.

18. DIRECTOR, NATIONAL RECONNAISSANCE OFFICE (NRO). The Director, NRO, under the authority, direction, and control of the USD(I), shall, in addition to the responsibilities in section 22 of this enclosure, evaluate CFIUS transactions to determine their impact and implications on overhead reconnaissance systems.

19. ASD(NII)/DoD CIO. The ASD(NII)/DoD CIO shall:

a. Evaluate CFIUS transactions to identify national security risks that may impact the mission of enabling net-centric operations, including risk to information and communications technology market, the global telecommunications infrastructure, National Security Systems, , command and control communications, non-intelligence space matters, information resources management, spectrum management, network operations, information systems, information assurance, positioning navigation and timing policy including airspace and military traffic control activities, sensitive information integration, contingency support, migration planning, and related matters.

b. Ensure adequate resources, in terms of staff and budget, are available for statutorily required monitoring and ensuring yearly compliance by foreign entities or their U.S. subsidiaries party to mitigation agreements with the Department of Defense for which ASD(NII)/DoD CIO is primarily responsible.

20. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). The Director, DISA, under the authority, direction, and control of the ASD(NII)/DoD CIO, shall, in addition to the responsibilities in section 22 of this enclosure:

a. Provide advice and technical recommendations to ASD(NII)/DoD CIO and other DoD Components as appropriate to support CFIUS transaction reviews.

b. Ensure adequate resources, in terms of staff and budget, are available for statutorily required monitoring and ensuring yearly compliance by foreign entities or their U.S. subsidiaries party to mitigation agreements with the Department of Defense for which the Director, DISA, is primarily responsible.

21. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE. The General Counsel of the Department of Defense shall:

a. Provide legal advice and assistance for reviews under this Instruction, including reviews of letters of certification and memorandums of determination.

b. Negotiate and draft proposed mitigation agreements, assurance letters, and other documents that lessen the risks in CFIUS transactions on behalf of the Department of Defense. Serve as the primary point of contact with legal counsel representing entities that are involved in CFIUS filings and engaged in negotiating and drafting proposed mitigation measures, assurance letters, and other legal documents required for DoD review of CFIUS filings.

c. As needed, provide the DoD position on both the adequacy of current statutes protecting national security and any proposed CFIUS legislation.

22. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Become familiar with the statutory review and investigation timelines of CFIUS transaction reviews. All CFIUS transaction reviews are time-sensitive and not releasable to the public; release to Congress is statutorily controlled. Should any third party request information about a current CFIUS case under review, provide the third party with a “no comment” and notify DTSA immediately.

b. Notify DTSA immediately upon discovery of potential national security concerns.

c. Develop clear, well-documented positions as requested in Enclosure 4 of this Instruction, which include identification of possible mitigation measures required to offset risks for those transactions for which the DoD Component has identified threats (including consequences if threat is realized) and vulnerabilities relating to national security for use in any subsequent mitigation agreement.

d. When recommending a second-stage investigation, provide DTSA as the DoD lead Component for CFIUS:

(1) A written recommendation for investigation signed by the DoD Components’ senior level official or director or a direct report deputy to one of these officials that includes the rationale and objective for requesting a second-stage investigation, in accordance with Enclosure 4 of this Instruction.

(2) Detailed analysis supporting mitigation measures or block recommendations in a Risk-Based Analysis (RBA) in accordance with situations described in paragraph 3.b. of Enclosure 4 of this Instruction.

(3) At an appropriate time during a subsequent second-stage investigation, any necessary assurance letters, draft term sheets or mitigation agreements, drafted and negotiated in conjunction with the Office of the General Counsel of the Department of Defense (OGC, DoD), DTSA, and other CFIUS members when appropriate.

(4) Support in drafting decision memorandums for OSD leadership.

(5) Briefings to DoD senior leadership as required.

(6) Formal briefings to CFIUS, as requested by DTSA or the CFIUS Chair in cooperation with DTSA, and attendance at DoD and CFIUS policy meetings in relevant filings.

e. Assist DTSA in developing DoD input for reports to the President of the United States.

f. Assist DTSA in long-term monitoring of mitigation agreements as noted in Enclosure 6 of this Instruction.

g. Ensure that adequate resources, in terms of staff and budget, are available for statutorily required monitoring and ensuring annual compliance by foreign entities or their U.S. subsidiaries that are party to mitigation agreements with the Department of Defense and for which a given DoD Component was primarily responsible due to its request for investigation.

h. Participate in all functions of the DoD CFIUS Monitoring Committee chaired by DTSA and described in Enclosure 6 of this Instruction.

i. Identify the specific DoD Component(s) office(s) to DTSA that will have responsibility for monitoring CFIUS mitigation agreements or parts thereof.

j. Provide DTSA with compliance statements with regard to any monitoring responsibilities the DoD Component(s) or office(s) may have at intervals determined by DTSA and the DoD CFIUS Monitoring Committee chaired by DTSA and described in Enclosure 6 of this Instruction.

23. SECRETARIES OF THE MILITARY DEPARTMENTS. The Secretaries of the Military Departments, in addition to the responsibilities in section 22 of this enclosure, shall:

a. Identify and assess the national security implications relevant to their respective Services arising from the transfer of technology and/or production capacity when an acquired firm is a current or former defense contractor or possesses critical technologies.

b. Determine the impact on the warfighter's capabilities and technological advantages should the products, services, or technologies involved in a given transaction be transferred to the foreign acquirer.

c. Ensure adequate resources, in terms of staff and budget, are available for statutorily required monitoring and ensuring yearly compliance by foreign entities or their U.S. subsidiaries party to mitigation agreements with the Department of Defense and for which the Military Department is primarily responsible.

24. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Chairman of the Joint Chiefs of Staff, in addition to the responsibilities in section 22 of this enclosure, shall:

a. Review and identify CFIUS filings that are likely to impact an area of Joint Staff interest or concern.

b. On a case-by-case basis, seek input from relevant Combatant Commands, Military Services, or any other DoD agency or organization not already so tasked by DTSA.

c. Forward the CFIUS case to the Commander, United States Transportation Command, for analysis and input in filings involving acquisition of portions of the U.S. military transportation network, to include air, land, or sea assets or services.

d. Forward the CFIUS case to the Commander, United States Strategic Command, for analysis and input in filings involving the acquisition of portions of the military integrated intelligence, surveillance, and reconnaissance network; military space and global strike

operations; military information operations; or integrated missile defense and robust command and control.

e. Forward the CFIUS case to the Commander, United States Special Operations Command, for evaluation and input in filings involving special operations peculiar and related technologies, or where business transactions may impact the defense posture or proliferation of advanced capabilities to a foreign nation.

f. Ensure adequate resources, in terms of staff and budget, are available for statutorily required monitoring and ensuring yearly compliance by foreign entities or their U.S. subsidiaries party to mitigation agreements with the Department of Defense and for which the Joint Staff is responsible.

25. COMMANDERS OF THE COMBATANT COMMANDS. The Commanders of the Combatant Commands, in addition to the responsibilities in section 22 of this enclosure, shall review any forwarded CFIUS filings likely to impact an area of interest or concern to the Combatant Command.

ENCLOSURE 3

PROCEDURES

1. DTSA INITIAL REVIEW

a. DTSA Initial CFIUS Filing Review. Following receipt of a CFIUS case from the Department of the Treasury, DTSA will conduct an initial analysis consisting of:

- (1) A preliminary determination of foreign government ownership.
- (2) Identification of the existence of DoD unclassified contracts or supply relationships.
- (3) Identification of classified contracts, facility security clearances, or security agreements by either firm in a CFIUS filing.
- (4) Identification of any DoD issues in a CFIUS filing that would support the CFIUS Chair designating the Department of Defense as a co-lead agency.

b. DTSA Staffing of CFIUS Transactions. Following DTSA initial review of a CFIUS transaction review received by the Department of Treasury, DTSA staff will forward the CFIUS case containing the proposed acquisition transaction to the relevant DoD Component(s) electronically and include:

- (1) A summary of the result of the initial analysis.
- (2) Any questions arising from this analysis to guide specific DoD Component(s) performing a review and that ultimately will assist DTSA in preparing a final DoD position.

2. DoD COMPONENT REVIEW

a. DoD CFIUS Review Process. DoD Components that are forwarded a CFIUS case file from DTSA for review will examine within the initial 21-day review period, at a minimum, any questions arising from DTSA's initial analysis, as well as the factors found in Enclosure 4 of this Instruction, unless other specific criteria are identified by DTSA pursuant to paragraph 2.f. of Enclosure 2.

b. DoD Component Requirements.

(1) DoD Components will provide all pertinent details regarding specific products, services, and technologies for all existing contracts, both unclassified and classified, that they have with the U.S. company being acquired and, to the extent possible, verify the accuracy of such contracts identified by the companies in their CFIUS filings.

(2) If any DoD Component identifies national security risks during its review, that DoD Component should evaluate whether the risks can be mitigated to an acceptable level through use of existing authorities, or whether a mitigation measure using the methodology found in Enclosure 5 of this Instruction may be necessary, including preparation of a RBA.

(3) If any DoD Component identifies national security risks that cannot or may not be mitigated during the initial 30-day review and would lead to a recommendation for a 45-day second-stage investigation, that Component will need to address the factors found in sections 2 and 3 of Enclosure 4 of this Instruction.

c. Internal Suspense Procedures. Concurrent with forwarding the CFIUS case file and DTSA's initial analysis to DoD Components, DTSA will provide to all DoD Components an internal suspense. DTSA will provide reminders to the relevant DoD Components as the internal DoD suspense approaches.

d. Caseload Updates. DTSA will provide status updates on all current and draft CFIUS filings to DoD Components on a regular basis.

e. DTSA Review of DoD Inputs. DTSA will review and evaluate coordination comments from all DoD Components. When national security issues have been identified, DTSA will chair meetings with affected DoD Components to clarify issues and arrive at consensus on the DoD position for the CFIUS filing.

f. Determination of National Security Issue. If DTSA and the affected DoD Component determine that national security risks can be reduced to an acceptable level through any given mitigation measure, they shall determine the appropriate monitoring strategy and identify monitoring responsibilities as found in Enclosure 5 of this Instruction.

g. DTSA Notification to Senior OSD Leadership. DTSA will notify DUSD(PI&CoS) and USD(P) of all CFIUS transactions that have adverse implications for national security and that may result in a recommendation to proceed to a 45-day investigation as soon as such risks and/or threats are identified, regardless of whether the formal review process has been completed.

3. DTSA PROCESSING AND TRANSMITTAL OF DoD CFIUS FILING RECOMMENDATION

a. DTSA Preparation of DoD Recommendation. Following the DoD internal CFIUS review suspense, DTSA will formulate and recommend a DoD position for each CFIUS case through DUSD(PI&CoS) to USD(P) or the Deputy Secretary of Defense as appropriate.

b. DoD Position Formulation. The DTSA-recommended DoD position in each CFIUS case following first- and second-stage investigations will be completed in accordance with clearance procedures stipulated by the CFIUS Chair.

c. Transmittal of DoD Position. The DoD position in each CFIUS case will be forwarded through DUSD(PI&CoS) to USD(P) or the Deputy Secretary of Defense.

4. WITHDRAWN CFIUS FILINGS. Should companies re-file their case with CFIUS following an approved withdrawal, and the re-filing does not add a new element of relevance to the Department of Defense, then DTSA shall:

a. Notify all DoD Component reviewers of the re-filing and provide copies of any pertinent documents including mitigation agreements.

b. Inform DoD component reviewers that DTSA believes that the re-filing does not add a new element of relevance for the Department of Defense.

c. Provide DoD component reviewers at least 1 business day to raise any objection prior to forwarding the previously determined DoD position for OSD leadership final determination.

5. CFIUS INTRAGENCY DISAGREEMENTS REGARDING JURISDICTION. When there is disagreement among CFIUS member agencies with regard to the Department of the Treasury's position on a jurisdictional question, DTSA will, with OGC, DoD, participation, prepare a package for a USD(P) decision and provide CFIUS and DoD Components with the resulting DoD position on jurisdiction. DoD component reviewers will continue formal review of the transaction until DTSA notifies them that CFIUS review of the case is no longer required.

6. DoD NON-NOTIFIED CFIUS REQUESTS

a. DoD Non-notified Request. DoD Component reviewers requesting CFIUS review of non-notified transaction(s) will forward to DTSA:

- (1) The name of the foreign acquirer.
- (2) The nature of the foreign acquirer's business.
- (3) The foreign acquirer's address and phone number.
- (4) The name of the U.S. company being acquired.
- (5) The nature of the U.S. company's business.
- (6) The U.S. company's address and phone number.
- (7) A description of the transaction and its dollar value.
- (8) A description of the national security issues raised by the non-notified transaction.

b. Notification of Non-notified Request. DTSA will staff approval of a request for a non-notified CFIUS filing with DUSD(PI&CoS). Once approved, DTSA will forward the request to

the CFIUS Chair for CFIUS review and a determination that the companies involved in the transaction should file with CFIUS. Once there is a CFIUS decision, DTSA will notify the requesting DoD component reviewer of the outcome.

7. DTSA CFIUS MANAGEMENT SUPPORT

a. DTSA's Support Role. As the DoD representative within the interagency process, DTSA is the primary point of support for specific DoD Component reviewers that may have interests in a given case based on the nature and classification of the transaction. To assist DTSA in representing the Department of Defense in CFIUS meetings, the guidelines in subparagraphs 7.a.(1) through (3) of this enclosure apply.

(1) For CFIUS filings where the CFIUS Chair requires an assessment before the normal 23-day suspense, or involving complex technical issues, the DoD Component with the most technical interest in a CFIUS acquisition will share primary responsibility with DTSA for analyzing, reviewing, and coordinating a DoD position on a "fast-track" basis due to the statutory time constraints inherent in the CFIUS process.

(2) For filings where a DoD Component shares primary responsibility with DTSA under the conditions described in subparagraph 7.a.(1) of this enclosure, other DoD Components with interests in the case, in whole or in part, shall be copied on all communications involving expedited analysis and decision memos, if feasible, before memorandums or briefings are delivered to OSD's leadership.

(3) In all filings with "fast-track" analysis, DTSA retains overall responsibility for processing and communication and will share all relevant information about the case with other co-lead agencies and will maintain timely contact with all other DoD Components.

b. Forwarding of DoD Position. In all CFIUS filings, DTSA will forward the final DoD positions to the CFIUS Chair in the appropriate format.

c. Provision of CFIUS memorandum on behalf of the DoD Executive Secretary. DTSA will obtain on behalf of the DoD Executive Secretary a copy of the CFIUS Chair's signed completion memorandum for archival purposes and distribute a copy to all DoD CFIUS reviewers.

d. DoD Management of CFIUS Mitigation Agreements. DTSA will manage DoD activities related to or arising from its role in monitoring mitigation agreements found in Enclosure 6 of this Instruction.

e. DTSA Management of the DoD CFIUS Monitoring Committee. As Chair of the DoD CFIUS Monitoring Committee, the Director, DTSA, shall:

(1) Develop and maintain a multi-year DoD CFIUS Strategic Mitigation Plan which sets out the DoD strategic policy with regard to DoD CFIUS mitigation and monitoring efforts, taking into account resource management and filing trends.

(2) Ensure that the DoD CFIUS Strategic Mitigation Plan identifies types of risk(s) usually found in different types of CFIUS acquisitions that the Department of Defense normally would seek to mitigate.

(3) Ensure that the DoD CFIUS Strategic Mitigation Plan identifies risk-reducing measures currently used in different types of CFIUS mitigation agreements where DoD Components are signatories.

(4) Ensure that the DoD CFIUS Strategic Mitigation Plan includes types of mitigation measures identified in this Instruction, as well as any others used to lessen risks in acquisitions.

(5) Ensure that the DoD CFIUS Strategic Mitigation Plan includes sample mitigation measures and agreements that can be used to assist DoD Components in reviewing risk mitigation measures and in tailoring mitigation agreements for use in future CFIUS transactions.

(6) Ensure that the DoD CFIUS Strategic Mitigation Plan includes and identifies the methods the Department of Defense uses to substantiate and document company compliance with mitigation agreements, as well as to maintain a record of compliance or noncompliance by companies.

(7) Monitor DoD Component evaluations of company compliance with mitigation agreements by serving as a repository for both DoD Component confirmations of company compliance with CFIUS mitigation agreements as well as any reports of breaches in agreements.

(8) Identify and address monitoring and mitigation issues common to two or more CFIUS mitigation agreements.

f. DoD Mitigation Agreement Compliance Requirements. DTSA will ensure that the DoD CFIUS Monitoring Committee:

(1) Updates, as appropriate, anticipated resource requirements for the DoD CFIUS Strategic Mitigation Plan at least 2 years out. The DoD CFIUS Strategic Mitigation Plan requires an annual analysis of past mitigation agreements monitored by the Department of Defense in order to determine if past DoD approaches to monitoring and mitigation can be improved.

(2) As the focal point for DoD monitoring, provides a forum for developing unified DoD responses to Congressional or Executive Branch CFIUS monitoring initiatives or proposals.

g. DoD CFIUS Monitoring Committee

(1) Committee guidance can be found in Enclosure 6 of this Instruction.

(2) Committee procedures are described in Enclosures 4 and 6 of this Instruction.

ENCLOSURE 4

DoD CFIUS SECURITY ASSESSMENT STRATEGY

1. STATUTORY REQUIREMENTS. Reference (b), as incorporated in Executive Order 11858 (Reference (h)), requires CFIUS to consider several specific national security factors when determining whether to exercise CFIUS authorities. These include:

- a. Domestic production needed for current and projected peacetime, contingency, and wartime national defense requirements.
- b. 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.
- c. 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.
- d. The potential effects of the transaction on the sales of military services, equipment, or technology to a country that supports terrorism or proliferates missile technology or chemical or biological weapons.
- e. The potential effects of the transaction on U.S. technological leadership in areas affecting U.S. national security.
- f. The potential national security-related effects on United States critical infrastructure, including major energy assets.
- g. The potential national security-related effects on United States critical technologies.
- h. Whether the transaction is a foreign government-controlled transaction, namely, whether the acquirer is controlled by, or acting on behalf of, a foreign government.
- i. When appropriate, and particularly with respect to foreign government-controlled transactions requiring further investigations:
 - (1) Adherence of foreign governments to nonproliferation control regimes, including treaties and multilateral supply guidelines.
 - (2) The relationship of a foreign government 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.

j. The long-term projection of the United States requirements for sources of energy and other critical resources and material.

2. FACTORS IN INTERNAL DoD CFIUS REVIEWS. During the first-stage investigation review, DoD Components will assess, at a minimum, the specific factors relevant to DoD national security interests:

a. Whether the U.S. firm produces a critical and/or highly vulnerable critical technology, critical and/or highly vulnerable infrastructure asset, critical law enforcement asset, or unique defense or infrastructure capability.

b. Whether the U.S. firm 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, thereby precluding the acquisition by a foreign entity.

c. Whether the U.S. firm is a single or sole qualified source supplier for DoD contracts, classified or unclassified, and whether it has technology with military applications.

d. Whether the company being acquired is part of DoD critical infrastructure that is essential to project, support, or sustain military forces.

e. Whether this acquisition negatively impacts the DoD Defense Critical Infrastructure Program (DCIP) as established in Reference (f); or whether the acquired company is subject to the provisions of Reference (g).

f. 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 through CFIUS Mitigation Agreements concluded through negotiation with the parties.

g. Whether there are current or upcoming DoD concerns or policies regarding any of the foreign countries and/or governments involved in this transaction including, at a minimum, an assessment by the OSD regional office director whether the country involved in the transaction poses a potential regional threat to U.S. interests.

3. SECOND-STAGE INVESTIGATIONS, MITIGATION MEASURES, AND BLOCKING TRANSACTIONS

a. DoD Component reviewers who recommend a second-stage investigation for a given CFIUS case must address the following items in their written recommendation:

(1) The rationale for requiring a second-stage investigation.

(2) The objective of the investigation.

- (3) The defense criticality or vulnerability associated with the assets of the firm being acquired.
- (4) To the extent known, the national security threat posed by the foreign party acquiring control.
- (5) To the extent known, the consequences to national security if the threat is realized, including the impact on DoD national security interests.
- (6) Remaining unanswered issues or questions relevant to determining whether foreign control will threaten to impair the national security.
- (7) The information needed to resolve unanswered issues or questions.
- (8) The extent to which, if any, there is credible evidence that the foreign interest that will exercise control might take action that threatens to impair the national security.
- (9) A discussion of the other provisions of law that have been considered in determining whether they provide adequate and appropriate authority to protect the national security.

b. When a DoD Component reviewer determines that mitigation measures under CFIUS authorities are required or that a given transaction should be blocked, then that Component must submit to DTSA, over the signature of their organization's senior official or director or a direct report deputy to one of these officials, an RBA. The RBA needs to justify pursuit of mitigation measures or a recommendation that the President of the United States block the transaction. See Enclosure 5 of this Instruction for additional guidance. RBAs must at a minimum:

- (1) Identify all national security risks posed by the transaction based on the threat, vulnerabilities, and potential adverse consequences if the risks are not mitigated.
- (2) Include how the National Intelligence Council (NIC) assessment for the given case impacts the threat analysis.
- (3) If applicable, include the types of risk mitigation measures believed to be reasonable and necessary to address the risks posed by the transaction.

ENCLOSURE 5

DoD CFIUS RISK AND MITIGATION METHODOLOGY

1. RISK METHODOLOGY

a. Risk Mitigation Methodology and Determining Risk. Risk(s) arising in CFIUS filings are inherently case-specific, as are the mitigation measures used to address those risks posed by a given CFIUS acquisition.

b. Assessing Risks in CFIUS Filings. Although risks in CFIUS filings are case-specific, the stages of the risk mitigation methodology are the same for, and are assessed in, each case. This methodology has four stages:

(1) Determine Preliminary Risk. Assess the criticality and/or vulnerability of the assets being acquired and compare them to the threat posed by the acquiring company and country, including consequences to national security if the threat is realized.

(2) Develop Mitigation Measures. Develop feasible measures to adequately mitigate or eliminate the preliminary risk or explain why no measures are capable of addressing the risk.

(3) Determine Overall Risk. Compare the risk that would remain after application of mitigation measures for the preliminary risk and include potential circumvention of the contemplated measures. The overall risk is that which remains after analyzing the impact of such circumvention, whether such circumvention is detectable or not, and whether the mitigation measures can be effectively monitored by the U.S. Government given available resources.

(4) Conclusion. State a conclusion about the way forward given the overall risk.

c. Classification Requirement. Information contained in a RBA should be classified no higher than SECRET//NOFORN. If the need arises to include information above this collateral level, this will be done as a special annex on a case-by-case basis in direct consultation with DTSA, or by other arrangements in the case of Special Programs.

2. DESCRIPTION OF RBA. An RBA of a CFIUS case is composed of three elements: vulnerability and/or criticality of the U.S. assets being acquired; the threat to those assets posed by the acquiring company or country; and the potential adverse consequences to national security if the threat is realized.

3. TYPES OF MITIGATION

a. Types of Mitigation. Generally, risks associated with a CFIUS case are lessened through mitigation measures in three categories:

(1) Technical Mitigation Measures. These mitigation measures address risks arising from vulnerabilities or critical assets with sensitive source codes, cutting-edge technological development, and communication infrastructure.

(2) Personnel Mitigation Measures. These mitigation measures address risks arising from foreign personnel having potential access to sensitive technology or other critical assets.

(3) Management Control Mitigation Measures. These mitigation measures oversee the successor company's ongoing implementation of mitigation agreements related to technical or personnel mitigation measures.

b. DoD Strategic Mitigation Plan. The DoD Strategic Mitigation Plan will address the DoD strategy for identifying, mitigating, and monitoring risks inherent in specific types of acquisitions and in specific mitigation agreements.

ENCLOSURE 6

DoD CFIUS MONITORING STRATEGY AND RESPONSIBILITY AND ROLE OF DoD
CFIUS MONITORING COMMITTEE

1. CFIUS MITIGATION AGREEMENT MONITORING STRATEGY

a. To protect national security, the Department of Defense will actively monitor any completed CFIUS case where the Department of Defense was a signatory to a mitigation or security agreement (or any other agreement) that enables a CFIUS acquisition.

b. The DoD Component that sponsored a mitigation or security agreement during the review of an acquisition, or portions thereof, leading to CFIUS approval of the foreign acquisition shall:

(1) Identify to DTSA the office and person responsible for oversight of the mitigation, security, or other agreement, or portions thereof, no later than 5 days following signature of the mitigation or security agreement.

(2) Notify DTSA when the office or person responsible for oversight of the mitigation, security, or other agreement, or portions thereof, changes.

(3) Identify to DTSA the office and person who will serve as its representative to the CFIUS Monitoring Committee.

c. Effective determination of compliance with mitigation and security agreements in certain CFIUS filings will involve support of many DoD Components. In these filings, all DoD Components will identify, during the CFIUS case review and the mitigation and security agreement process, which portion of the agreement(s) they will be responsible for monitoring.

d. DTSA will, on a yearly basis, forward the compliance verifications received from the DoD Components, along with its own mitigation compliance verifications for agreements for which it has primary responsibility, through DUSD(PI&CoS) to USD(P).

e. All compliance verifications will be kept on file for no fewer than 10 years after the expiration, if any, of mitigation, security, or other agreement leading to CFIUS approval of the foreign acquisition, whichever is later.

2. DoD CFIUS MONITORING COMMITTEE

a. The DoD CFIUS Monitoring Committee is hereby established.

b.. The Director, DTSA, will chair the DoD CFIUS Monitoring Committee, consisting of one representative from each DoD Component that sponsored a mitigation or security agreement

of a CFIUS case; the OGC, DoD; and the Offices of USD(AT&L), USD(I), and ASD(NII)/DoD CIO.

c. The CFIUS Monitoring Committee will meet no less than quarterly, but more often if required. The CFIUS Monitoring Committee shall:

(1) Serve as a repository for both DoD Component certifications of company compliance with CFIUS mitigation agreements and reports of their breach.

(2) Identify any monitoring or mitigation issues common to two or more CFIUS mitigation agreements which the DoD is responsible for monitoring.

(3) Determine if any mitigation or monitoring issues common to two or more CFIUS mitigation agreements are resolvable through unified DoD action such as substantive correction or amendment to mitigation agreements, or a procedural change to how they are drafted and negotiated.

(4) Annually determine if past DoD approaches to monitoring and mitigation can be improved, either substantively or procedurally, through analysis of past mitigation agreements monitored by the Department of Defense.

(5) Collate and forward to the Department of the Treasury the DoD CFIUS mitigation and monitoring inputs for all statutorily required Congressional reports.

(6) Provide a forum for developing a unified DoD response to Congressional or Executive branch CFIUS monitoring initiatives or proposals by being the focal point for DoD monitoring.

(7) If required for implementation, forward to PDUSDP, through the Chair, any CFIUS Monitoring Committee initiatives or proposals.

ENCLOSURE 7

DoD CFIUS REVIEW PROCEDURE DIAGRAM

Figure. DoD CFIUS Review Process

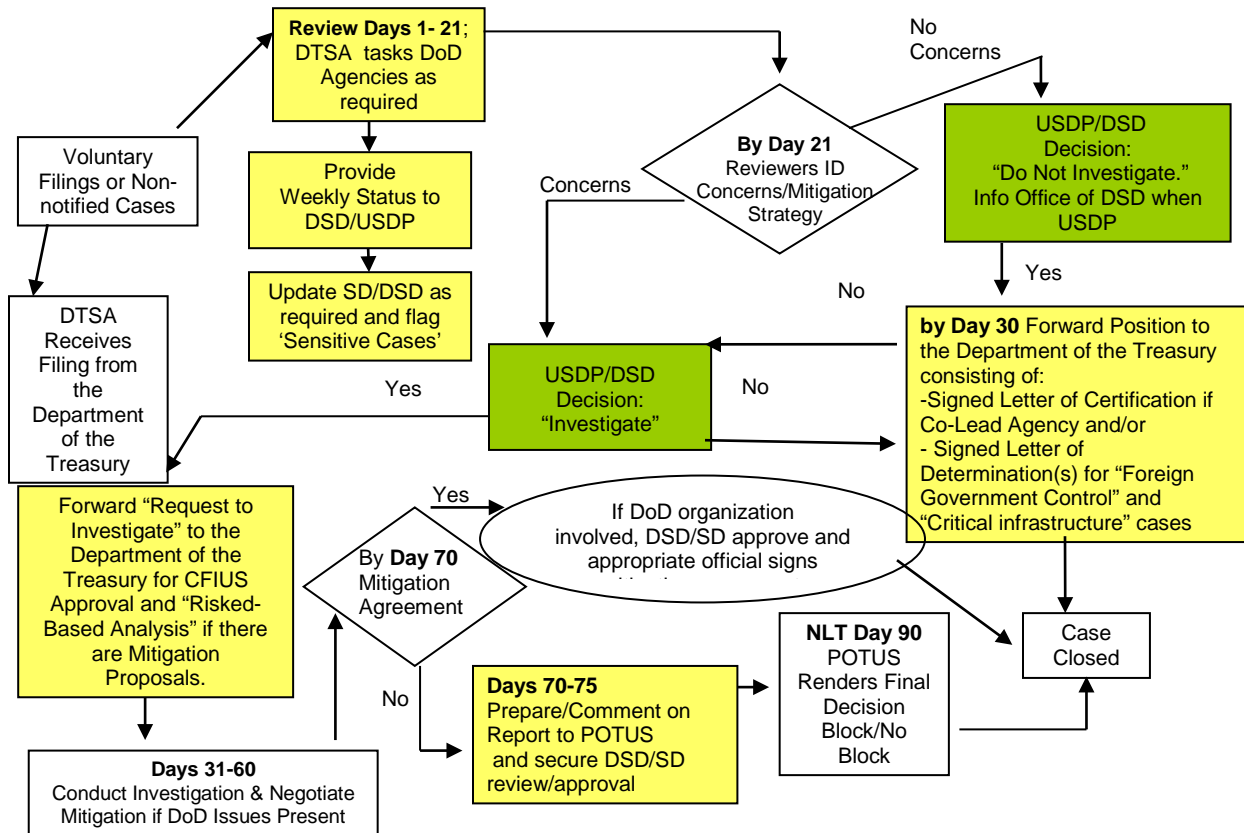


Table. DoD CFIUS Reviewers

Under Secretary of Defense for Policy
Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense for Intelligence
Chairman of the Joint Chiefs of Staff
Assistant Secretary of Defense for International Security Affairs
Deputy Under Secretary of Defense for Policy Integration and Chief of Staff
Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
Assistant Secretary of Defense for Homeland Defense & Americas' Security Affairs
Assistant Secretary of Defense for Global Strategic Affairs
Deputy Under Secretary of Defense for Strategy, Plans, and Force Development
Assistant Secretary of Defense for Asian and Pacific Security Affairs
General Counsel of the Department of Defense
Director, National Security Agency/Chief, Central Security Service
Director, Defense Advanced Research Projects Agency
Director, Defense Intelligence Agency
Director, Defense Logistics Agency
Director, Missile Defense Agency
Director, Defense Technology Security Administration
Director, National Reconnaissance Office
Deputy Assistant Secretary of the Air Force/Science, Technology, and Engineering
Assistant Secretary of the Army/Acquisition, Logistics and Technology
Deputy Assistant Secretary of the Navy/International Programs

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(HD&ASA)	Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks, Information and Integration/Department of Defense Chief Information Officer
CFIUS	Committee on Foreign Investment in the United States
DoDD	DoD Directive
DISA	Defense Information Systems Agency
DIA	Defense Intelligence Agency
DNI	Director National Intelligence
DTSA	Defense Technology Security Administration
DUSD(PI& CoS)	Deputy Under Secretary of Defense for Policy Integration and Chief of Staff
EAR	Export Administration Regulations
ITAR	International Traffic in Arms Regulations
NIC	National Intelligence Council
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OGC, DoD	Office of the General Counsel of the Department of Defense
RBA	Risk-Based Analysis
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
USD(P)	Under Secretary of Defense for Policy
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

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

acquisition. A merger, or takeover of persons engaged in interstate commerce in the United States by or with foreign persons by any means, including purchase, conversion, or acquisition of voting securities or voting proxy rights resulting in acquisition of control; or acquisition of business technology, research, and development facilities, or personnel of the person engaged in interstate commerce if there will likely be substantial use of these items by the acquiring firm.

CFIUS. An inter-agency committee chaired by the Secretary of the Department of the Treasury that serves the President in reviewing the national security implications of foreign investment in the economy. It was first established by Reference (h) and substantively empowered by statute in Reference (b). In accordance with statutory implementing regulations found in part 800 of title 31, Code of Federal Regulations (CFR) (Reference (i)), CFIUS reviews individual acquisitions to determine if they threaten to impair U.S. national security interests.

consequences. The impact on national security if the threat is realized. The identification of a threat includes an estimate of its probable occurrence and an assessment of the results or impact on U.S. national security interests should the threat actually be realized.

covered transaction. An acquisition that CFIUS is legally entitled to review for their national security implications.

critical infrastructure. Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of the particular systems or assets over which foreign control is acquired would have an adverse impact on national security.

critical technologies

With respect to defense articles (defined in part 120.6 of title 22, CFR, also known as “The International Traffic in Arms Regulations” (ITAR) (Reference (j)), or defense services (defined in part 120.9 of Reference (j)), those technologies specified in the part 121.1 of Reference (j) (also known as “The United States Munitions List”);

With respect to dual-use categories of systems, equipment, and components; test, inspection, and production equipment; materials; software; and technology, those technologies specified in part 774 of title 15, CFR, also known as “The Commerce Control List in the Export Administration Regulations” (EAR) (Reference (k));

With respect to nuclear equipment, materials, and technology, those technologies specified in part 110 of title 10, CFR, “Export and Import of Nuclear Equipment and Material,” (Reference (l));

With respect to select agents and toxins, those technologies specified in part 331 of title 7, CFR (Reference (m)), part 121 of title 9, CFR (Reference (n)), and part 73 of title 42, CFR, “Export and Import of Select Agents and Toxins,” (Reference (o)); and any other technologies affecting the critical infrastructure; and

With respect to emerging critical defense technology still under development, research, engineering development, or engineering and technology integration that putatively when complete will produce a defense article or defense service, including its underlying technology and software, which would be covered by the ITAR, or a dual-use article, including its underlying technology and software, which would be covered by the EAR in explicit terms, i.e., other than via EAR99.

criticality. Whether an asset is essential to a current military or defense system or process (e.g., a weapons platform or defense infrastructure component) or a future defense or military system such as critical defense technology under development.

compliance verification. The process by which the Department of Defense comports with the statutory requirement of Reference (b) that CFIUS evaluate compliance with mitigation agreements.

DoD CFIUS Monitoring Committee. The DoD committee that oversees DoD agency certifications of company compliance with mitigation agreements; identifies and resolves monitoring or mitigation agreement issues; determines required improvements in the DoD approach to monitoring and mitigation in the CFIUS process; and develops a unified DoD response to Congressional or Executive Branch CFIUS monitoring initiatives or proposals.

DoD national security interests. Those factors that enable the Department of Defense to fulfill its mission of protecting and defending the United States.

foreign-government-controlled transaction. Any covered transaction that could result in the control of any person engaged in interstate commerce in the United States by a foreign government or entity controlled by or acting on behalf of a foreign government.

lead agency. The agency or agencies designated by the Department of the Treasury as the agency or agencies to act on behalf of the CFIUS for a review of a transaction.

mitigation. Measures that lessen or eliminate risks to DoD national security interests arising from CFIUS transactions. Mitigation measures include, but are not limited to, measures that would involve the negotiation of agreements with the parties to the 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 any risk to U.S. national security that arises as a result of the covered transaction not resolved under existing statutory authorities such as Reference (g).

monitoring. The process by which the responsible U.S. Government parties to a mitigation agreement determine that company signatories are adhering to the agreement.

non-notified transactions. Acquisitions that have not been submitted for CFIUS review.

preliminary risk. The preliminary risk of the transaction is determined by comparing the criticality and/or vulnerability of the assets being acquired to the potential threat and potential consequences. Note that the appropriate preliminary risk from the perspective of the CFIUS process must be described in terms of the incremental risk posed by the transaction. If the only risk that exists after the transaction is the same risk that existed before the transaction, then that risk is not considered an appropriate rationale for CFIUS-based mitigation.

risk. The risk posed by a CFIUS transaction to the DoD ability to fulfill its responsibilities in protecting and defending U.S. national security is composed of three elements: criticality and/or

vulnerability of the U.S. assets being acquired, the threat to those assets posed by the acquiring company and/or country, and the consequences to national security if the threat is realized.

RBA. A mandatory written statement submitted by a component or agency requesting CFIUS mitigation, which is a prerequisite to DoD requesting authority for such measures from the CFIUS interagency members.

security agreements. Subsets of mitigation agreements that provide for monitoring mitigation of security and technology control requirements through a variety of methods. Mitigation agreements negotiated under the National Industrial Security Program as described in Reference (g) are not included in this definition.

threat. The extent to which the acquiring company or country has demonstrated the capability and intent to compromise U.S. national security in the area of the asset being acquired or in general. Threats can range widely including, for example, targeting of U.S. critical technology for unauthorized transfer, efforts to attack and exploit defense-related information systems, and attempts to tamper with defense electronic system components or software. The major sources of threat data are the security threat assessment of the NIC and the risk assessment of DIA.

vulnerability. The probability that an asset can be stolen, destroyed, controlled, misdirected, or countered through attack or exploitation because of the difficulty of protecting it. In the case of a production capability, the greater the DoD reliance on the firm being acquired, then the greater is the vulnerability of the production assets.