United States Government Accountability Office

Report to the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, House of Representatives

July 2018

COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES

Action Needed to Address Evolving National Security Concerns Facing the Department of Defense

GAO-18-494

July 2018

COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES

Action Needed to Address Evolving National Security Concerns Facing the Department of Defense

GAO Highlights

Highlights of GAO-18-494, a report to the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, House of Representatives

Why GAO Did This Study

Foreign acquisitions of U.S. companies can pose challenges for the U.S. government as it balances the economic benefits of foreign direct investment with the need to protect national security. CFIUS is an interagency group, led by Treasury, that reviews certain transactions—foreign acquisitions or mergers of U.S. businesses—to determine their effect on U.S. national security and whether the transaction may proceed.

GAO was asked to review DOD's ability, as a member of CFIUS, to address defense issues. This report assesses factors, if any, that affect DOD's ability to identify and address national security concerns through the CFIUS process, among other objectives. GAO analyzed data on DOD co-led transactions from January 2012 through December 2017, the most recent data available. GAO also interviewed DOD and Treasury officials and reviewed documentation to identify DOD's CFIUS processes, resources, and responsibilities and selected a non-generalizable sample of nine DOD component reviewers, based on their participation in the CFIUS process.

What GAO Recommends

GAO is making eight recommendations, including that DOD assess resources needed to address workload, assess risks from foreign investment in emerging technologies and in close proximity to critical military locations, and update its policies and processes to better reflect the evolving national security concerns facing the department. DOD and Treasury agreed with GAO's recommendations, and have identified some actions to address them.

View GAO-18-494. For more information, contact Marie A. Mak (202) 512-4841 or makm@gao.gov

What GAO Found

The Department of Defense (DOD) faces challenges identifying and addressing evolving national security concerns posed by some foreign investments in the United States.

- **Resources:** DOD's Office of Manufacturing and Industrial Base Policy represents the department and coordinates DOD's participation on the Committee on Foreign Investment in the United States (CFIUS). As a committee member, DOD co-leads CFIUS's review and investigation of transactions between foreign acquirers and U.S. businesses where it has expertise. DOD co-led 99 transactions in calendar year 2017, or 57 percent more transactions than it co-led in 2012, while the annual authorized positions increased from 12 to 17 during that same time period. DOD's workload has also been affected by the volume and complexity of the transactions it is responsible for co-leading, in addition to other CFIUS responsibilities, such as identifying transactions that foreign acquirers do not voluntarily file with CFIUS. DOD has taken some steps to address its resource limitations, but has not fully assessed the department-wide resources needed to address its growing workload.
- **Emerging Technology and Proximity:** DOD officials identified some investments that pose national security concerns from foreign acquirers gaining access to emerging technologies or being in close proximity to critical military locations, which, according to officials, cannot always be addressed through CFIUS because the investments would not result in foreign control of a U.S. business. DOD and Department of the Treasury (Treasury) officials said addressing these investments may require legislative action. DOD is taking steps to identify critical emerging technologies and military locations that should be protected from foreign investment. However, DOD has not fully assessed risks from these types of foreign investment or what additional authorities, if any, may be necessary for it to address them.
- **Policy:** DOD's CFIUS Instruction does not clearly identify some reviewer responsibilities or processes for identifying transactions that foreign acquirers do not voluntarily file with CFIUS. The policy is also outdated and inconsistent with current practices.

DOD's CFIUS Instruction and federal internal control standards emphasize the importance of assessing organizational structures, policies, and procedures to respond to risks. Without assessing resources needed to address its CFIUS workload and risks from foreign investment in emerging technologies or in proximity to critical military locations, and ensuring its policies and processes clearly reflect the issues facing the department, DOD is at risk of being unable to respond to evolving national security concerns.

This is a public version of a sensitive report that GAO issued in April 2018. Information that DOD and Treasury deemed sensitive has been omitted.

Contents

Figures

Abbreviations

CFIUS	Committee on Foreign Investment in the United States
DOD	Department of Defense
MIBP	Office of Manufacturing and Industrial Base Policy
OUSD AT&L	Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
Treasury	Department of the Treasury

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

July 10, 2018

The Honorable Elise Stefanik
Chairwoman
The Honorable Jim Langevin
Ranking Member
Subcommittee on Emerging Threats and Capabilities
Committee on Armed Services
House of Representatives

Foreign acquisitions of U.S. companies can pose challenges for the U.S. government as it balances the economic benefits of foreign direct investment in the United States against the potential that an acquisition may harm national security. The Committee on Foreign Investment in the United States (CFIUS) is responsible for reviewing covered transactions—mergers, acquisitions, or takeovers that could result in foreign control of a U.S. business—and for determining the effect of such transactions on U.S. national security.[1] Following its review of a covered transaction, the committee may draft mitigation agreement measures to address any threats to national security posed by the transaction. If CFIUS concludes national security concerns cannot be mitigated, the committee may elevate the transaction to the President to determine if the transaction should be prohibited or suspended. The committee is chaired by the Secretary of the Treasury and has eight other voting member agencies, including the Department of Defense (DOD).[2] CFIUS's authority was last updated in 2007 with the passage of the Foreign Investment and National Security Act of 2007, which currently guides the CFIUS process.[3] Among other changes, this legislation formalized agency responsibilities and added additional factors agencies should

[1]The term "covered transaction" means any merger, acquisition, or takeover that is proposed or pending after August 23, 1988, by or with any foreign person that could result in foreign control of any person engaged in interstate commerce in the United States. 50 U.S.C. § 4565(a)(3). See also 31 C.F.R § 800.301.

[2]CFIUS is an interagency group that was created in 1975, and today operates pursuant to 50 U.S.C. § 4565 as implemented by Executive Order 11858, as amended, and regulations at 31 C.F.R. Part 800.

[3]FINSA is the most recent amendment to section 721 of the Defense Production Act of 1950. Pub. L. No. 110-49, 121 Stat. 246 (2007) (amending section 721 of the Defense Production Act of 1950, codified as amended at 50 U.S.C. § 4565).

consider as part of their review. In 2017, bills were introduced in Congress proposing revisions to CFIUS.[4]

The U. S. economy has historically been the world's largest recipient of foreign direct investment, receiving $373.4 billion in 2016, according to the Bureau of Economic Analysis. The Bureau also reported that from 2012 to 2016, Chinese foreign direct investment in the United States has almost tripled from $3.6 billion to $10.3 billion.[5] In response to these recent trends in foreign investment, including increasing Chinese investment in U.S. technology companies, members of Congress have raised questions about the effectiveness of the CFIUS process in protecting national security, particularly in protecting DOD's industrial base and critical technologies from foreign control. In addition, the National Defense Authorization Act for Fiscal Year 2018 required the development of a plan and recommendations to improve the effectiveness of the interagency vetting of foreign investments that could potentially impair the national security of the United States.[6] Ensuring the effective protection of technologies critical to U.S. national security interests has been on GAO's High-Risk List since 2007. Our body of work in this area has identified progress in improving the effectiveness of the programs designed to protect technologies critical to U.S. national security interests, but government-wide challenges remain, including the need to address weaknesses in individual programs and fully implement export control reform.[7] Further, in February 2018, we reported on CFIUS workload and staffing as well as views on potential changes to CFIUS.[8]

You asked us to review DOD's ability, as a member of CFIUS, to address defense issues. This report assesses factors, if any, that affect DOD's

[4]See, for example, the Foreign Investment Risk Review Modernization Act of 2017, H.R. 4311, 115th Cong. (2017). Proposed changes include a change in the definition of a "covered transaction" to include certain purchases or leases by a foreign person of private or public real estate.

[5]Dollar amounts have been adjusted for inflation and are expressed in constant 2016 dollars.

[6]Pub. L. No. 115-91 (2017).

[7]GAO, *Critical Technologies: Agency Initiatives Address Some Weaknesses but Additional Interagency Collaboration Is Needed*, GAO-15-288 (Washington D.C.: Feb. 10, 2015).

[8]GAO, *Committee on Foreign Investment in the United States: Treasury Should Coordinate Assessments of Resources Needed to Address Increased Workload*, GAO-18-249 (Washington, D.C.: Feb. 14, 2018).

ability to (1) identify and address national security concerns through the CFIUS process, and (2) develop and monitor mitigation agreements through the CFIUS process.

This report is a public version of a sensitive report that we issued on April 5, 2018.[9] DOD and the Department of the Treasury (Treasury) deemed some of the information in our April report to be sensitive, which must be protected from public disclosure. Therefore, this report omits sensitive information related to (1) DOD's resources to perform certain CFIUS functions, like monitoring mitigation agreements and identifying non-notified transactions; (2) the availability of location information as part of notices that companies file with CFIUS; and (3) the resources and communication required between DOD and the components to develop and monitor mitigation agreements through the CFIUS process. Although the information provided in this report is more limited, this report addresses the same objectives and uses the same methodology as the sensitive report.

To assess what factors, if any, affect DOD's ability to identify and address national security concerns through the CFIUS process, we reviewed relevant documentation, including: CFIUS-related laws and regulations; DOD policies and guidance; and DOD and CFIUS internal reports. While there are other mechanisms that address national security concerns, including export controls such as the International Traffic in Arms Regulations and Export Administration Regulations, our review focused on DOD's responsibilities, processes, and challenges addressing national security concerns as a member of CFIUS. To assess DOD's efforts to identify and address national security concerns it identified, we analyzed data on transactions that DOD was responsible for co-leading from January 1, 2012 through December 31, 2017, the most recent data available. Based on information on the collection and management of Department of the Treasury (Treasury) and DOD transaction data, our review of related documentation, and interviews with relevant Treasury and DOD officials, we determined that these data were sufficiently reliable for our purposes. We also interviewed officials at Treasury, the Office of Manufacturing and Industrial Base Policy (MIBP)—the DOD office responsible for coordinating the CFIUS process within the department—and selected DOD component reviewers to discuss DOD's CFIUS

[9]GAO, *Committee on Foreign Investment in the United States: Action Needed to Address Evolving National Security Concerns Facing the Department of Defense,* GAO-18-261SU (Washington, D.C.: Apr. 5, 2018).

workload and resources.[10] In this report, we define resources as the authorized positions, assigned personnel, and personnel performing contract services related to CFIUS functions, and CFIUS-related costs. We also discussed with these officials any limitations to addressing certain national security concerns through the CFIUS process, and guidance for conducting CFIUS reviews and identifying transactions not voluntarily filed with the committee—known as non-notified transactions.[11]

We selected a non-generalizable sample of nine DOD component reviewers based primarily on their responsibilities for reviewing transactions for key issues relevant to DOD, including concerns with foreign investment in critical and emerging technologies and in proximity to critical military locations. To obtain a range of views, we also solicited MIBP's recommendations to identify components with varying levels of participation and input into the CFIUS process. We obtained responses from each component about similarities and differences in their CFIUS processes and any challenges they face identifying and addressing national security concerns. Findings based on information collected from the nine components cannot be generalized to all components.

To assess what factors, if any, affect DOD's ability to develop and monitor mitigation agreements through the CFIUS process, we reviewed CFIUS-related laws and regulations and DOD policies and guidance to identify DOD and its components' responsibilities and processes for developing and monitoring compliance with mitigation agreements. To identify actions DOD has taken to mitigate national security concerns, we analyzed data from January 1, 2012 through December 31, 2017, the most recent data available, to determine the number of mitigation agreements DOD is responsible for, and actions DOD has taken to monitor these agreements. Based on information on the collection and

[10]DOD component reviewers are organizations responsible for reviewing and investigating transactions submitted to CFIUS to determine if they pose any national security concerns. DOD components include the Office of the Secretary of Defense, the military departments, the Office of the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General, the Defense Agencies, the DOD Field Activities, and all other organizational entities within DOD. In this report, we also refer to some components more specifically, such as the military departments. For a list of DOD components with CFIUS responsibilities, see app. I.

[11]If member agencies become aware of a transaction that might be covered that has not been voluntarily notified to CFIUS and may raise national security considerations, CFIUS may invite the parties to the transaction to submit a notice. CFIUS also has the authority to unilaterally initiate a review of the transaction. 50 U.S.C. § 4565(b)(1)(D).

management of Treasury and DOD CFIUS mitigation agreement data, our review of related documentation, and interviews with relevant Treasury and DOD officials, we determined that these data were sufficiently reliable for our purposes. We interviewed officials at Treasury, MIBP, and DOD components—including those identified as part of our non-generalizable sample—to identify any challenges they face developing and enforcing mitigation agreements. To provide illustrative examples of the types of measures included in CFIUS mitigation agreements, we reviewed all of the active mitigation agreements from one component with responsibilities for monitoring mitigation agreements involving proximity issues. These agreements are not generalizable to other components. Appendix II provides more information about our overall scope and methodology.

The performance audit upon which this report is based was conducted from January 2017 to April 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with DOD and Treasury from April 2018 to July 2018 to prepare this unclassified version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

Background

CFIUS was established by executive order in 1975 to monitor the effect of and to coordinate U.S. policy on foreign investment in the United States.[12] In 1988, Congress enacted the Exon-Florio amendment adding section 721 to the Defense Production Act of 1950, which authorized the President to investigate the effect of certain foreign acquisitions of U.S. companies on national security and to suspend or prohibit acquisitions that might threaten to impair national security.[13] The President delegated this investigative authority to CFIUS. The Foreign Investment and

[12]Exec. Order No. 11,858, 40 Fed. Reg. 20,263 (May 7, 1975).

[13]Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, Title V, Subtitle A, Part II, § 5021, 102 Stat. 1425 (Aug. 23, 1988). The law specifies that the President is authorized to investigate "mergers, acquisitions, and takeovers proposed or pending on or after the date of enactment of this section by or with foreign persons which could result in foreign control of persons engaged in interstate commerce in the United States."

National Security Act of 2007 further amended the Defense Production Act and formally established CFIUS in statute.[14]

CFIUS is responsible for reviewing and investigating covered transactions to determine the effects of the transaction on national security. The Foreign Investment and National Security Act of 2007 does not formally define national security, but provides a number of factors for consideration by CFIUS and the President in determining whether a covered transaction poses a national security risk. These factors include the potential national security effects on U.S. critical technologies and whether the transaction could result in the control of a U.S. business by a foreign government (for a full list of factors, see Appendix III). CFIUS may also consider other factors in determining whether a transaction poses a national security risk.

Chaired by the Secretary of the Treasury, CFIUS includes voting members from the Departments of Commerce, Defense, Energy, State, Justice, and Homeland Security; the Office of the U.S. Trade Representative; and the Office of Science and Technology Policy.[15] Treasury is responsible for a number of tasks. According to Treasury officials, these tasks include coordinating operations of the committee, facilitating information collection from parties involved in the transaction (such as a foreign acquirer and U.S. business owner involved in an acquisition), reviewing and sharing data on mergers and acquisitions with member agencies, and managing CFIUS time frames.[16] Treasury also communicates with the parties on CFIUS's behalf. The committee generally has three core functions:

[14]Pub. L. No. 110-49, § 3 (codified at 50 U.S.C. § 4565(k)). The President's authority to suspend or prohibit any covered transaction that threatens to impair the national security of the United States may only be invoked when no law other than the Defense Production Act and the International Emergency Economic Powers Act provides adequate and appropriate authority to protect national security, and when there is credible evidence that the foreign interest exercising control might take action that threatens to impair the national security.

[15]In addition to the nine voting members, the Office of the Director of National Intelligence and the Department of Labor are non-voting *ex officio* members, with roles as defined in statute and regulation. Five White House offices also observe and, as appropriate, participate in CFIUS activities. CFIUS also solicits perspectives and expertise from non-member participant agencies, such as the Department of Agriculture, when necessary.

[16]For a full definition of "party" or "parties to a transaction" see CFIUS regulations at 31 C.F.R. § 800.220.

- review and investigate transactions that have been voluntarily submitted—or notified—to the committee by the parties to the transaction and take action as necessary to address potential national security concerns;
- monitor and enforce compliance with mitigation agreements; and
- identify transactions of concern that have not been voluntarily notified to CFIUS for review, referred to in this report as non-notified transactions.

The Foreign Investment and National Security Act of 2007 does not require that parties notify CFIUS of a transaction.[17]

In examining covered transactions, CFIUS members seek to identify and address, as appropriate, any national security concerns that arise as a result of the transaction. CFIUS reviews notices that have been voluntarily submitted—or notified—to the committee by parties to potentially covered transactions. Notices to CFIUS contain information concerning the nature of the transaction and the parties involved, such as the business activities performed by the U.S. business and any products or services supplied to the U.S. government. After receiving a notice, Treasury drafts an analysis to assess whether the transaction submitted is a covered transaction, meaning whether the transaction could result in foreign control of a U.S. business.

With limited exceptions, a transaction receives safe harbor—meaning the transaction cannot be reviewed again—when the CFIUS process is completed and the committee has determined that the transaction may proceed.[18] CFIUS does not review every transaction or investment by foreign entities. According to Treasury officials, there are certain transactions by foreign entities that CFIUS does not have the authority to review. These non-covered transactions and investments include the establishment of a business, referred to as a greenfield investment, and acquisitions of assets—such as equipment, intellectual property, or real property—if such assets do not constitute a U.S. business.[19]

[17]50 U.S.C. § 4565(b).

[18]According to Treasury officials, safe harbor provides the parties to the transaction some certainty that CFIUS and the President will not subject the transaction to review again.

[19]See 31 C.F.R. §§ 800.301, 800.302. See also 31 C.F.R. § 226 (definition of U.S. business).

If CFIUS member agencies become aware of a transaction that might be covered that has not been voluntarily notified to the committee and may raise national security considerations, CFIUS may invite the parties to the transaction to submit a notice. CFIUS may choose to unilaterally review any transaction that could be covered.[20] Treasury, DOD, and several other member agencies have processes for identifying non-notified transactions for CFIUS to potentially review.

CFIUS Process

The CFIUS process for examining transactions that have been notified to the committee is comprised of up to four stages:

- pre-notice consultation,
- national security review (30 days),
- national security investigation (45 days), and
- presidential action.[21]

In some cases, before a transaction is accepted and reviewed by CFIUS, Treasury may conduct a pre-notice consultation with parties to a transaction. This is not a required part of the process. For the purposes of this review, we focus on three stages—the national security review, national security investigation, and presidential action.

For each transaction accepted and reviewed by CFIUS, an agency or agencies with relevant expertise are identified to act as a co-lead with Treasury.[22] Each agency in turn distributes the transaction to various offices within its agency to provide an assessment of the transaction and identify national security risks, which is then provided to CFIUS. For example, the committee may reach consensus that no investigation is required if it is determined that the covered transaction will not impair national security or that the national security concerns are addressed under existing authorities, such as export controls. If these conclusions

[20]50 U.S.C. § 4565(b)(1)(D).

[21]For the purposes of this report, we refer to activities that occur during any of the four stages of this process as the CFIUS process.

[22]CFIUS may also reject a notice if the parties do not satisfy requirements in the regulations, such as not including all of the information required for CFIUS to review the transaction, or if, during the course of the CFIUS process, there is a material change to the transaction, a material misstatement, or a material omission in the notice by the parties.

are reached, the national security review ends, and the transaction proceeds.[23] However, if, for example, an agency identifies an unresolved national security risk, the agency may draft a risk-based analysis and CFIUS may undertake a national security investigation. If during the investigation the committee members reach consensus that a national security risk exists, but the risks can be mitigated, mitigation agreement measures are drafted to address those risks, and these measures are negotiated with the other members of the committee and the parties to the transaction.[24]

The CFIUS process may conclude after consensus is reached by all agencies and the co-lead agencies certify to members of Congress that there are no unresolved national security concerns, and the transaction receives safe harbor.[25] At the end of the national security investigation, if the committee does not reach consensus that there are no unresolved national security concerns or the committee concludes by consensus that a foreign investment threatens to impair national security and the threat cannot be mitigated, CFIUS elevates the transaction to the President. The President may prohibit or suspend the transaction. At any point prior to the conclusion of the process, parties may request to withdraw from the CFIUS process. In some cases, the notice is resubmitted once the parties believe that they have addressed the committee's concerns; in other cases, the companies may choose to withdraw and abandon their

[23]After CFIUS completes its review of the covered transaction, the committee provides a written certification to members of Congress, signed by the co-lead agencies, that there are no unresolved national security concerns.

[24]When a covered transaction presents national security risks, CFIUS, or a lead agency acting on behalf of CFIUS may enter into mitigation agreements with parties to the transaction, or impose conditions on the transaction to address such risks.

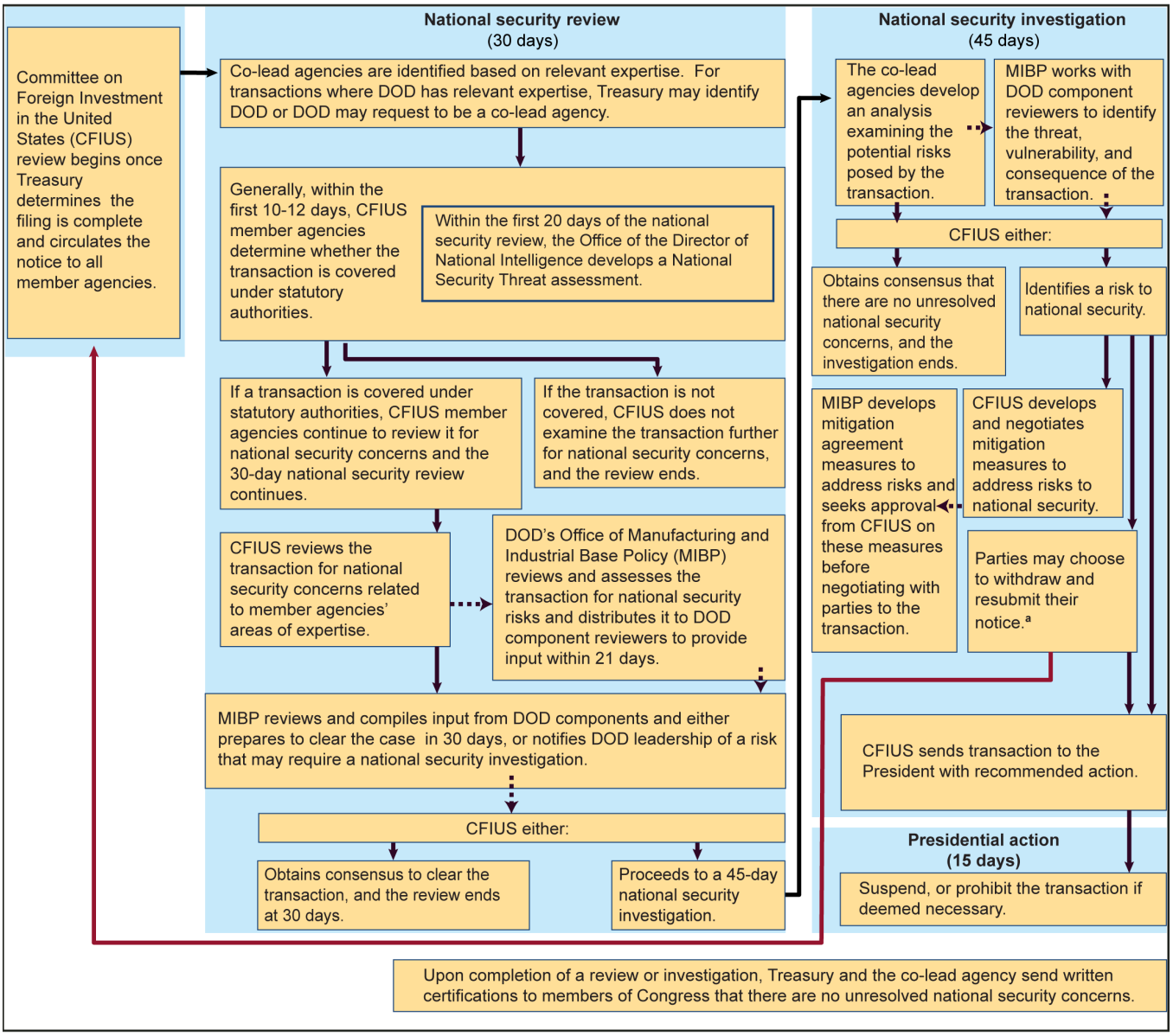
[25]According to DOD officials, while the Foreign Investment and National Security Act of 2007 does not require that the decision to approve a transaction be made by consensus, in practice, CFIUS seeks consensus among the member agencies on every transaction. As a matter of practice, before CFIUS clears a transaction to proceed, each member agency confirms to Treasury, at politically accountable levels, that it has no unresolved national security concerns with the transaction. Any agency that has a different assessment of the national security risks posed by a transaction has the ability to elevate that assessment to a higher level within CFIUS and, ultimately, to the President.

transaction.[26] See figure 1 for an overview of the CFIUS process for reviewing and investigating selected transactions.[27]

[26]For example, if CFIUS has determined that national security concerns cannot be mitigated, CFIUS typically advises the parties that the committee will recommend that the President prohibit the transaction in its current form. Sometimes companies choose to withdraw and subsequently abandon the transaction. If the parties withdraw and re-submit a transaction, the 30-day national security review period begins again, and the committee has another 75 days to complete the review and investigation of the transaction.

[27]See GAO-18-249 for a more detailed description of the CFIUS process.

Figure 1: DOD's Participation in the Process for Reviewing and Investigating Transactions Notified to the Committee on Foreign Investment in the United States (CFIUS)



Source: GAO analysis of Department of the Treasury (Treasury) and Department of the Defense (DOD) documents. | GAO-18-494

[a]According to Treasury officials, parties may withdraw and resubmit their notice at any point in the process to allow more time to engage with CFIUS to resolve national security concerns identified by the committee. Parties may also withdraw and subsequently choose to abandon the transaction.

DOD CFIUS Process

DOD Instruction 2000.25, *Procedures for Reviewing and Monitoring Transactions Filed with the Committee on Foreign Investment in the United States* (DOD's Instruction), provides policy and guidance on the DOD CFIUS process and assigns responsibilities in that process.[28] In March 2011, DOD's CFIUS responsibilities were reassigned from the Defense Technology Security Administration to the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD (AT&L)).[29] The transfer of responsibilities, effective in fiscal year 2012, was intended to better align CFIUS's mission with the DOD office responsible for industrial policy. Within OUSD (AT&L), MIBP serves as the lead office for CFIUS, reviews transactions for DOD equities, and distributes them to more than 30 organizations within DOD—referred to in this report as DOD components —to determine whether the transaction poses any national security concerns.[30] These component reviewers include organizations within the Office of the Secretary of Defense, as well as the military departments, among others. For a full list of DOD component reviewers, see appendix I.

According to MIBP's processes, it is responsible for reviewing and compiling comments and input from all DOD component reviewers during the 30-day national security review.[31] When national security concerns with a transaction are identified, MIBP is to coordinate with affected DOD component reviewers to clarify issues and arrive at consensus on the

[28]DOD Instruction 2000.25, *Procedures for Reviewing and Monitoring Transactions Filed with the Committee on Foreign Investment in the United States,* (Aug. 5, 2010).

[29]The National Defense Authorization Act for Fiscal year 2017 eliminated the position of OUSD(AT&L) effective February 1, 2018. Pub. L. No. 114-328, § 901(a) and (b) (2016) (codified at 10 U.S.C. §§ 133a and 133b). The position has been divided into the Under Secretary of Defense for Research and Engineering and the Under Secretary of Defense for Acquisition and Sustainment. According to DOD officials, the Assistant Secretary of Defense for Research and Engineering is now the Under Secretary of Defense for Research and Engineering. For the purposes of this report, we are using the titles of Assistant Secretary of Defense for Research and Engineering and OUSD(AT&L) as these reflect the organization of DOD at the time of our review.

[30]DOD's 2010 Instruction identifies more than 30 components that may be involved in reviewing CFIUS transactions, and according to MIBP officials, additional components may review depending on the scope of the transaction.

[31]Concurrent with the review process, the Office of the Director of National Intelligence develops a national security threat assessment, with input and support from the intelligence community, to be completed during the first 20 days of the national security review. Certain DOD components also participate in providing input to this process. 50 U.S.C. § 4565(b)(4).

DOD position for the transaction. DOD is typically designated as a co-lead agency for transactions where it has identified equities—such as transactions involving companies that are DOD suppliers—or other potential national security concerns. If no national security concerns are identified by DOD, MIBP will recommend that the transaction proceed.

However, if national security concerns are identified by DOD and the committee requires additional time to complete its review, DOD recommends that the transaction proceed to a 45-day national security investigation period. During this period, MIBP coordinates with DOD component reviewers to draft and deliver a risk-based analysis to Treasury within the statutory investigation time frame. The assessment provides a description of the risk—in terms of threat, vulnerability, and consequence—arising from the covered transaction. If the risks can be addressed, DOD develops measures to be included in the mitigation agreement that it is then responsible for monitoring and enforcing as a signatory agency to the mitigation agreement.[32]

DOD guidance identifies three basic types of mitigation measures:

1. **Technical mitigation measures**, which seek to address risks related to vulnerabilities or critical assets with sensitive source codes, cutting-edge technologies, and communications infrastructure.
2. **Personnel mitigation measures**, which seek to address risks arising from foreign personnel having access to sensitive technology or other critical assets.
3. **Management control mitigation measures**, which seek to oversee companies' ongoing implementation of mitigation agreements related to technical or personnel mitigation measures.

DOD, along with other lead agencies, carries out its monitoring responsibilities on behalf of the committee and reports back to the committee on the status of their responsibilities and company compliance on at least a quarterly basis.[33] DOD's Instruction requires the

[32]If other co-lead agencies have equities in the transaction MIBP may work with them to develop and enforce the mitigation agreement. MIBP officials said they are also sometimes signatories to mitigation agreements even if they are not a co-lead agency when reviewing and investigating the transaction.

[33]In addition, signatories to mitigation measures that were entered into before the Foreign Investment and National Security Act of 2007 took effect also report to CFIUS quarterly on compliance with those measures.

identification of feasible measures to mitigate or eliminate the risks posed by a transaction and emphasizes that adequate resources, in terms of personnel and budget, should be provided to DOD and the components for monitoring and ensuring compliance with mitigation agreements.

Our Prior Work on CFIUS

We have conducted prior work related to CFIUS issues, including whether CFIUS has the resources to address its current workload and whether CFIUS is able to address national security concerns related to the proximity of certain real estate transactions to defense test and training ranges.

- In February 2018, we reported on CFIUS workload and staffing as well as stakeholder perspectives on potential changes to CFIUS. We found that as the volume and complexity of CFIUS reviews have increased in recent years, member agency officials have expressed concerns that current CFIUS staffing levels may not be adequate to complete core functions of the committee.[34] We recommended that Treasury should coordinate member agencies' efforts to better understand the staffing levels needed to address the current and projected CFIUS workload associated with core committee functions. Treasury agreed with our recommendation.
- In December 2014, in reviewing DOD's assessment of foreign encroachment risks on federally managed land, we found that DOD did not have the information it needed to determine whether activities by foreign entities near test and training ranges, such as performing certain sensitive training techniques, could pose a threat to its mission.[35] We also reported that CFIUS is the only formal option in regard to transactions involving foreign companies or entities that accounts for national security concerns related to proximity to military test and training ranges. We recommended that DOD develop and implement guidance for conducting an assessment of risks to test and training ranges from foreign encroachment. We also recommended that DOD collaborate with other federal agencies managing land and transactions adjacent to DOD's test and training ranges to obtain additional information on transactions near these ranges. DOD agreed

[34]GAO-18-249.

[35]GAO, *Defense Infrastructure: Risk Assessment Needed to Identify If Foreign Encroachment Threatens Test and Training Ranges,* GAO-15-149 (Washington, D.C.: Dec. 16, 2014).

with our recommendations and has begun collecting data to identify locations the military services consider to be at risk from foreign encroachment and collaborating with federal land management agencies, as discussed later in the report.[36]

Resources and Evolving National Security Risks Pose Challenges for Identifying and Addressing DOD's Concerns through the CFIUS Process

DOD has reviewed hundreds of transactions involving foreign acquirers and U.S. businesses since 2012, but faces several challenges in identifying and addressing national security concerns through the CFIUS process. These challenges are: (1) resources not aligned with an increasing workload; (2) some national security concerns not defined or addressed in DOD's Instruction; (3) some investments that pose national security concerns not always able to be addressed through the CFIUS process; and (4) current component reviewer responsibilities and CFIUS processes not reflected in DOD's Instruction.

DOD Has Not Assessed Resources to Address a Substantially Increased CFIUS Workload

DOD faces challenges addressing an increasing CFIUS workload with its current resources.[37] For example, we found that the number of DOD personnel with CFIUS responsibilities has not kept pace with the growing workload. The number of transactions CFIUS reviewed from 2012 through 2017 more than doubled, increasing from 114 transactions to 238 transactions. During that time, the number of transactions DOD was responsible for co-leading increased by about 57 percent, to 99

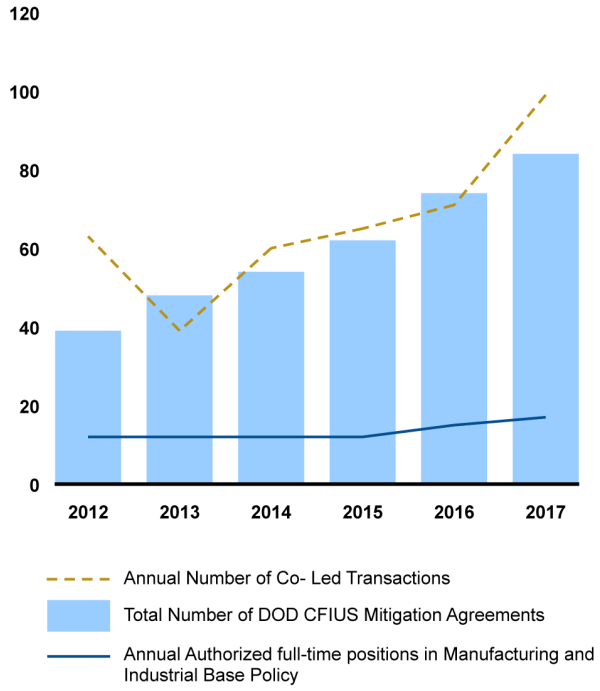
[36]In 2016, we further reviewed DOD's efforts to assess the national security risks and effects of foreign encroachment on federally managed lands, and found that DOD had made limited progress since our 2014 report, see GAO, *Defense Infrastructure: DOD Has Made Limited Progress in Assessing Foreign Encroachment Risks on Federally Managed Land*, GAO-16-381R (Washington, D.C.: Apr. 13, 2016). We also reported on CFIUS's limited role in identifying risks of GSA leasing from foreign companies, see GAO, *Federal Real Property: GSA Should Inform Tenant Agencies When Leasing High-Security Space from Foreign Owners,* GAO-17-195 (Washington, D.C.: Jan. 3, 2017).

[37]In our February 2018 report on CFIUS, we reported that CFIUS has not assessed whether current staffing levels across CFIUS member agencies is adequate to address the core functions of the committee. For purposes of this report, we use the term "resources" to refer more broadly to DOD's authorized positions, assigned personnel, and personnel performing contract services related to CFIUS functions, and CFIUS-related costs.

transactions in calendar year 2017.[38] From 2016 through 2017 alone, these increases resulted in DOD reviewing almost 65 additional transactions, and co-leading about 30 additional transactions, a substantial increase in workload in one year. DOD also experienced an increase in the cumulative number of mitigation agreements it was responsible for monitoring, more than doubling from 39 in 2012 to 84 in 2017. Figure 2 provides additional information on DOD's workload and authorized positions in MIBP—the lead DOD office for CFIUS.

[38]2017 figures on DOD's co-led transactions and mitigation agreements are based on transactions submitted to CFIUS as of December 31, 2017. As of that date, some transactions submitted were still under review which could affect the final number of DOD co-led transactions and cumulative mitigation agreements for calendar year 2017.

Figure 2: Department of Defense's (DOD) Committee on Foreign Investment in the United States (CFIUS) Workload and Resources, Calendar Years 2012-2017



Source: GAO analysis of Department of Defense (DOD) and Department of the Treasury data. | GAO-18-494

Notes: The above graphic represents DOD's cumulative mitigation agreement responsibilities from 2012 through 2017.

2017 figures on DOD's co-led transactions and mitigation agreements are based on transactions submitted to CFIUS as of December 31, 2017. As of that date, some transactions submitted were still under review which could affect the final number of calendar year 2017 DOD co-led transactions and cumulative mitigation agreements.

From 2012 to 2017 authorized CFIUS positions within DOD's Office of Manufacturing and Industrial Base Policy increased from 12 to 17. These positions perform a range of CFIUS activities, including reviewing transactions and developing and monitoring mitigation agreements, among other activities. The number of positions dedicated to performing these activities has varied over time.

Based on our review of data on transactions reviewed by CFIUS, DOD's workload has also been affected by the volume and amount of time spent on the transactions it has reviewed. We found almost half of DOD's co-led transactions from 2015 through 2016—83 of 136 transactions, or 61 percent—required 45-day national security investigations. According to Treasury officials, the number of transactions requiring national security investigations increases member agencies' workload because these transactions are usually more complex and require additional resources to review. Further, 9 DOD co-led transactions from 2015 through 2016 were withdrawn and resubmitted to CFIUS, and another 7 were

withdrawn and abandoned because of national security concerns or because the committee was going to recommend that the transaction be prohibited. MIBP officials told us that withdrawn and resubmitted or withdrawn and abandoned transactions indicate the complexity of their workload, because a significant number of hours are spent either reviewing resubmitted transactions or justifying the committee's decision to prohibit the transactions. Moreover, MIBP officials said that depending on the scope and complexity of the national security concerns identified within a transaction, they have had to redirect resources from other functions to support their review responsibilities. As a result, the official said there have been instances where MIBP has had to shift priorities and delay performing other CFIUS tasks in order to assist with reviewing high priority transactions.

In addition to reviewing transactions, as a co-lead agency, DOD is also responsible for negotiating any mitigation agreements or other conditions necessary to protect national security, and monitoring compliance with those agreements or conditions. However, according to DOD officials and documents we reviewed, there are limited resources within MIBP and at the DOD component level to do so. For example, MIBP officials said that the volume and complexity of mitigation agreements have increased their workload monitoring these agreements and strained their available resources. Specific details on the effect of mitigation agreement workload increases on MIBP's resources have been omitted because that information is considered sensitive.

In addition, MIBP officials stated that because mitigation agreements typically do not expire, the number of agreements MIBP will be responsible for monitoring will continue to increase in the future. For example, based on our review of MIBP mitigation agreement information, 6 transactions with active mitigation agreements that MIBP is monitoring have been in place for 10 years or more.[39]

We also found that MIBP has limited personnel available to identify transactions not voluntarily filed with CFIUS—non-notified transactions—that could pose national security concerns. In the absence of voluntary reporting by the parties involved or independent discovery of the transaction, it is possible that CFIUS may not review a non-notified

[39]According to officials, while some CFIUS mitigation agreements have sunset provisions or have been terminated, most do not have an end date.

covered transaction that could pose a risk to national security. To address this concern, MIBP officials began efforts to identify and research non-notified transactions in fiscal year 2016 and, at one point, had up to four personnel involved in this effort. However, according to MIBP officials, three of those personnel were reassigned to help conduct reviews of notified transactions, leaving one person responsible for identifying and researching non-notified transactions relevant to DOD. Specific details on the effect of limited personnel on MIBP's ability to identify non-notified transactions have been omitted because the information is considered sensitive.

To perform its CFIUS responsibilities, OUSD (AT&L) began receiving some funding for CFIUS in fiscal year 2014—on average about $2.4 million dollars a year. However, according to an MIBP official, the funding MIBP receives for CFIUS is typically received after other priorities within OUSD (AT&L) have been addressed. Further, OUSD (AT&L)'s funding does not include CFIUS responsibilities being performed by the other DOD components, which according to MIBP officials do not typically have their own resources for performing CFIUS responsibilities. Among the components we spoke with, the amount of time and personnel dedicated to CFIUS responsibilities varies greatly. According to these components, the amount of time and personnel reviewing transactions ranged from one person dedicating a few hours a month at one component, to a full-time responsibility for six personnel at another component. However, most of the components we spoke with said that CFIUS is a part-time responsibility, and only four of the nine components we spoke with had dedicated personnel to support CFIUS responsibilities. MIBP officials confirmed that the components often have limited personnel and funding to perform CFIUS responsibilities, which can affect the level of involvement components have in reviewing transactions, monitoring mitigation agreements, and researching the non-notified transactions.

Recognizing the resource constraints posed by its increased workload, MIBP has taken some steps to assess and adjust its CFIUS resources. For example, MIBP received an increase in its authorized positions in fiscal years 2016 and 2017. Specifically, authorized positions increased from 12 to 17, and according to MIBP officials, 16 of the 17 positions were filled as of October 2017. In January 2017, MIBP requested that component reviewers estimate their CFIUS resource needs to address increases in CFIUS workload. According to an MIBP official, this information was used to support a fiscal year 2019 request for additional funding and personnel to perform CFIUS responsibilities department-wide, and for funding to further develop information technology solutions

for managing DOD's CFIUS process. However, MIBP officials told us their request was only partially funded by the department, and that MIBP would have to determine how to distribute the funding received across the various components to perform its CFIUS responsibilities.

DOD's Instruction states that DOD components shall ensure that adequate resources, in terms of personnel and budget, are available for statutorily required mitigation agreement monitoring and compliance activities.[40] Moreover, federal internal control standards state an agency should establish the organizational structure necessary to achieve its objectives and periodically reevaluate this structure.[41] In this case, this includes the resources needed to accomplish CFIUS responsibilities, such as monitoring mitigation agreements and identifying non-notified transactions. However, according to an MIBP official, prior increases in authorized positions were not added based on any formal review or analysis of resource needs or capability gaps. While MIBP has taken some steps to address its resource limitations, MIBP and some other DOD component officials we spoke with who have CFIUS responsibilities continue to face resource constraints to address their growing workload. Even after receiving approval for some additional funding across DOD to support CFIUS responsibilities, DOD's resource limitations could be further exacerbated if the number of transactions continues to increase. Without a formal analysis to assess and prioritize the resources necessary for performing its current and future CFIUS responsibilities, DOD will likely face challenges carrying out the duties and responsibilities outlined in its CFIUS policy. In addition to keeping up with the workload involved in reviewing notified transactions, the risks include not knowing whether violations of mitigation agreements or non-notified transactions are occurring that could pose risks to national security.

National Security Concerns for Some Investments Are Not Well-Defined in DOD Policy

DOD faces evolving national security concerns from foreign investments in U.S. businesses developing emerging technologies and in proximity to critical military locations, but there are inconsistencies in how DOD is reviewing these investments. DOD's Instruction identifies factors to assess relevant to DOD national security interests, such as whether a

[40]Department of Defense Instruction 2000.25, *Procedures for Reviewing and Monitoring Transactions Filed with CFIUS*.

[41]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014).

firm produces critical technologies or unique defense capabilities, or whether a company being acquired is part of DOD critical infrastructure that is essential to project, support, or sustain military forces. However, DOD's Instruction does not address the extent to which emerging technologies and proximity to critical military locations are considered under these factors, or whether and how components should review and prioritize transactions for these concerns.

- ***Emerging Technology:*** Officials at several of the DOD components we spoke with identified challenges addressing concerns related to emerging technology, such as artificial intelligence and robotics, through the CFIUS process and varied as to whether they elevate concerns with transactions involving emerging technology. For example, officials at four components said that it can be difficult to explain the risks associated with foreign investment in U.S. businesses developing emerging technologies, particularly if the technology in question is not already being used in a defense program or not being acquired through a traditional merger or acquisition. Officials from another component noted that it can be difficult to identify vulnerabilities and explain the need to protect early stage technologies through the CFIUS process if the technology is not advanced enough. DOD's Instruction defines critical technologies based in part on those items that are already subject to export controls, but does not specify the types of emerging technologies that could be of concern for the department.[42] Officials at several components noted that it can be difficult for them to identify which emerging technologies are going to be important to DOD to know whether transactions should be mitigated or prohibited. DOD has several lists identifying critical technologies or assets, but does not have an agreed-upon list of emerging technologies that should be protected from foreign investment, making it difficult for components to know which emerging technologies are of concern to the department.

  A recent DOD report noted that having an agreed-upon list of critical technologies would provide clarity on which transactions reviewed by

[42]Instead, DOD's Instruction states that emerging critical defense technology that is still under research or development, that putatively when complete will produce a defense article or service, including its underlying technology and software that would be subject to certain export controls, would be considered critical.

CFIUS should be prohibited or suspended.[43] According to MIBP officials, they recently initiated a study to identify leading companies and technology areas critical to the department now and in the future. They intend for the study, planned to be completed in spring of 2018, to identify critical and emerging technology sectors and companies not currently included in the defense industrial base. According to DOD officials knowledgeable of the study, MIBP plans to use the results to work with the department's Office of Small Business and others on ways to use internal DOD resources to protect emerging technologies and intellectual property that are critical to DOD before they are subject to foreign investment. However, officials did not state how the study would help them address emerging technology through CFIUS-related reviews or whether the results of the study would inform changes to DOD's Instruction or otherwise be used to help guide components on which emerging technologies are critical to the department.[44]

- ***Proximity:*** Each of the military departments varies in how it reviews transactions for proximity to critical military locations.[45] According to DOD reports, transactions near certain military locations can present encroachment issues or opportunities for persistent surveillance and collection of sensitive information of training procedures or of the integration of certain technological capabilities into major weapon systems.[46] When asked about how transactions are reviewed for proximity concerns, MIBP officials said they defer to the military departments to identify what constitutes a concern and do not limit proximity to certain locations. Moreover, MIBP officials stated that

[43]Defense Innovation Unit Experimental, *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation*, (June 24, 2017).

[44]Our prior work has reported that previous DOD efforts to identify critical military technologies, for example through the Military Critical Technology List, have not been kept up to date, but that widespread requirements to know what technologies are militarily critical remain. See GAO-15-288.

[45]The three military departments include the departments of the Army, Air Force, and Navy, and are the primary DOD components responsible for reviewing transactions for proximity concerns to critical military locations, like certain test and training ranges.

[46]Secretary of Defense, Under Secretary of Defense (Personnel and Readiness) *Report to Congress 2017 Sustainable Ranges,* (Feb. 24, 2017) and Office of the Assistant Secretary of Defense for Readiness, *Secretary of Defense Report to the Congressional Defense Committees Security Risks Related to Foreign Investment in the United States*, (September 30, 2015).

depending on the transaction, proximity concerns can arise regardless of distance to a critical location, and that the circumstances surrounding a transaction should be reviewed on a case-by-case basis to account for those concerns.

Proximity is not defined in the current DOD Instruction or listed as a factor that the military departments should consider when reviewing transactions. Officials from two of the military departments we spoke with review every transaction on a case-by-case basis for proximity concerns. According to documentation from the third department, it limits its reviews to acquiring companies from certain countries and only assesses those transactions for proximity concerns if the target location is within a certain distance of designated critical locations or assets. These different approaches for reviewing transactions have resulted in inconsistencies among the military departments in the types of proximity concerns they elevate to CFIUS. For example, in one transaction, we found that officials from the third military department recognized a concern near a training range used by all three military departments. While the transaction was ultimately withdrawn because CFIUS planned to recommend that the President prohibit or suspend the transaction, the third department did not identify a national security risk because it did not meet its criteria. Officials from this military department stated that greater clarification on the types of proximity concerns DOD wants to elevate through the CFIUS process, as well as criteria that component reviewers should use to identify risks, would be helpful.

Our prior work has identified challenges DOD faces in identifying risks to foreign encroachment near defense training ranges. In a December 2014 report, we recommended that DOD develop and implement guidance for assessing risks to certain test and training ranges from foreign encroachment based on mission criticalities and level of threat.[47] According to DOD officials, they recently conducted a data call to the military departments to identify the locations that they consider to be at risk from foreign encroachment. DOD plans to use this information to develop guidance, not related to the CFIUS process, to assess the risks that test and training ranges face from foreign encroachment.

[47]GAO-15-149.

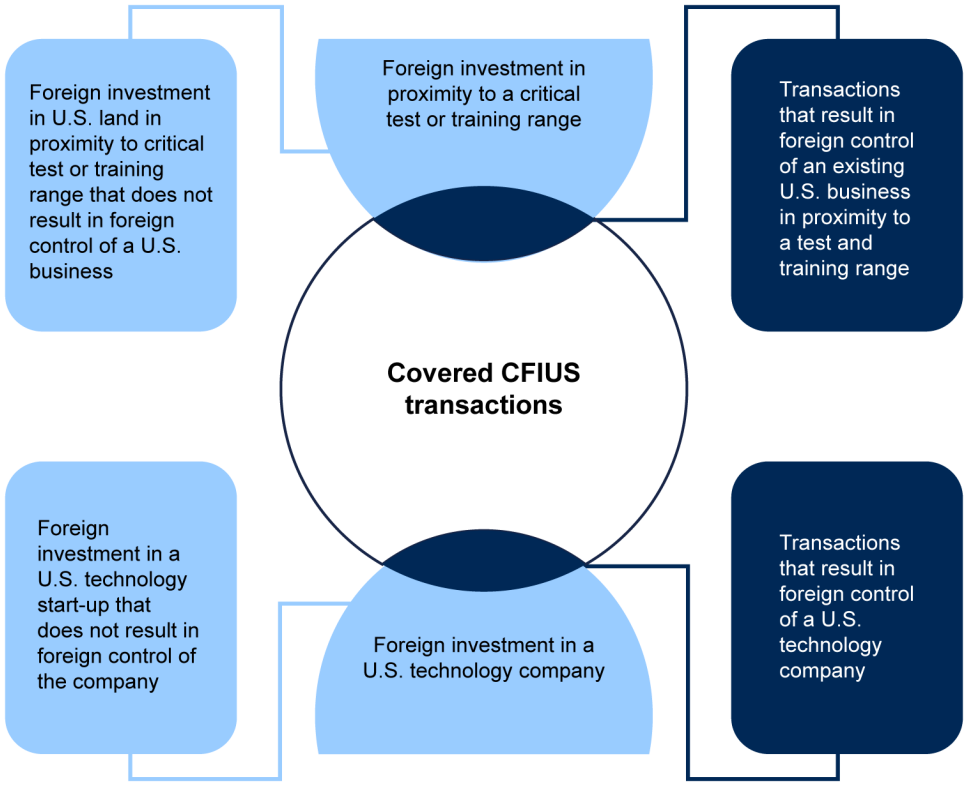
Federal internal control standards state that agencies should clearly define objectives and risk tolerances; identify, analyze, and respond to risks, and communicate necessary information to achieve their objectives.[48] DOD is taking steps to identify and assess areas of concern related to emerging technology and proximity, but these efforts are not specific to the CFIUS process and have not yet been completed or communicated to components through DOD's Instruction, or otherwise. As a result, the components lack clear and consistent guidance on how to review transactions for these specific types of national security concerns facing the department. Without clarity on the types of transactions and national security risks that should be addressed, for example by incorporating the results of its efforts into DOD's Instruction, component reviewers will likely continue to be inconsistent in reviewing transactions and identifying and prioritizing national security concerns.

DOD Has Identified Some Investments That Present National Security Concerns but Are Not Addressed through the CFIUS Process

In addition to challenges identifying certain national security concerns within DOD, CFIUS officials at Treasury and DOD indicated that national security concerns for some foreign investments—such as those related to critical and emerging technologies and proximity to certain military locations—can arise that the committee does not have the authority to review. For example, pursuant to CFIUS regulations, the purchase of property that does not constitute a U.S. business by a foreign person or the licensing of emerging intellectual property to a foreign person are not covered transactions and therefore not addressed through the CFIUS process. As shown in figure 3, while some foreign investments that may result in national security concerns related to critical and emerging technology and proximity are addressed through the CFIUS process, others are not. According to DOD reports, CFIUS is one of the only tools able to address foreign investment in the United States, but is limited in its ability to address some investments in emerging technology and in proximity to military locations. Without the ability to address national security concerns arising from these investments, DOD is at risk of losing access to technologies, assets, and locations critical to maintaining and advancing U.S. technological superiority.

[48]GAO-14-704G.

Figure 3: DOD-Identified Examples of Investments That May or May Not Be Addressed by the CFIUS Process



Source: GAO analysis of DOD documents 50 U.S.C. § 4565 and 31 C.F.R. Part 800. | GAO-18-494

Note: Graphic does not represent a numerical calculation.

Joint Ventures and Other Investments Can Result in Technology Transfers That Are Not Addressed through the CFIUS Process

A June 2017 DOD report found that although CFIUS is one of the only tools available to address technology transfers as a result of foreign investment, it is not effective at stopping technology transfer for investments that are not addressed through the CFIUS process, like certain joint ventures and other minority investments that do not result in foreign control.[49] However, according to DOD documents and officials, these investments can result in technology transfers that threaten U.S. national security. For example, according to the DOD report, Chinese

[49]Defense Innovation Unit Experimental, *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation.*

investors have been active in emerging technology sectors like artificial intelligence, augmented and virtual reality, and robotics, and Chinese investment in venture-backed start-ups is on the rise. The report also found that China's continued foreign investment in critical emerging technology companies may have consequences for DOD's ability to work with these companies in the future and its ability to maintain U.S. technological superiority.[50]

DOD officials cited concerns with their inability to address certain investments through the CFIUS process that can result in technology transfers or limit DOD access to emerging technologies. For example, DOD officials from three components cited instances when companies entered into joint ventures or other investment structures after withdrawing their transaction from the CFIUS process. A DOD official at one component cited a 2016 transaction where CFIUS planned to recommend that the President prohibit the transaction to prevent the transfer of a critical technology from a U.S. company to a foreign acquirer. Following the companies' subsequent withdrawal from the CFIUS process, they entered into a joint venture. While CFIUS is aware of the joint venture and that it could result in the same transfer of technology CFIUS attempted to prevent by proposing to prohibit the original transaction, the committee has not yet determined whether it can be addressed through the CFIUS process because CFIUS is only able to review certain types of joint ventures. According to Treasury officials, when these circumstances arise they are sometimes able to review the joint venture, depending on the structure of the investment and whether it meets the definition of a covered transaction pursuant to law and associated regulations.[51] Yet, even if this joint venture is ultimately reviewed as a covered transaction, the technology that DOD and CFIUS were originally concerned with may have already been transferred to the foreign acquirer.

DOD and Treasury officials also identified concerns with broader foreign investment trends in critical and emerging technology that may not be addressed through the CFIUS process. For example, according to MIBP officials, they are concerned about foreign-owned enterprises exploiting

[50]Our prior work has also reported on the importance of technological superiority to U.S military and foreign policy strategies. See GAO-15-288.

[51]50 U.S.C. § 4565(a)(3), 31 C.F.R. § 800.224(e) (formation of a joint venture included in definition of transaction) and 31 C.F.R. § 800.301(d) (explaining when a joint venture is a covered transaction).

critical technologies by structuring investments to avoid the CFIUS process, and noted that multiple investment structures exist that can allow foreign acquirers to gain access and influence over critical capabilities. DOD and Treasury officials acknowledged the importance of critical and emerging technologies and the consequences to DOD's technological superiority if adversaries are able to use these technologies to advance their own military capabilities. According to Treasury officials, determining whether and how CFIUS should expand its scope to address these concerns is one of the challenges they have encountered when they have considered potential legislative changes to the CFIUS process. For example, they said that if the scope of the law was expanded, it could pose additional resource challenges, as CFIUS agencies would be required to review an expanded number of potentially complex transactions.

According to federal internal control standards, agencies should identify, analyze, and respond to significant changes that could affect their operations.[52] As noted earlier, DOD is in the process of identifying emerging technologies that will be essential to the defense industrial base, an important step towards informing future decision-making within the department. However, according to MIBP officials, the study will primarily be focused on identifying specific technology companies of importance to the department. As noted earlier, the study is not specific to CFIUS, and as a result plans for the study do not indicate that it will identify and assess other limitations facing MIBP, like those encountered addressing certain types of foreign investments that are not addressed through the CFIUS process but that pose risks to DOD's technological and military superiority. Given the importance of critical and emerging technology to DOD, assessing any challenges DOD faces addressing certain foreign investments in critical and emerging technologies through the CFIUS process, and considering whether additional authority is needed, would better position DOD to address any unresolved national security concerns associated with these types of foreign investments. Without such an assessment, DOD remains at risk of not having the necessary tools and authorities to prevent the transfer of critical and emerging technologies to foreign acquirers, which is important for maintaining a viable defense industrial base and U.S. technological superiority.

[52]GAO-14-704G.

Some Foreign Investments Not Addressed through CFIUS Process Pose Proximity Concerns near Critical Military Locations

Some proximity concerns near critical military locations can be addressed by CFIUS, but DOD also identified challenges addressing proximity concerns with investments that are not able to be addressed through the CFIUS process. For example, the establishment of businesses (which may include land purchases) in the United States that do not include an existing U.S. business—referred to as greenfield investments—are not considered covered transactions, but can pose proximity concerns when near certain military locations.[53] Officials at MIBP and several other components expressed concerns with their inability to address proximity concerns arising from these investments, which can pose significant national security risks and limit DOD's ability to perform necessary test and training activities. We identified at least two greenfield investments that have occurred since 2016 that have posed proximity concerns near critical military locations, and were not able to be addressed through the CFIUS process.

- One investment involving a purchase of land presented risks due to its proximity to an Air Force base. According to *DOD's Report to Congress 2017 Sustainable Ranges*, the investment involved a U.S. company with substantial foreign financing, potentially subjecting training range missions performed at the base to persistent monitoring by a foreign government.[54] According to officials, although the Air Force identified concerns with the investment, because it did not result in foreign control of a U.S. business, it was determined to not be a covered transaction.
- Officials from another military department identified an investment that was not voluntarily filed with CFIUS and posed proximity issues near a training range. According to military department officials, the investment involved the same foreign acquirer that had been a source of concern in other voluntarily filed CFIUS transactions. The military department elevated its concerns to CFIUS through the non-notified process, but, according to officials, Treasury ultimately determined that it was not a covered transaction because there was no foreign control over a U.S. business. Moreover, because the investment was already completed, the company had started construction that

[53]In February 2018, we reported that DOD, along with a few other CFIUS member agencies and other outside experts, said that more clearly including the creation of new businesses and joint ventures could improve CFIUS coverage. See GAO-18-249.

[54]Secretary of Defense, Under Secretary of Defense (Personnel and Readiness), *Report to Congress 2017 Sustainable Ranges*.

threatened to encroach upon a training range that is one of only two in the country available to perform certain types of training. Military department officials said it was too soon to determine the effect that this investment would have on their ability to perform training, but emphasized the criticality of protecting unique testing and training range spaces.

Our prior work on defense training ranges also identified limitations DOD faces in addressing proximity and encroachment concerns from foreign investment.[55] For example, we found in 2014 that officials from the Navy and Air Force, in particular, had concerns about the number of investment-related projects by foreign entities near their ranges (such as leases for mining or oil or natural gas exploration), which could pose potential security risks. However, we reported that DOD does not have access to the information needed to determine whether foreign investment activities near testing and training ranges pose a threat because other civilian federal agencies, such as the Departments of Interior and Transportation, that are responsible for approving these transactions face legal, regulatory, or resource challenges that prevent them from collecting information unrelated to their missions. We found that, although DOD has had some success obtaining information on foreign investment near test and training ranges, these efforts have been based on informal coordination between military liaisons at certain bases and local Department of Interior representatives. In addition to our recommendation that DOD develop and implement guidance for assessing risks to certain test and training ranges from foreign encroachment, we recommended that DOD collaborate with these other federal agencies to gather additional information needed for transactions in proximity to DOD test and training ranges, and seek legislative relief if needed. DOD concurred with our recommendations and has taken some steps to address them. For example, as noted earlier, DOD is in the process of developing guidance to assess risks to test and training ranges based on its identification of locations it considers to be at risk from foreign encroachment. According to DOD officials, they have also drafted legislative proposals to address limitations to their ability to gather information from the land management agencies on foreign investments in proximity to critical military locations. According to DOD officials, these proposals have not been submitted to Congress due to concerns raised by the federal land management agencies, but DOD continues to explore the possibility of legislative action to address these concerns.

[55]GAO-15-149.

We also reported that DOD uses multiple methods, in coordination with other federal agencies, to identify potential business activities near DOD test and training ranges. But CFIUS is the only formal option in regard to transactions involving foreign companies or entities that accounts for national security concerns. A 2015 DOD report to Congress on security risks related to foreign investment in the United States found that there are no authorities in the current federal land management framework that would require federal land management agencies to prevent a transaction from occurring if DOD identified a national security concern.[56] The report further states that CFIUS and the Foreign Investment and National Security Act of 2007 are the only federal authorities available to DOD to assess national security risks posed by foreign investment in the vicinity of critical military locations, like DOD training and test ranges, but that the CFIUS process is not intended to address such national security risks. While CFIUS is able to address proximity concerns that arise through covered transactions, DOD has reported that it has limited ability to identify, assess, and mitigate national security concerns for investments that are not considered covered transactions through CFIUS, such as greenfield investments. However, DOD's report does not identify, assess, or make recommendations about what additional DOD authority, if any, would be necessary to address these concerns, and as noted earlier, DOD's efforts to develop and implement guidance based on its identification of locations that they consider to be at risk from foreign encroachment are still in progress.

According to federal internal control standards, agencies should establish policies and procedures to respond to risks; and identify, analyze, and respond to significant changes that could affect their operations.[57] DOD is in the process of identifying locations it considers to be at risk from foreign encroachment, which can eventually be used to inform its review of foreign investments for proximity concerns, but DOD states that it is currently unable to address concerns related to greenfield investments through the CFIUS process because they are not considered covered transactions.[58] Moreover, DOD reported that CFIUS is not a DOD-led process, and DOD is just one of nine member agencies. Members of

[56]Office of the Assistant Secretary of Defense for Readiness, *Secretary of Defense Report to the Congressional Defense Committees Security Risks Related to Foreign Investment in the United States*.

[57]GAO-14-704G.

[58]50 U.S.C. § 4565 and 31 C.F.R. § 800.301(c).

Congress have recently proposed legislation that would expand the definition of covered transactions to include foreign acquisitions or leases of real estate in proximity to U.S. military locations, but the legislation is pending. Taking additional steps to assess what authority, if any, is needed to address foreign investment in proximity to certain critical military locations and raising these concerns to Congress, as necessary, would better position DOD to address its concerns. Until DOD completes efforts to develop and implement guidance assessing risks to critical locations that should be protected from foreign encroachment, and assesses what authority, if any, is necessary to independently address concerns with investments near these areas, it remains at risk of not protecting these locations from the national security risks posed by foreign adversaries.

Detailed Location Information Not Included in Notices Submitted to CFIUS

Detailed location information is not always included in notices submitted to CFIUS, which can affect DOD's ability to review transactions for their proximity to critical military locations. Some CFIUS transactions can involve numerous properties or locations, and information on the geographic coordinates of these locations is used by MIBP and the components when determining if there could be national security concerns with a transaction. Specific details on the use of geographic coordinates to identify whether a transaction may pose proximity concerns near critical military locations have been omitted because the information is sensitive.

According to Treasury officials, DOD often requests geographic coordinates once a notice is submitted, and Treasury officials said they have attempted to gather more detailed location information as part of notices. However, officials at one military department said that while there have been improvements in the availability of this information in notices, there are still some companies that do not include the geographic coordinate information. Treasury officials stated that CFIUS has the authority to require this information from companies and has considered revising its regulations to require this information. However, Treasury has not yet done so. Federal internal control standards state that agencies should establish policies and procedures to respond to risk and use quality information to achieve its objectives.[59] Requiring information on geographic coordinates for all target locations in notices submitted to

[59]GAO-14-704G.

CFIUS will improve DOD's ability to more efficiently identify and address proximity concerns with covered transactions.

DOD Has Not Updated Policy to Reflect Changes in Components' Review Responsibilities and Processes

DOD's Instruction identifies CFIUS-related responsibilities and processes for reviewing transactions, but that policy has not been updated to reflect current component reviewer roles and responsibilities or processes for addressing non-notified transactions that may pose national security concerns for the department. The current DOD Instruction was issued in 2010—prior to the transfer of CFIUS responsibilities from the Defense Technology Security Administration to MIBP—but has not been updated to reflect the change. Moreover, the Instruction includes a list of the types of information components should provide to request a non-notified transaction be submitted to CFIUS for further action but has no guidance or expectations for whether or how components should identify and research them. In addition to DOD's Instruction, which is the guiding policy for DOD's CFIUS procedures, in June 2016, MIBP developed an internal process document describing its process for reviewing CFIUS transactions; developing and monitoring mitigation agreements; and identifying and reviewing non-notified transactions. While MIBP officials said the process document is based on the DOD Instruction and is more up-to-date, it is intended to be an internal reference document for MIBP employees and contractors, and it has not been distributed more broadly to the components involved in reviewing transactions for CFIUS.

Moreover, the DOD Instruction does not reflect the department's responsibilities for reviewing transactions. For example, MIBP's internal process document identifies advisory and primary reviewers who are responsible for providing inputs on transactions.[60] However, based on our review of the DOD Instruction, advisory and primary component responsibilities are not differentiated, and several of the advisory reviewers that are identified in MIBP's internal process document are not listed as reviewers in the current Instruction. For example, according to DOD documentation and officials, the Assistant Secretary of Defense for Research and Engineering is an advisory reviewer for CFIUS cases and coordinates input from several other reviewers—including the Defense MicroElectronics Activity and Defense Advanced Research Projects

[60]Advisory reviewers are intended to provide narrowly scoped inputs and expertise about the vulnerabilities of the company being acquired, while primary reviewers are intended to provide broader inputs related to the consequences DOD would face if those vulnerabilities were exploited.

Agency—to determine if a transaction involves a critical technology. However, the Assistant Secretary of Defense for Research and Engineering's responsibilities for coordinating these inputs are not identified in the current DOD Instruction, nor is this office listed as a reviewer.[61] Our review of DOD's Instruction, internal guidance, and other documentation identified several other discrepancies between component responsibilities identified in the Instruction and what is occurring in practice. For example, the Under Secretary of Defense for Personnel and Readiness, among other things, coordinates with OUSD (AT&L) and the Director of Operational Test and Evaluation on the effects of encroachment on DOD test and training areas. While MIBP officials identified the Office of the Under Secretary of Defense for Personnel and Readiness as a CFIUS reviewer, this office is not identified as a reviewer in the DOD Instruction or internal MIBP process document.

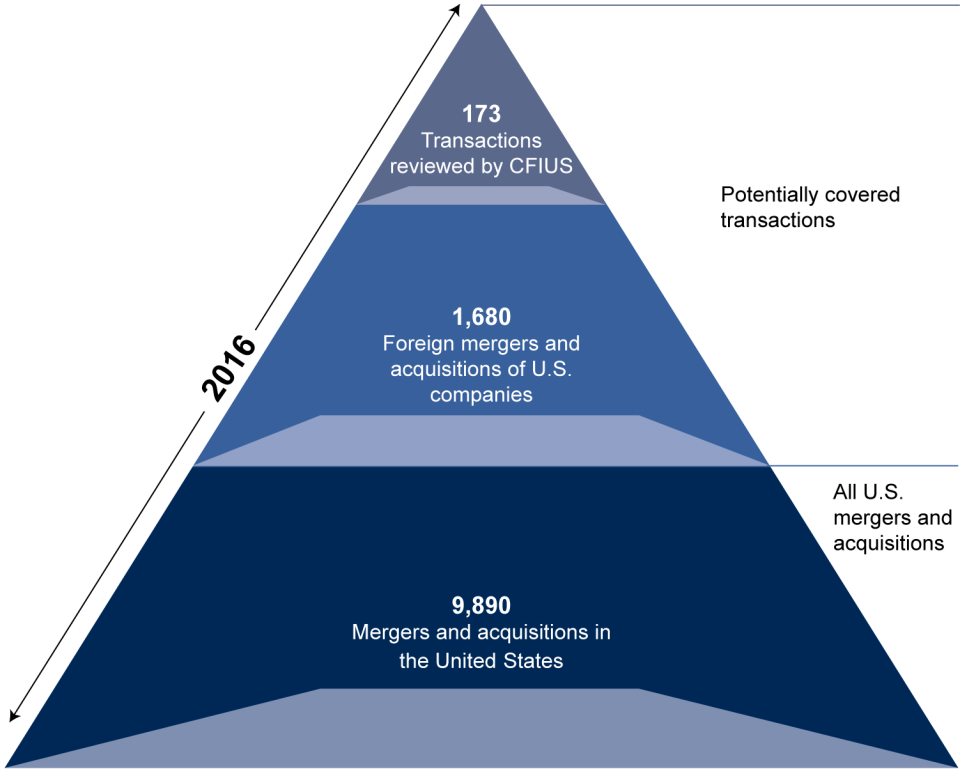
In addition to not having up-to-date information on reviewer roles and responsibilities, the DOD Instruction does not include guidance on how MIBP and the components should identify and research non-notified transactions that may pose national security concerns. As discussed above, because the CFIUS process is based on voluntary notices submitted by parties to transactions, DOD and Treasury officials stated that it is important to monitor foreign acquisitions of U.S. companies that are not filed with CFIUS to determine if any may present national security concerns. As shown in figure 4, there were approximately 1,680 mergers and acquisitions involving foreign acquisitions of U.S. companies in 2016.[62] While not all foreign acquisitions of U.S companies pose national security concerns that would warrant them being reviewed by CFIUS, DOD officials acknowledged challenges with their ability to identify and research these transactions. Specific details on the challenges DOD

[61]According to technical comments provided by MIBP, the Assistant Secretary of Defense for Research and Engineering functions as a primary stakeholder in practice, and the Defense MicroElectronics Activity and Defense Advanced Research Projects Agency also provide their input on CFIUS transactions directly to MIBP.

[62]Our estimated number of mergers and acquisitions and mergers and acquisitions involving foreign acquisitions represents a subset of what would be considered a "transaction" under CFIUS regulations. CFIUS regulations define a transaction as a proposed or completed merger, acquisition, or takeover that includes (a) the acquisition of an ownership interest in an entity; (b) the acquisition or conversion of convertible voting instruments of an entity; (c) the acquisition of proxies from holders of a voting interest in an entity; (d) a merger or consolidation; (e) the formation of a joint venture; or (f) a long-term lease under which a lessee makes substantially all business decisions concerning the operation of a leased entity, as if it were the owner.

faces identifying non-notified transactions have been omitted because the information is considered sensitive.

Figure 4: Mergers and Acquisitions and Foreign Mergers and Acquisitions of U.S. Companies in 2016 in Relation to Transactions Reviewed by the Committee on Foreign Investment in the United States (CFIUS)



Source: GAO analysis of Department of the Treasury and Bloomberg data. | GAO-18-494

Notes: Our estimated number of mergers and acquisitions and mergers and acquisitions involving foreign acquisitions represents a subset of what would be considered a "transaction" under CFIUS regulations. CFIUS regulations define a transaction as a proposed or completed merger, acquisition, or takeover that includes (a) the acquisition of an ownership interest in an entity; (b) the acquisition or conversion of convertible voting instruments of an entity; (c) the acquisition of proxies from holders of a voting interest in an entity; (d) a merger or consolidation; (e) the formation of a joint venture; or (f) a long-term lease under which a lessee makes substantially all business decisions concerning the operation of a leased entity, as if it were the owner.

Data on mergers and acquisitions were pulled from Bloomberg on February 14, 2018.

In addition to challenges identifying non-notified transactions within MIBP, DOD component reviewers' awareness of the non-notified transaction process varied across the components that we spoke with, and participation in this part of the process is ad hoc. For example, five of the

nine components in our sample said they do not have processes in place to identify transactions that have not been voluntarily filed but present risks to national security that could warrant CFIUS review. Officials from four components we spoke with said they have identified non-notified transactions. However, officials from most other DOD components told us they either are not involved or occasionally review non-notified transactions once MIBP identifies them, and they do not proactively perform non-notified transaction research, in part due to resource constraints.

Officials from some components were also uncertain about whether they should elevate some non-notified transactions of concern. For example, DOD's Instruction does not explain when, pursuant to CFIUS regulations, joint ventures are covered transactions. It also does not explain that, even if a non-notified transaction has been completed—meaning a foreign acquirer has already finalized the purchase of a U.S. company—CFIUS can still recommend that the President suspend or prohibit the transaction.[63] Officials from two components said that they are aware of completed joint ventures or other transactions that were of concern but not voluntarily filed, and that they did not elevate them. According to these officials, they assumed the joint ventures would not be covered or that there was nothing CFIUS could do to address their concerns.

In May 2017, the MIBP official responsible for non-notified transactions began a DOD pilot working group for researching non-notified transactions. According to the official, the working group is intended to leverage component reviewer resources and involve them in performing research on non-notified transactions identified by MIBP. However, as of June 2017, participation in the group was limited to 5 of the more than 30 DOD component reviewers, and its processes for reviewing and distributing transactions are still evolving. While this action represents a positive step towards establishing and formalizing efforts to identify non-notified transactions, MIBP officials expressed concern that their ability to identify transactions that may pose risks is not as developed as they would like it to be. Specific details on MIBP's ability to identify

[63]Once a non-notified transaction is filed with CFIUS, it is subject to the same review and investigation as a voluntary notice. If it is determined to be a covered transaction and national security concerns are identified, the parties to the transaction may be subject to mitigation measures; or, if the transaction is elevated to the President it may be prohibited or suspended regardless of whether the transaction has already been completed.

transactions that may pose risks have been omitted because the information is considered sensitive.

In contrast to DOD's limited non-notified guidance, the Department of Homeland Security, another member agency of CFIUS, has guidance for reviewing non-notified transactions in its *Instruction for Department of Homeland Security Participation in the Committee on Foreign Investment in the United States*.[64] According to the Instruction, each week a digest of non-notified transactions is to be sent to Department of Homeland Security components for review, and selected components are required to provide any concerns with the transaction within 7 days. The Department of Homeland Security then determines whether to prepare a non-notified request to forward the transaction on to CFIUS so that the committee can determine whether the transaction merits further action.

Federal internal control standards state that agencies should identify and document agency responsibilities and processes in policy, and periodically review and update policies based on changes.[65] According to MIBP officials, they have been revising DOD's Instruction for over 3 years, and recently began the formal department-wide review process. MIBP officials said they had not released updated guidance to reflect changes in responsibilities and processes sooner because of challenges with employee attrition and leadership changes, which have resulted in multiple rewrites. However, several components we spoke with referenced the need for updated or standardized guidance to inform their CFIUS review responsibilities and the development of their own component-level guidance. It has been over 5 years since MIBP was assigned responsibility for CFIUS, raising questions about the prioritization of CFIUS within the department. Without clear and updated guidance on reviewer responsibilities and established processes and guidance on the identification and review of non-notified transactions, DOD is at risk of inconsistencies in its review of transactions, and it may be unable to address non-notified transactions that pose national security concerns in a timely and efficient manner.

[64]Department of Homeland Security, *Instruction for Department of Homeland Security Participation in the Committee on Foreign Investment in the United States,* (Aug. 4, 2014).

[65]GAO-14-704G.

DOD Faces Several Challenges Developing and Monitoring CFIUS Mitigation Agreements

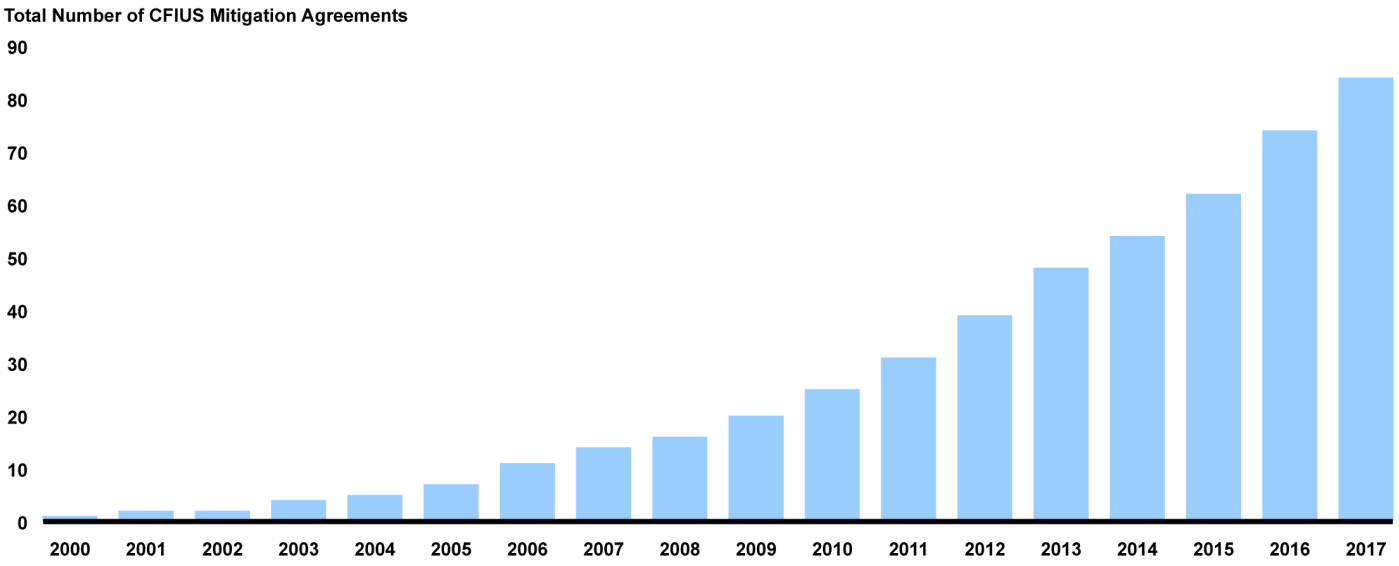
As noted above, mitigation agreements address any threats to national security posed by a transaction. DOD is responsible for most of the CFIUS mitigation agreements, but faces a variety of challenges when taking action to mitigate national security concerns and ensure the effectiveness of the agreements. These challenges relate to insufficient personnel resources compared to MIBP's workload, and unclear communication about the delineation of responsibilities between MIBP and the DOD components. Moreover, DOD has not reported to Congress on its responsibilities for monitoring and enforcing mitigation agreements.

DOD Is Responsible for Most CFIUS Mitigation Agreements

DOD is responsible for more mitigation agreements than other CFIUS member agencies, monitoring 84 of the total of 141 mitigation agreements for CFIUS, or about 60 percent as of the end of calendar year 2017.[66] DOD's responsibility for mitigation agreements more than doubled between 2012 and 2017. Figure 5 shows how DOD's CFIUS mitigation agreement-related responsibilities have increased since 2000.

[66]Some of the mitigation agreements have been terminated. For example, if CFIUS determines that the original national security risk no longer exists, a process is initiated to close out the agreement.

Figure 5: DOD's Mitigation Agreement Responsibilities on the Committee on Foreign Investment in the United States (CFIUS), Calendar Year 2000 to 2017



Source: GAO analysis of Department of Defense (DOD) data. | GAO-18-494

We reviewed Treasury data on transactions from January 2015 through December 2016 to identify the types of national security concerns DOD mitigated through the CFIUS process. We found that the 22 mitigation agreements implemented by DOD during this period included acquisitions of U.S. companies in the aerospace, energy, real estate, and information technology industries, among others. Seventeen of these agreements were implemented to address either supply assurance—DOD's access to certain products or services—or proximity issues.

Based on the Committee on Foreign Investment in the United States Annual Report to Congress for Calendar Year 2015 and our review of DOD documentation, the mitigation measures that have been negotiated and adopted since 2015 may require the parties to the transaction to take actions such as:

- Ensuring that only authorized persons have access to certain technology and information;[67]

[67]According to officials, in one instance, this includes a prohibition on communication with the foreign parent company.

- Appointing a U.S. government approved security officer;
- Providing annual reports and independent audits;
- Notifying security officers or relevant U.S. government parties in advance of foreign national visits to the U.S. business for approval;
- Providing written notification when additional assets are purchased;
- Providing written notification and obtaining CFIUS approval of other parties joining the joint venture;[68] and
- Requiring supply assurance for products or services being provided to the government.

Based on our review of a non-generalizable sample of nine mitigation agreements provided by one of the DOD component reviewers, mitigation agreements typically have more than one measure. For example, there were between 4 and 10 different measures in each agreement we reviewed, and in one agreement, one measure required the submission of more than 100 reports. While some of the mitigation measures require the parties to the agreement to take action and report to DOD, MIBP also monitors and enforces compliance with mitigation measures by conducting on-site compliance reviews and investigations if violations are discovered.

If a company violates a mitigation agreement, CFIUS has the authority to impose penalties, although, according to Treasury and DOD officials, the committee has not taken action to enforce penalties for non-compliance with a mitigation agreement. CFIUS regulations state that any person who intentionally or through gross negligence violates a material provision of a mitigation agreement may be liable for a civil penalty not to exceed $250,000 per violation or the value of the transaction, whichever is greater.[69] DOD officials and the Deputy Assistant Secretary for Investment Security at Treasury stated that the regulatory standard regarding taking action against a company that has violated a mitigation agreement is high. They noted it is difficult to prove that a company violated a mitigation agreement intentionally or through gross negligence, and that the national security effect may exist even if the cause of the

[68]We identified one example of this type of mitigation measure.

[69]31 C.F.R. § 800.801(b).

violation is ordinary negligence.[70] In October 2017, MIBP officials reported six instances since 2013 where companies were not in compliance with their mitigation agreements, but stated that none of these instances were the result of intentional or grossly negligent actions. They told us that DOD has not recommended that CFIUS take action to impose penalties in these cases. In general, according to Treasury and MIBP officials, CFIUS member agencies work with companies to establish a culture of compliance and correct violations of the mitigation agreements as opposed to imposing fines or penalties.

DOD Faces Challenges in Developing and Monitoring CFIUS Mitigation Agreements

MIBP and the DOD components face a variety of challenges, to include developing and monitoring mitigation agreements as a result of limited personnel resources compared to an increasing workload; and communicating about mitigation agreement responsibilities between DOD and the components. Some of the specific details on personnel resource challenges and communication between MIBP and the components have been omitted because the information is sensitive.

In addition to resource challenges within MIBP, resources for mitigation agreement-related activities within the DOD components are also limited and can vary. Officials from at least one component stated that they are not involved in developing or monitoring mitigation agreements because they do not have the resources to do so. Further, citing concerns with DOD's ability to effectively oversee mitigation agreements, officials from three DOD components stated that DOD should recommend prohibiting transactions more often than imposing mitigation agreements. For example, an official from one DOD component with CFIUS responsibilities stated that it is not plausible that these agreements can be properly executed because adversaries have the resources to conceal the fact that they are not complying with the mitigation agreement. Officials from another DOD component also expressed concerns with mitigation agreement enforcement, and stated that they were likely to recommend prohibiting transactions in the future instead of negotiating mitigation agreements in transactions where a national security risk has been identified.

[70]Treasury has drafted supplemental guidance for member agencies on the process and information required to enforce penalties, but the guidance is not yet finalized. Treasury officials said they are also considering revising the CFIUS regulations regarding the assessment of penalties.

A June 2017 DOD report on technology transfer and emerging technology found that given concerns about the cost and effectiveness of mitigation agreements, if the mitigation agreements cannot be simple, CFIUS should recommend that the President suspend or prohibit the transaction. Similarly, officials at the Navy stated that mitigation measures are more effective if they can be fully implemented before the transaction is closed, as opposed to those that require ongoing monitoring. MIBP officials stated that if resource shortfalls continue, they run the risk of having to recommend that the President prohibit transactions because they are unable to implement or monitor additional mitigation agreements.

To bolster available DOD resources for monitoring mitigation agreements, MIBP is in the process of expanding on a case-by-case basis its use of third-party monitors—private auditing and consulting firms approved by DOD and CFIUS but paid for by the foreign acquirer.[71] In these instances, the acquirer is responsible for contracting with qualified third-party independent monitors, which MIBP officials stated they believe could result in cost savings to the government by reducing the resources it uses to respond to routine notifications and requests for approval. MIBP officials stated that this concept would allow MIBP to better extend control over the range of agreements by focusing on monitoring the third-party monitors. However, these officials also acknowledged that the use of third-party monitors can present an inherent conflict of interest by having foreign acquirers funding their own compliance and mitigation agreement monitoring. It is too soon to assess the effect of the expansion of third-party monitoring on improving MIBP's ability to oversee compliance with mitigation agreements.

In addition, we found that MIBP has not clearly communicated expectations and responsibilities for developing and monitoring mitigation agreements to some DOD components. This has led to confusion about what is expected of the components during this part of the process and raised uncertainty within the components we met with about the effectiveness of the mitigation agreements. For example, DOD's Instruction requires components to identify, as applicable, mitigation agreement measures as part of their risk-based analysis and participate in monitoring the mitigation agreements in instances when they have identified a risk. However, officials from several DOD components said

[71]Third-party monitors are companies that are subject matter experts in cyber security, engineering, financial auditing, systems engineering, and legal matters and conduct audits of CFIUS mitigation agreement to monitor company compliance with mitigation measures.

that they either do not include mitigation measures in their risk-based analysis or have been asked not to by MIBP. According to Treasury officials, the CFIUS process has been updated and the proposal of mitigation measures can occur before or during the development of an agency's risk-based analysis, but this information is not reflected in DOD's Instruction, and DOD officials could not identify whether or how this change in process had been communicated to the components.

In addition, officials at one DOD component cited examples of unclear communication regarding their responsibilities for mitigation agreement documentation. For example, these officials told us they requested, but did not receive, documentation from MIBP to ensure compliance with four of the nine mitigation agreements it is responsible for monitoring. According to documentation from this component, it had not received approximately 110 of 133 documents and other reporting requirements that were necessary to determine whether the company was in compliance with the mitigation agreement. According to MIBP officials, they had received the required documentation from the company but did not share it with the component because they were not related to the mitigation agreement measures that the component was responsible for monitoring. As a result of this miscommunication, the component thought that it was responsible for reviewing the missing documentation. MIBP officials stated that they plan to expand and improve their capability to provide DOD components access to the necessary documentation in the future. Officials from MIBP and the component said MIBP currently maintains a shared drive where it stores mitigation agreement documentation, but not all components have access to this documentation.

Additionally, while DOD's Instruction states that DOD components that propose mitigation measures should participate in overseeing those measures, two of the nine components in our sample reported being actively involved in ensuring compliance with mitigation agreements or performing site visits. Two components have allocated several full-time personnel to the task and another has guidance that directs its involvement in CFIUS mitigation agreement monitoring.[72] For example, Navy officials said they have established an office to review transactions

[72]Air Force Instruction 63-141 states that Air Force officials should be involved in monitoring the mitigation agreements that they propose, but Air Force officials said they have not been involved in actively monitoring or performing site visits for any mitigation agreements, in part because they do not have the resources to do so.

that may pose proximity-related risks and monitor proximity-related mitigation agreements, but they have not been given the authority by MIBP to make a final determination regarding whether parties are in compliance with the agreements or to participate in all discussions with the parties. MIBP officials stated that they seek component input on all mitigation agreements, but that MIBP has taken the lead in developing and monitoring DOD mitigation agreements and ensuring compliance because the DOD components have not historically had the resources to dedicate to this responsibility.

DOD's Instruction identifies oversight and communication mechanisms that have not been implemented, but could assist the department in addressing challenges monitoring and ensuring compliance with its CFIUS mitigation agreements. For example, DOD's Instruction establishes a CFIUS Monitoring Committee, made up of relevant DOD component reviewers, to serve as the focal point for DOD monitoring. Among other things, the CFIUS Monitoring Committee was intended to meet quarterly. DOD's Instruction also calls for the development of a DOD CFIUS Strategic Mitigation Plan to include things such as:

- identification of strategic policy for mitigation and monitoring efforts, taking into account resource management and filing trends;
- identification of methods to substantiate and document company compliance with mitigation agreements and maintain records of that compliance; and
- annual analysis of past mitigation in order to determine if past approaches to monitoring and mitigation can be improved.

However, according to MIBP officials, the CFIUS Monitoring Committee and the Strategic Mitigation Plan were not implemented because MIBP did not have the resources to do so. MIBP officials also said they did not see the establishment of the CFIUS Monitoring Committee with relevant DOD components as necessary because MIBP has taken primary responsibility for monitoring mitigation agreements. In addition to not implementing these oversight and communication mechanisms, MIBP has not updated DOD's Instruction to account for policies that are no longer practiced, such as requiring proposed mitigation measures as part of the risk-based analysis, or having components take responsibility for monitoring the mitigation measures they recommend. According to federal internal control standards, to achieve an entity's objectives,

management assigns responsibility and delegates authority to key roles throughout the entity.[73] In addition, management should internally communicate the necessary quality information to achieve the entity's objectives. Updated and improved guidance, including communication about MIBP's management of mitigation agreements and component involvement in developing and monitoring them, could help provide additional oversight of DOD's mitigation agreements and address resource challenges associated with an increasing workload.

DOD Has Not Reported on Review of Mitigation Agreement Monitoring Responsibilities

DOD has not reported its findings to Congress on a review regarding monitoring and enforcing mitigation agreements. A 2013 House Report asked the Secretary of Defense to review the role of the Deputy Assistant Secretary of MIBP in monitoring CFIUS mitigation agreements in which DOD was the lead or co-lead and determine if the Defense Security Service is suited to perform these functions, and report the findings.[74] The House Armed Services Committee noted concerns over whether MIBP, as a policy organization, has the resources and technical expertise to provide reasonable oversight of implementation and compliance with mitigation agreements. The House Report stated that DOD may benefit from leveraging the capabilities of the Defense Security Service, which already reviews every CFIUS filing on behalf of the National Industrial Security Program, and monitors compliance with its own mitigation agreements as part of that program.

DOD was to report on the findings on the review in 2013, but, according to MIBP officials, it has been delayed because disagreement exists within DOD regarding where responsibility for monitoring mitigation agreements should reside. Both MIBP and Defense Security Service officials we spoke with said that their office is the best equipped to perform CFIUS mitigation agreement responsibilities. As a result, formal coordination of the department's response has not been completed. As of January 2018, MIBP officials said that while they recognize the need to complete the response, DOD has not committed to a specific time frame for the response. Reporting the findings to the congressional defense committees will facilitate the identification of current challenges related to CFIUS mitigation agreement oversight, and could address questions

[73]GAO-14-704G.

[74]H.R. Rep. No. 113-102, at 294 (2013).

about the capabilities and responsibilities necessary to effectively monitor and enforce CFIUS mitigation agreements.

Conclusions

Growing foreign direct investment in the United States provides important economic benefits, but can also pose national security risks when that investment comes from potential adversaries. Ensuring that DOD has the resources, processes, and information necessary to perform its responsibilities under CFIUS is essential at a time when the number and complexity of transactions being reviewed by CFIUS has grown significantly. According to officials, the types of investments that pose risks have evolved, making questions about foreign control difficult to determine and mitigate, including investments involving important emerging technologies or real estate purchases in close proximity to sensitive military locations.

In light of these issues, assessing CFIUS resource requirements across the department, completing efforts to identify and communicate critical national security concerns, assessing whether DOD has the necessary authority to address these concerns, and ensuring its policies and practices reflect current DOD component reviewers and processes will be essential to DOD's ability to address the evolving risks it faces from foreign investment. For national security concerns that DOD determines it does not have the authority to address, it may be necessary for DOD to seek legislative action. Further, without updating DOD's CFIUS guidance to reflect current requirements and reporting on reviews requested by a committee of Congress on the department's responsibilities for monitoring mitigation agreements, DOD will likely continue to face challenges facilitating intra-departmental communication and questions about the prioritization of CFIUS within DOD.

Recommendations for Executive Action

We are making a total of eight recommendations: four to the Secretary of Defense, three to the Deputy Assistant Secretary of Defense for MIBP, and one to the Secretary of the Treasury. Specifically:

The Secretary of Defense should assess CFIUS resource requirements within MIBP and DOD component reviewers in light of increasing workload, and prioritize personnel and funding resources accordingly to review, mitigate, and monitor transactions that are of concern to the department. (Recommendation 1)

The Secretary of Defense, in coordination with the Deputy Assistant Secretary of Defense for MIBP and Office of the Under Secretary of Defense, Personnel and Readiness, should incorporate the results of its efforts to identify, assess, and prioritize national security concerns related to foreign investment in emerging technologies and in proximity to certain critical military locations, into DOD Instruction 2000.25 and communicate the results to DOD component reviewers. (Recommendation 2)

Following the completion of its emerging technology study, the Deputy Assistant Secretary of Defense for MIBP should assess what additional authorities may be necessary to address risks related to foreign investment in critical and emerging technologies, and seek legislative action to address risks posed by these investments as appropriate. (Recommendation 3)

Following the department's efforts to identify critical locations and develop and implement guidance assessing risks to these locations from foreign encroachment, the Secretary of Defense should assess what additional authorities, if any, may be necessary to address national security risks from foreign investments in proximity to these locations, and seek legislative action as appropriate. (Recommendation 4)

The Secretary of the Treasury should provide clarification to parties filing a notice of a transaction with CFIUS that for filings involving multiple locations, geographic coordinates are required to be part of the notification. (Recommendation 5)

The Deputy Assistant Secretary of Defense for MIBP should update DOD Instruction 2000.25, to include additional guidance and clarification regarding DOD component responsibilities during the CFIUS process and DOD processes for identifying non-notified transactions. (Recommendation 6)

The Deputy Assistant Secretary of Defense for MIBP should update and implement requirements identified in DOD Instruction 2000.25 regarding management and oversight of mitigation agreements, such as taking into account the resources needed to effectively monitor agreements, improving communication methods between MIBP and the DOD components, and clarifying component responsibilities in developing and monitoring mitigation agreements. (Recommendation 7)

The Secretary of Defense should submit the response to the House Report reviewing the role of the Deputy Assistant Secretary of Defense

for MIBP in monitoring CFIUS mitigation agreements, and determining if the Defense Security Service is suited to perform these functions. (Recommendation 8)

Agency Comments and Our Evaluation

DOD and Treasury provided written comments on a draft of the sensitive report. These comments are reprinted in appendixes IV and V, respectively. We also received technical comments from both agencies, which we incorporated as appropriate. Both departments concurred with our recommendations.

In its written comments, DOD agreed to use a recent assessment of CFIUS resource needs to inform its upcoming budget requests. We acknowledge MIBP's recent efforts to identify and prioritize resource needs in support of its CFIUS responsibilities. As DOD develops its budget request, we encourage the department to consider increases in DOD's CFIUS workload and the resources required to support essential CFIUS functions, like monitoring mitigation agreements and identifying non-notified transactions that may pose national security risks. DOD also agreed to update its guidance related to CFIUS procedures and responsibilities, and complete assessments about additional authorities the department may need to address national security concerns related to foreign investments in U.S. companies developing critical and emerging technologies or in proximity to critical military locations. In its comments, DOD stated it has identified over 40 critical military locations and expects to develop guidance for assessing the risks posed by foreign investments in proximity to these locations. DOD also agreed to complete its response to the House Report reviewing MIBP's role in monitoring CFIUS mitigation agreements. In its comments, DOD stated it is continuing to explore the implementation of third-party monitors as an alternative solution for monitoring CFIUS mitigation agreements.

In its written comments, Treasury concurred with our recommendation to provide clarification that parties filing a notice with CFIUS should include geographic coordinates as part of their notice. Treasury has updated information on its website to clarify that addresses and/or geographic coordinates are required for a CFIUS filing to be considered complete.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, the Deputy Assistant Secretary of Defense for MIBP, and the Secretary of the Treasury. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-4841 or makm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VI.

Marie A. Mak
Director, Contracting and National Security Acquisitions

Appendix I: Department of Defense (DOD) Offices and Organizations with Committee on Foreign Investment in the Unites States (CFIUS) Review Responsibilities

Table 1: DOD Offices and Organizations with CFIUS Review Responsibilities

Under Secretary of Defense for Policy
Director, Defense Technology Security Administration
Deputy Under Secretary of Defense for Policy Integration and Chief of Staff
Deputy Under Secretary of Defense for Strategy, Plans, and Force Development
Assistant Secretary of Defense for International Security Affairs
Assistant Secretary of Defense for Asian Pacific Security Affairs
Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
Deputy Assistant Secretary of Defense for Western Hemisphere Affairs
Assistant Secretary of Defense for Global Strategic Affairs
Under Secretary of Defense for Acquisition, Technology, and Logistics
Director, Defense Advanced Research Projects Agency
Director, Special Programs
Director, Defense Logistics Agency
Director, Missile Defense Agency
Under Secretary of Defense for Intelligence
Director, National Security Agency
Director, Defense Intelligence Agency
Director, National Reconnaissance Office
Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer
Director, Defense Information Systems Agency
General Counsel of DOD
Heads of the DOD Components
Secretaries of the Military Departments[a]
Chairman of the Joint Chiefs of Staff
Commanders of the Combatant Commands[b]

Source: DOD Instruction 2000.25, Procedures for Reviewing and Monitoring Transactions Filed with CFIUS. I GAO-18-494

[a]There are three military departments—the Departments of the Army, Air Force, and Navy. According to Enclosure 7 of DOD 2000.25, the Assistant Secretary of the Army/Acquisition, Logistics, and Technology, Deputy Assistant Secretary of the Air Force, Science, Technology, and Logistics, and the Deputy Assistant Secretary of the Navy/International Programs, perform CFIUS reviewer responsibilities within the military departments.

[b]There are nine geographic or functional combatant commands—U.S. Africa Command, U.S. Central Command, U.S. European Command, U.S. Northern Command, U.S. Pacific Command, U.S. Southern Command, U.S. Special Operations Command, U.S. Strategic Command, and U.S. Transportation Command.

Appendix II: Objectives, Scope and Methodology

This report assesses factors, if any, that affect the Department of Defense's (DOD) ability to (1) identify and address national security concerns through the Committee on Foreign Investment in the United States (CFIUS) process, and (2) develop and monitor mitigation agreements through the CFIUS process.

This report is a public version of a sensitive report that we issued on April 5, 2018.[1] DOD and the Department of the Treasury (Treasury) deemed some of the information in our April report to be sensitive, which must be protected from public disclosure. Therefore, this report omits sensitive information related to (1) DOD's resources to perform certain CFIUS functions, like monitoring mitigation agreements and identifying non-notified transactions; (2) the availability of location information as part of notices that companies file with CFIUS; and (3) the resources and communication required between DOD and the components to develop and monitor mitigation agreements through the CFIUS process. Although the information provided in this report is more limited, this report addresses the same objectives and uses the same methodology as the sensitive report.

To assess what factors, if any, affect DOD's ability to identify and address national security concerns through the CFIUS process, we reviewed relevant documentation, including: CFIUS-related laws and Department of the Treasury (Treasury) regulations; DOD policies and guidance; and DOD and CFIUS internal reports to identify DOD's responsibilities and processes for identifying and addressing national security concerns through the CFIUS process. While there are other authorities, including export controls such as the International Traffic in Arms Regulations and Export Administration Regulations, which in certain circumstances may be used to address national security concerns that arise through foreign investment, our review focused on the DOD's responsibilities addressing national security concerns through the CFIUS process. To assess DOD's efforts to identify and address national security concerns it identified, we gathered and analyzed data on transactions that DOD was responsible for co-leading from January 1, 2012, through December 31, 2017, the most recent data available. To identify resources dedicated to supporting CFIUS activities within the Office of Manufacturing and Industrial Base Policy (MIBP)—the DOD office responsible for coordinating the CFIUS

[1]GAO, *Committee on Foreign Investment in the United States: Action Needed to Address Evolving National Security Concerns Facing the Department of Defense,* GAO-18-261SU (Washington, D.C.: Apr. 5, 2018).

process on behalf of DOD—we analyzed MIBP data from 2012 through 2017 on DOD personnel resources, and reviewed budget amounts from 2012 through 2016 for DOD CFIUS activities from DOD budget documents. To identify the outcomes of transactions not voluntarily filed with CFIUS—known as non-notified transactions—we gathered and analyzed data on the number of non-notified transactions MIBP has identified and researched since the beginning of fiscal year 2016, when they started formally tracking that information. Based on information on the collection and management of Treasury and DOD transaction data, our review of related documentation, and interviews with relevant Treasury and DOD officials, we determined that these data were sufficiently reliable for the purposes of this report. To identify challenges DOD faces addressing certain national security concerns, such as protecting emerging and critical technology and foreign investments in proximity to certain critical military locations, we reviewed a non-generalizable sample of CFIUS case file information for seven transactions. We selected these transactions based on examples identified by DOD components, and the types of national security concerns, including those related to emerging technology and proximity, that DOD officials identified throughout the review. We interviewed officials at Treasury, MIBP, and selected DOD component reviewers to discuss DOD's CFIUS workload and resources.[2] In this report, we define resources as the authorized positions, assigned personnel, personnel performing contract services related to CFIUS functions, and CFIUS-related costs. We also discussed with these officials any limitations to addressing certain national security concerns—like protecting emerging technology and foreign investment in proximity to critical military locations—through CFIUS, and guidance for the CFIUS process and identifying non-notified transactions. Additional information on the DOD components included in this review can be found below.

To identify calendar year 2016 mergers and acquisitions involving U.S. businesses, and the proportion of those mergers and acquisitions involving foreign acquirers, we reviewed data available from the

[2]DOD component reviewers are organizations responsible for reviewing transactions submitted to CFIUS to determine if they pose any national security concerns. DOD components include the Office of the Secretary of Defense, the military departments, the Office of the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General, the Defense Agencies, the DOD Field Activities, and all other organizational entities within DOD. In this report, we also refer to some components more specifically, such as the military departments. For a list of DOD components with CFIUS responsibilities, see app. I.

Bloomberg Terminal, which is a commercial database containing data on mergers and acquisitions. We gathered data on total 2016 mergers and acquisitions involving U.S. companies that were announced, pending, or completed. We also gathered data on 2016 mergers and acquisitions that were announced, pending, or completed involving U.S. companies and foreign acquirers to illustrate the number of potentially covered transactions that may not be voluntarily notified to CFIUS. We assessed the reliability of these data by reviewing relevant documentation and ensuring the data gathered aligned with the search criteria identified. We determined the data were sufficiently reliable for our purposes of displaying total U.S. mergers and acquisitions and the proportion of those transactions that involve foreign acquirers and thus could be potentially covered transactions by CFIUS.

To assess what factors, if any, affect DOD's ability to develop and monitor mitigation agreements through the CFIUS process, we reviewed CFIUS-related laws and regulations and DOD policies and guidance to identify DOD and its component reviewers' responsibilities and processes for developing and monitoring compliance with mitigation agreements. We also reviewed the Committee on Foreign Investment in the United States Annual Report to Congress for Calendar Years 2014 and 2015. To identify actions DOD has taken to mitigate national security concerns, we analyzed data to identify the number of mitigation agreements DOD is responsible for and actions DOD has taken to mitigate and monitor transactions with national security concerns from January 1, 2012 through December 31, 2017, the most recent data available. Based on information on the collection and management of Treasury and DOD CFIUS mitigation agreement data, our review of related documentation, and interviews with relevant Treasury and DOD officials, we determined that these data were sufficiently reliable for the purposes of this report. We also reviewed executive summaries compiled by MIBP of the DOD-co-led transactions with mitigation agreements, as well as selected CFIUS case file documentation for seven transactions. We interviewed officials at Treasury, MIBP, and DOD component reviewers to identify any challenges they face developing and enforcing mitigation agreements. To provide illustrative examples of the types of measures included in CFIUS mitigation agreements, we reviewed all of the active mitigation agreements from one component with responsibilities for monitoring mitigation agreements involving proximity issues. These agreements are not generalizable to other components.

To gather a range of views on issues related to both objectives, we selected a non-generalizable sample of nine DOD component reviewers

responsible for identifying, reviewing, and investigating transactions. These components included officials from: the Departments of the Army, Air Force, and Navy; the DOD Chief Information Officer, the Defense Information Systems Agency; the Defense MicroElectronics Activity; the Defense Advanced Research Projects Agency; the National Security Agency; and the Office of Manufacturing and Industrial Base Policy, Industrial Base Assessments.[3]

Our selection was based primarily on these components' responsibilities for reviewing and investigating transactions for key issues DOD identified as relevant to its review of transactions, including risks related to emerging technology and proximity risks. We also solicited MIBP's recommendations to identify components with varying levels of participation and input into the CFIUS process. We interviewed all nine components and in some cases also received written responses from them to identify similarities and differences in their processes, any challenges they face identifying and addressing national security concerns through CFIUS, and their involvement and any challenges they face developing or monitoring mitigation agreements. Findings based on information collected from the nine components cannot be generalized to all DOD components. In addition to the components included in our sample, we also interviewed and received documentation from other DOD organizations about the CFIUS process. These organizations included officials from: the Defense Innovation Unit Experimental; the Defense Security Service; the Defense Technology Security Administration; the Assistant Secretary of Defense for Research and Engineering; and the Office of the Under Secretary of Defense for Intelligence. We do not include information gathered from these other components in statements based on our non-generalizable sample.

The performance audit upon which this report is based was conducted from January 2017 to April 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with DOD and Treasury from April 2018 to July

[3]MIBP's Global Markets and Investments is the lead DOD CFIUS office. MIBP's Industrial Base Assessments office provides specific input on the effect that a transaction may have on DOD's industrial base.

2018 to prepare this unclassified version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

Appendix III: Factors the Committee on Foreign Investment in the United States Considers to Determine Whether Submitted Transactions Pose a National Security Risk

Table 2: Factors CFIUS Considers to Determine Whether Submitted Transactions Pose a National Security Risk

- The potential effects of the transaction on the domestic production needed for projected national defense requirements
- The potential effects of the transaction on the capability and capacity of domestic industries to meet national defense requirements, including the availability of human resources, products, technology, materials, and other supplies and services
- The potential effects of a foreign person's control of domestic industries and commercial activity on the capability and capacity of the United States to meet the requirements of national security
- The potential effects of the transaction on U.S. international technological leadership in areas affecting U.S. national security
- The potential national security related effects on U.S. critical technologies
- The potential effects on the long-term projection of U.S. requirements for sources of energy and other critical resources and material
- The potential national security related effects of the transaction on U.S. critical infrastructure, including [physical critical infrastructure such as] major energy assets
- The potential effects of the transaction on the sales of military goods, equipment, or technology to countries that present concerns related to terrorism; missile proliferation; chemical, biological, or nuclear weapons proliferation; or regional military threats
- The potential that the transaction presents for transshipment or diversion of technologies with military applications, including the relevant country's export control system
- Whether the transaction could result in the control of a U.S. business by a foreign government or by an entity controlled by or acting on behalf of a foreign government
- The relevant foreign country's record of adherence to nonproliferation control regimes and record of cooperating with U.S. counterterrorism efforts
- Other factors that the President or the committee may determine to be appropriate, generally or in connection with a specific review or investigation

Source: Department of the Treasury: Office of Investment Security Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States, 73 Fed. Reg. 74,567 (Dec. 8, 2008) (detailing the illustrative list of factors in section 721(f) of the Defense Production Act of 1950, as amended. | GAO-18-494

Appendix IV: Comments from the Department of Defense

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION
AND SUSTAINMENT

MAR 15 2018

Ms. Marie A. Mak
Director, Acquisition and Sourcing Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Mak:

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report, GAO-18-261SU, "COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES: Action Needed to Address Evolving National Security Concerns Facing the Department of Defense," dated January 30, 2018 (GAO Code 101443). Detailed comments on the report recommendations are enclosed.

Sincerely,

for Eric D. Chewning
Deputy Assistance Secretary of Defense for
Manufacturing and Industrial Base Policy

Enclosure:
As stated

GAO Draft Report Dated January 30, 2018
GAO-18-261SU (GAO CODE 101443)

"COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES: ACTION NEEDED TO ADDRESS EVOLVING NATIONAL SECURITY CONCERNS FACING THE DEPARTMENT OF DEFENSE"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense assess CFIUS resource requirements within MIBP and DoD component reviewers in light of increasing workload, and prioritize personnel and funding resources accordingly to review, mitigate, and monitor transactions that are of concern to the department.

DoD RESPONSE: Concur. MIBP conducted an assessment of resource needs as part of the program objective memorandum issue paper process for fiscal year 2019. MIBP anticipates that the assessment will serve as the baseline for implementing this recommendation.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense, in coordination with the Deputy Assistant Secretary of Defense for MIBP and Office of the Under Secretary of Defense, Personnel and Readiness, incorporate the results of the its efforts to identify, assess, and prioritize national security concerns related to foreign investment in emerging technologies and in proximity to certain critical military locations, into DoD Instruction 2000.25 and communication the results to DoD component reviewers.

DoD RESPONSE: Concur. DoD is in the process of updating DoD Instruction 2000.25, incorporating clearer and more robust procedures throughout the lifecycle of Committee on Foreign Investment in the United States (CFIUS) cases.

RECOMMENDATION 3: The GAO recommends that, following the completion of the emerging technology study, the Deputy Assistant Secretary of Defense for MIBP should assess what additional authorities may be necessary to address risk related to foreign investment in critical and emerging technologies and seek legislative action to address risks posed by these investments as appropriate.

DoD RESPONSE: Concur.

RECOMMENDATION 4: The GAO recommends that following the departments' efforts to identify critical locations and develop and implement guidance assessing the risks to these locations from foreign encroachment, the Secretary of Defense assess what additional authorities, if any, may be necessary to address national security risks from foreign investments in proximity to these locations, and seek legislative action as appropriate.

DoD RESPONSE: Concur. DoD has identified over 40 mission essential locations and expects to develop guidance on assessing the risk posed by foreign land access in proximity to these locations.

RECOMMENDATION 5: The GAO recommends that the Secretary of the Treasury should provide clarification to the parties filing a notice of a transaction with CFIUS that for filings involving multiple locations, geographic coordinates are required to be part of the notification.

DoD RESPONSE: Concur. DoD looks forward to working with the Chairperson of CFIUS to implement this recommendation and to incorporate the geographic coordinate data as part of CFIUS case reviews.

RECOMMENDATION 6: The GAO recommends that the Deputy Assistant Secretary of Defense for MIBP update DoD Instruction 2000.25, to include additional guidance and clarification regarding DoD component responsibilities during the CFIUS process and DoD processes for identifying non-notified transactions.

DoD RESPONSE: Concur. DoD is in the process of updating DoD Instruction 2000.25 with new procedures for handling non-notified transactions.

RECOMMENDATION 7: The GAO recommends that the Deputy Assistant Secretary of Defense for MIBP update and implement the requirements identified in DoD Instruction 2000.25 regarding management an oversight of mitigation agreements, such as taking into account the resources needed to effectively monitor agreements, improving communication methods between MIBP and the DoD components, and clarifying component responsibilities in developing and monitoring mitigation agreements.

DoD RESPONSE: Concur. DoD is in the process of updating DoD Instruction 2000.25 with new procedures for the management and oversight of CFIUS mitigation agreements to which DoD is a party.

RECOMMENDATION 8: The GAO recommends that the Secretary of Defense submit the response to the House Report reviewing the role of the Deputy Assistant Secretary of Defense for MIBP in monitoring CFIUS mitigation agreements, and determining if the Defense Security Service is suited to perform these functions.

DoD RESPONSE: Concur. In light of the changing foreign investment, DoD has given careful consideration to the implementation of third-party monitors as an fiscally responsible, scalable, and effective alternative solution for monitoring CFIUS mitigation agreements. The number of mitigation agreements that require monitoring increases each year, and the resources necessary to monitor them increases proportionally. Rather than asking the U.S. taxpayer to bear these increasing costs, DoD is exploring how to shift the burden to the foreign acquirers. We could accomplish that shift by requiring the parties to employ company-compensated, trusted third-party monitors with specific expertise in the necessary mitigation fields. This arrangement would lead to a net increase in government revenue by reducing government overhead associated with long-term compliance monitoring.

Appendix V: Comments from the Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

MAR 07 2018

Marie A. Mak
Director, Acquisition and Sourcing Management
U.S. Government Accountability Office
441 G St. N.W.
Washington, DC 20548

Dear Ms. Mak:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report entitled *Committee on Foreign Investment in the United States: Action Needed to Address Evolving National Security Concerns Facing the Department of Defense* (GAO-18-261).

The Department of the Treasury (Treasury), as the chair of the Committee on Foreign Investment in the United States (CFIUS), appreciates the work conducted by the Government Accountability Office (GAO) over the past year. Treasury concurs with GAO's recommendation that Treasury should clarify to parties filing notices with CFIUS that geographic coordinates are required as part of the notice. As such, Treasury updated the frequently asked questions regarding CFIUS on our website to clarify that addresses and geographic coordinates are required in order for a filing to be complete.

Enclosed with this letter are our technical comments on the draft report. If you have any questions, please contact Brian Reissaus at (202) 622-0182.

Sincerely,

Aimen N. Mir
Deputy Assistant Secretary
Investment Security

Enclosure:
As stated

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Marie A. Mak, 202-512-4841 or MakM@gao.gov

Staff Acknowledgments

In addition to the contact names above, W. William Russell (Assistant Director), Katherine Trimble (Assistant Director), Meghan Perez (Analyst-in-Charge), and Heather B. Miller were principal contributors to this report. In addition, the following people made contributions to this report: Justin Fisher, Stephanie Gustafson, Kate Lenane, Alyssa Weir, and Robin Wilson.