



April 2024

# FOREIGN INVESTMENT IN THE U.S.

## Efforts to Mitigate National Security Risks Can Be Strengthened

# GAO Highlights

Highlights of [GAO-24-107358](#), a report to congressional requesters

## Why GAO Did This Study

The U.S. is historically the world's largest recipient of foreign investment. This benefits the U.S. economy but can also present national security risks. CFIUS is an interagency committee authorized to review certain transactions involving foreign investment in the U.S. to identify risks to national security. To mitigate such risks, CFIUS has authority to enter into legal agreements with the companies involved and to monitor compliance with the agreements. Treasury serves as the committee's chair.

GAO was asked to review issues related to CFIUS mitigation agreements. This report (1) describes trends in mitigation agreements from 2000 through 2022, (2) evaluates selected CFIUS member agencies' approaches to monitoring and enforcing compliance with mitigation agreements and reviewing them for continued relevance, and (3) assesses the selected agencies' staffing for monitoring and enforcement. GAO selected five member agencies on the basis of the number of mitigation agreements each agency manages. GAO reviewed laws, regulations, and agency guidance. GAO also conducted a nongeneralizable review of mitigation agreements and interviewed agency officials. This is a public version of a sensitive report GAO issued in January 2024. Information Treasury identified as sensitive has been omitted.

## What GAO Recommends

GAO is making five recommendations to Treasury to help enhance CFIUS's capacity to monitor and enforce compliance with mitigation agreements. Treasury agreed with the recommendations.

View [GAO-24-107358](#). For more information, contact Kimberly Gianopoulos at (202) 512-8612 or [GianopoulosK@gao.gov](mailto:GianopoulosK@gao.gov).

April 2024

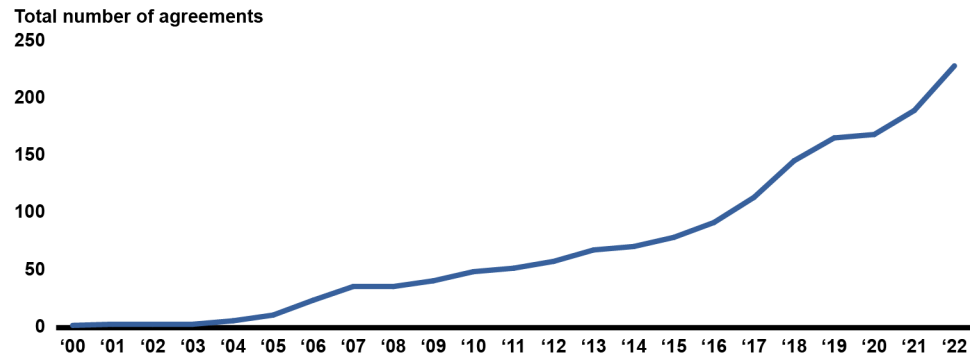
# FOREIGN INVESTMENT IN THE U.S.

## Efforts to Mitigate National Security Risks Can Be Strengthened

### What GAO Found

The Committee on Foreign Investment in the United States (CFIUS) enters into agreements that require companies to mitigate national security risks stemming from foreign investment. Since 2000, the number of mitigation agreements has grown steadily, rising roughly fourfold in the last decade. The Departments of Defense and the Treasury manage the largest numbers of mitigation agreements. To mitigate risks—such as foreign investors' accessing certain sensitive data—CFIUS imposes various measures. For example, CFIUS might require the U.S. company to establish access controls for certain information systems.

Number of Active CFIUS Mitigation Agreements, by Calendar Year, 2000–2022



Source: GAO analysis of Department of the Treasury data on the Committee on Foreign Investment in the United States (CFIUS). | [GAO-24-107358](#)

Note: "Mitigation agreements" includes agreements listed in notes to fig. 4, [GAO-24-107358](#).

Selected CFIUS member agencies monitor compliance with mitigation agreements by, among other things, conducting site visits to companies and working with independent auditors and monitors. If a company violates an agreement, CFIUS can take enforcement action, including imposing monetary penalties. The Department of the Treasury, as the committee's chair, issued public guidelines on CFIUS penalties in 2022. But CFIUS does not yet have a documented committee-wide process for deciding on enforcement actions, which has led to challenges in responding to certain violations, according to officials. CFIUS also does not have a documented committee-wide process for reviewing agreements for continued relevance. Documenting such processes would help ensure CFIUS member agencies respond in a timely manner to violations and can focus their resources on mitigation agreements that remain relevant.

Over the last decade, selected CFIUS member agencies have expanded staffing to monitor and enforce compliance with the rising number of mitigation agreements. Treasury plans to expand its monitoring capacity by approximately doubling its staff. But Treasury has not documented its objectives for this increase, which it based on an estimate rather than an assessment of its needs. Documenting these objectives would allow Treasury to assess whether the increased staffing enables it to meet them. Further, officials of other selected member agencies said their staffing levels affect their monitoring, and CFIUS has not previously coordinated on staffing. Regular staffing coordination would help ensure CFIUS member agencies can effectively monitor and enforce compliance.

---

# Contents

---

---

Letter		1
	Background	4
	Mitigation Agreements Nearly Quadrupled in Last Decade, Monitored Primarily by Two Agencies	12
	CFIUS Is Developing Guidance for Monitoring Compliance but Does Not Have Documented Processes for Enforcing and Reviewing Agreements	15
	Opportunities Exist to Better Support CFIUS Staffing for Monitoring and Enforcement	27
	Conclusions	35
	Recommendations for Executive Action	36
	Agency Comments	37
Appendix I	Objectives, Scope, and Methodology	39
Appendix II	Comments from the Department of the Treasury	42
Appendix III	GAO Contact and Staff Acknowledgments	44
Figures		
	Figure 1: Members of the Committee on Foreign Investment in the United States	6
	Figure 2: Committee on Foreign Investment in the United States (CFIUS) General Transaction Review Process	8
	Figure 3: Examples of National Security Risks Addressed by CFIUS Mitigation Agreements	11
	Figure 4: Number of Active CFIUS Mitigation Agreements, Including New and Continuing Agreements, Dec. 2000– Dec. 2022	13
	Figure 5: Examples of CFIUS Monitoring Agency Techniques for Monitoring Mitigation Agreements	16
	Figure 6: Total Number of Staff at Five Selected CFIUS Agencies Who Dedicated at Least Half of Their Time to Monitoring and Enforcing Compliance with Mitigation Agreements, Fiscal Years 2013–2022	28

---

---

## Abbreviations

CFIUS	Committee on Foreign Investment in the United States
CMA	CFIUS monitoring agency
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
DOE	Department of Energy
FIRRMA	Foreign Investment Risk Review Modernization Act of 2018
FTE	full-time equivalent

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



April 18, 2024

The Honorable John Cornyn  
Ranking Member  
Subcommittee on International Trade, Customs,  
and Global Competitiveness  
Committee on Finance  
United States Senate

The Honorable Robert P. Casey, Jr.  
Committee on Finance  
United States Senate

The United States is the world's largest recipient of foreign investment—more than \$5 trillion in 2022, according to the Bureau of Economic Analysis. Foreign investment benefits the U.S. economy and helps create jobs, but it can also pose national security risks. The interagency Committee on Foreign Investment in the United States (CFIUS) is authorized to review certain transactions involving foreign investment in the United States, as well as certain real estate transactions by foreign persons, to determine the transactions' effect on U.S. national security.

When CFIUS determines that a transaction poses a risk to national security—for example, if the transaction gives the foreign investor access to certain sensitive data or technology—CFIUS has authority to negotiate an agreement and impose conditions to mitigate the risk. (This report generally refers to both agreements and conditions as mitigation agreements.<sup>1</sup>) CFIUS member agencies then monitor and enforce compliance with the agreement by the parties involved in the transaction.<sup>2</sup>

However, trends in the number and complexity of foreign investment transactions filed with CFIUS have raised questions about its ability to effectively monitor and enforce transaction parties' compliance with mitigation agreements. We reported in 2018 that trends in the volume and complexity of foreign investment transactions filed with CFIUS, together

---

<sup>1</sup>See 50 U.S.C. § 4565(l)(3). CFIUS refers to its actions under this authority variously as mitigation agreements, national security agreements, letters of assurance, orders, and conditions. For purposes of this report, we generally refer to these collectively as mitigation agreements.

<sup>2</sup>CFIUS members include the heads of the Departments of the Treasury (chair), Commerce, Defense, Energy, Homeland Security, Justice, and State and the Offices of Science & Technology Policy and the U.S. Trade Representative.

---

with staffing constraints, may have limited CFIUS members' ability to monitor compliance with mitigation agreements.<sup>3</sup> In its most recent public report, CFIUS acknowledged that the transactions it reviews are increasingly complex and result in more mitigation agreements to address the national security risks it identifies.<sup>4</sup>

You asked us to review issues related to CFIUS mitigation agreements. This report (1) describes trends in mitigation agreements from 2000 through 2022, (2) evaluates selected CFIUS member agencies' approaches to monitoring and enforcing compliance with mitigation agreements and reviewing them for continued relevance, and (3) assesses the selected agencies' staffing for monitoring and enforcement. This report is one in a series related to CFIUS processes for reviewing foreign investments.<sup>5</sup>

This report is a public version of a sensitive report that we issued on January 22, 2024.<sup>6</sup> This public version of that report addresses the same objectives and uses the same methodology. However, this report omits certain information that Treasury identified as sensitive, requiring protection from public disclosure. Specifically, this report omits

---

<sup>3</sup>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).

<sup>4</sup>Department of the Treasury, *Committee on Foreign Investment in the United States. Annual Report to Congress. Report Period: CY 2022*.

<sup>5</sup>We have published five related reviews of, respectively, (1) the Department of Agriculture's efforts to share data on foreign investments in agricultural land with CFIUS; (2) CFIUS processes related to selected real estate transactions; (3) the Department of Defense's (DOD) ability, as a CFIUS member, to address defense issues; (4) CFIUS processes for reviewing covered transactions and workload challenges; and (5) DOD's ability to identify whether foreign encroachment threatens certain defense facilities. See GAO, *Foreign Investments in U.S. Agricultural Land: Enhancing Efforts to Collect, Track, and Share Key Information Could Better Identify National Security Risks*, [GAO-24-106337](#) (Washington, D.C.: Jan. 18, 2024); *Committee on Foreign Investment in the United States: Selected Transactions Involving Real Estate May Share Certain National Security Risks, but Dispositions Can Vary Due to Case-Specific Factors*, [GAO-19-417C](#) (Washington, D.C.: June 14, 2019); *Committee on Foreign Investment in the United States: Action Needed to Address Evolving National Security Concerns Facing the Department of Defense*, [GAO-18-494](#) (Washington, D.C.: July 10, 2018); *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); *Defense Infrastructure: Risk Assessment Needed to Identify If Foreign Encroachment Threatens Test and Training Ranges*, [GAO-15-149](#) (Washington, D.C.: Dec. 16, 2014).

<sup>6</sup>GAO, *Foreign Investment in the U.S.: Efforts to Mitigate National Security Risks Can Be Strengthened*, [GAO-24-106259SU](#) (Washington, D.C.: Jan. 22, 2024).

---

information related to, in the first objective, characteristics of mitigation agreements that were active in 2023, including the country and the type of national security risk; in the second objective, Treasury's internal guidance and processes for enforcement of mitigation agreements; and in the third objective, the number of selected agencies' staff who monitor and enforce mitigation agreements.

To address our reporting objectives, we reviewed relevant laws, executive orders, and regulations. In addition, to describe trends in mitigation agreements, we analyzed Treasury data on those that were active or terminated between 2000 and 2022. To determine the reliability of the data, we reviewed the data for errors and inconsistencies, interviewed agency officials about the data, and reviewed trends in the data with them. We determined that the data were sufficiently reliable to assess trends in mitigation agreements since 2000.

To evaluate selected agencies' approaches to monitoring and enforcing compliance with mitigation agreements and reviewing them for continued relevance, we selected five CFIUS member agencies—Treasury and the Departments of Defense (DOD), Energy (DOE), Homeland Security (DHS), and Justice (DOJ)—on the basis of the number of mitigation agreements each was managing as of March 2023.<sup>7</sup> We reviewed internal guidance documents and interviewed officials of each of the selected agencies. We also assessed agency processes against internal control principles related to responding to risks and implementing control activities<sup>8</sup> and against leading practices for interagency collaboration.<sup>9</sup> In addition, we selected and reviewed a nongeneralizable sample of 19 mitigation agreements to understand and illustrate how the selected CFIUS agencies monitor and enforce compliance.

To assess the selected agencies' staffing for monitoring and enforcement, we obtained staffing estimates for fiscal years 2013 through 2022. To determine the reliability of the data, we reviewed the data for errors and inconsistencies and interviewed agency officials. We determined that the data were sufficiently reliable for assessing the agencies' staffing for

---

<sup>7</sup>We have omitted the number of mitigation agreements each agency manages, because Treasury identified that information as sensitive.

<sup>8</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

<sup>9</sup>GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, [GAO-23-105520](#) (Washington, D.C.: May 24, 2023).

---

monitoring and enforcement. We assessed agency staffing processes against internal control principles related to defining objectives and establishing the organizational structure to achieve objectives;<sup>10</sup> against federal guidance on workforce planning;<sup>11</sup> and against leading practices for interagency collaboration.<sup>12</sup> Appendix I provides more information about our scope and methodology.

The performance audit on which this report is based was conducted from September 2022 to January 2024 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 Treasury, from February to April 2024, to prepare this version of the original sensitive report for public release. This public version was also prepared in accordance with generally accepted government auditing standards.

---

## Background

### CFIUS Overview

CFIUS is an interagency committee authorized by law to review and address national security risks arising from certain transactions involving foreign investment in the United States. CFIUS reviews notifications of foreign investments, which are submitted on a largely voluntary basis, to evaluate whether those transactions pose a threat to national security. Transactions within CFIUS's jurisdiction, generally referred to as "covered" transactions, include certain mergers, acquisitions, or takeovers by or with a foreign person that could result in foreign control of a U.S. business; certain noncontrolling but generally nonpassive investments by some foreign persons in certain types of U.S. businesses; and certain real estate transactions in the United States by foreign persons.

CFIUS's work on specific transactions generally includes

- 1) reviewing transaction notices submitted to the committee and taking action as necessary to address any national security risk,

---

<sup>10</sup>[GAO-14-704G](#).

<sup>11</sup>Office of Personnel Management, *Workforce Planning Guide* (November 2022).

<sup>12</sup>[GAO-23-105520](#).



- 
- 2) monitoring and enforcing compliance with mitigation agreements, and
  - 3) identifying transactions of concern for which no notice was submitted.

CFIUS legal authorities have evolved over time.<sup>13</sup> The most recent significant statutory update to CFIUS authority occurred in 2018 with the enactment of the Foreign Investment Risk Review Modernization Act (FIRRMA).<sup>14</sup> FIRRMA expanded CFIUS's jurisdiction regarding certain noncontrolling investments and real estate transactions by or with a foreign person and updated its review process, among other changes.<sup>15</sup> FIRRMA also required CFIUS to develop compliance plans that detail how the committee will monitor and enforce compliance with mitigation agreements that are entered into for covered transactions.<sup>16</sup>

The Secretary of the Treasury serves as CFIUS's chair. The committee includes eight other agencies as voting members and two agencies as nonvoting, ex officio members (see fig. 1). CFIUS invites other federal government agencies to participate in the CFIUS process as needed for individual transactions.

---

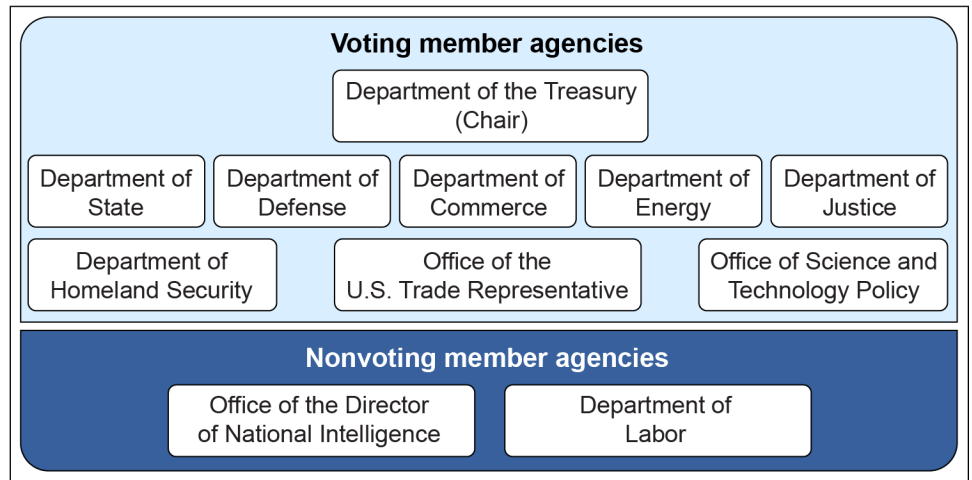
<sup>13</sup>CFIUS was established by Executive Order in 1975 to monitor the effect of, and to coordinate U.S. policy on, foreign investment in the United States. Exec. Order No. 11,858, 40 Fed. Reg. 20,263 (May 7, 1975). In 1988, Congress enacted the Exon-Florio amendment adding section 721 to the Defense Production Act of 1950, which authorized the President or the President's designee 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. Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, § 5021, 102 Stat. 1425 (Aug. 23, 1988). The President delegated this investigative authority to CFIUS. Exec. Order No. 12,661, 54 Fed. Reg. 779 (Dec. 27, 1988). The Foreign Investment and National Security Act of 2007 (FINSA) further amended section 721 and formally established CFIUS in statute. Pub. L. No. 110-49, § 3, 121 Stat. 246, 252 (July 26, 2007) (codified as amended at 50 U.S.C. § 4565).

<sup>14</sup>John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, §§ 1701-1728, 132 Stat. 1636, 2173-2208 (Aug. 13, 2018) (codified as amended at 50 U.S.C. § 4565).

<sup>15</sup>See Pub. L. No. 115-232, § 1703. A foreign investment is considered noncontrolling if it does not convey controlling equity interest to the foreign investor. For additional information on covered investments, see 31 C.F.R. §§ 800.211 and 800.303.

<sup>16</sup>See Pub. L. No. 115-232, § 1718. Compliance plans require the inclusion of certain elements. See 50 U.S.C. § 4565(l)(6)(C).

**Figure 1: Members of the Committee on Foreign Investment in the United States**



Source: GAO analysis of agency documents. | GAO-24-107358

The Secretary of the Treasury has certain operational responsibilities as the chair of CFIUS. According to Treasury officials, these include coordinating the committee’s operations, facilitating collection of information from parties involved in a transaction (such as a foreign acquirer and U.S. business involved in a transaction), reviewing and circulating information about covered transactions with member agencies, and managing the transaction review process in accordance with statutory time frames. Treasury also communicates with transaction parties, members of Congress, and the public on CFIUS’s behalf.

## CFIUS Process for Reviewing Transactions

In general, parties to a foreign investment transaction jointly and voluntarily file a notice of the transaction with CFIUS, which CFIUS then reviews in accordance with specific statutory processes and timelines.<sup>17</sup> Notices to CFIUS should contain applicable information about the nature of the transaction and the parties involved. Under FIRRMA, certain transactions are subject to mandatory filing, such as those involving critical technologies.<sup>18</sup> In general, any CFIUS member agency can initiate a review of any covered transaction for which no notice was filed if the

<sup>17</sup>50 U.S.C. § 4565(b)(1)(C) (implemented in regulations at 31 C.F.R. §§ 800.501, et seq., and 802.501, et seq.). Parties may also provide a short-form declaration as an alternative to CFIUS’s traditional voluntary notice. See 50 U.S.C. § 4565(b)(1)(C)(v).

<sup>18</sup>See Pub. L. No. 115-232, § 1706.

---

agency determines that the transaction is within CFIUS's jurisdiction and that it may raise national security concerns.<sup>19</sup>

During its initial review—known as a national security review—CFIUS determines whether the transaction is covered by its legal authorities and therefore is within its jurisdiction. CFIUS also assesses whether the transaction poses risks to national security. The committee generally also identifies at least one other agency with relevant expertise to work with Treasury to guide the transaction through the CFIUS process. If CFIUS finds that the covered transaction does not present national security risks or that other provisions of law provide adequate and appropriate authority to address the risks, CFIUS may end its review. However, if the potential national security risks are unresolved at the end of the review period, or if the committee requires additional time, CFIUS may proceed to a national security investigation. If the investigation identifies an unresolved national security risk, CFIUS may work with the transaction parties as appropriate to mitigate the potential risk.

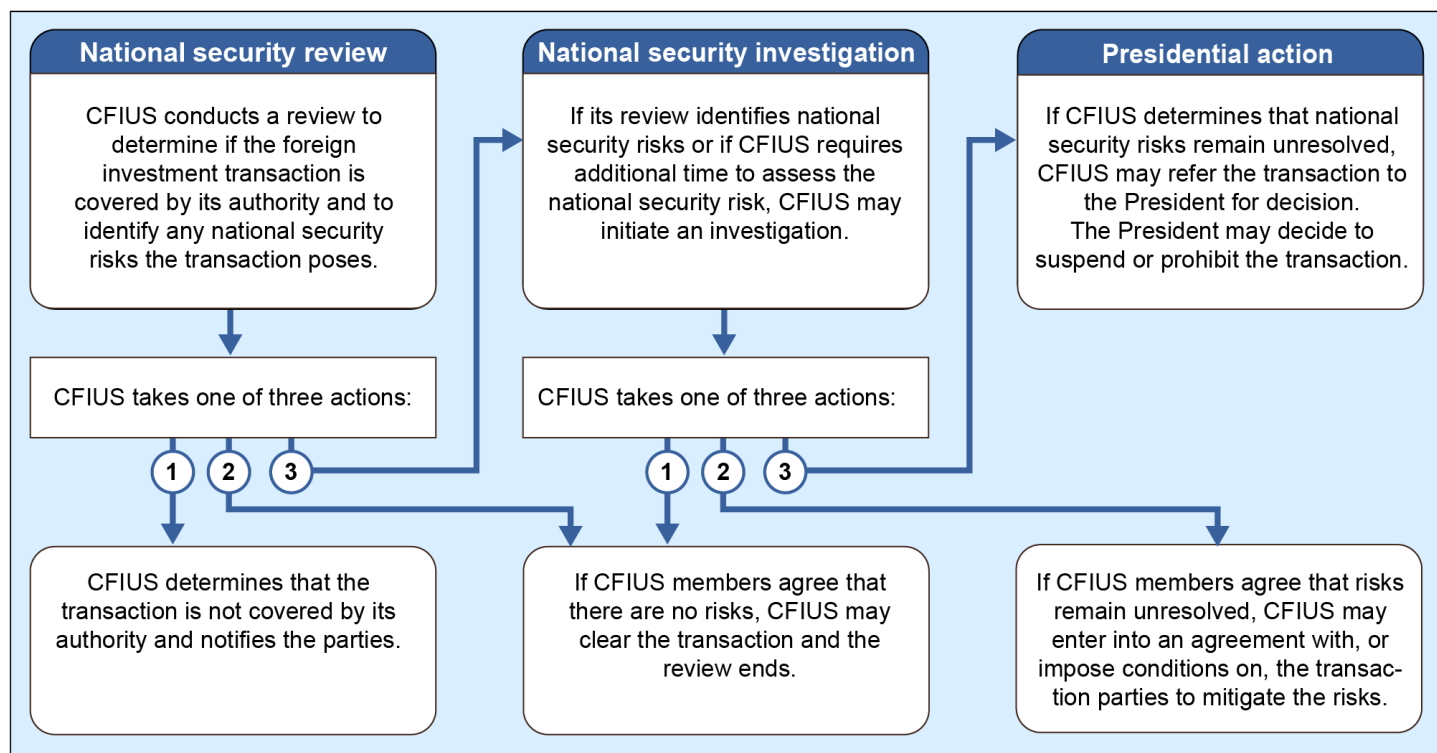
CFIUS clears a transaction and ends its review or investigation if it has determined that (1) the transaction does not pose any unresolved national security risks, (2) any national security risks are adequately addressed by other laws, or (3) mitigation measures that CFIUS agreed to or imposed resolve any national security risks. However, if any national security risks remain unresolved after an investigation, CFIUS may refer the transaction to the President for action unless the transaction parties decide to withdraw the filing and abandon the transaction. The President has the authority to suspend or prohibit a transaction, including by requiring that

---

<sup>19</sup>CFIUS refers to these as non-notified transactions. According to its annual report to Congress for 2022, CFIUS identified and formally considered 84 non-notified transactions, 11 of which resulted in a request to the parties to file the transaction with CFIUS. The annual report notes that these numbers exclude transactions for which the parties voluntarily filed with CFIUS upon being contacted and also exclude transactions that CFIUS preliminarily considered as potential non-notified transactions. The report states that non-notified transactions are among the most complicated that CFIUS considers and often require mitigation measures to address national security risks.

the foreign party divest itself from the U.S. entity.<sup>20</sup> See figure 2 for an overview of CFIUS’s transaction review process.

**Figure 2: Committee on Foreign Investment in the United States (CFIUS) General Transaction Review Process**



Source: GAO analysis of Treasury documents and 50 U.S.C. § 4565. | GAO-24-107358

Note: The parties to a foreign investment transaction may choose to withdraw the transaction notice it filed with CFIUS and abandon the transaction at any point during the review process.

<sup>20</sup>Congress directed that this authority can be invoked only when, in the President’s judgment, no law other than section 721 of the Defense Production Act of 1950, as amended, 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 person acquiring an interest might take action that threatens to impair the national security. See 50 U.S.C. § 4565(d)(4). According to CFIUS, a foreign acquirer may agree to divest itself of all or part of a U.S. company in lieu of a referral to the President. Divestment typically occurs through the parties’ withdrawing the notice and abandoning the transaction.

---

## CFIUS Authority to Enter into Agreements and Impose Conditions

CFIUS may enter into agreements with, or impose conditions on, transaction parties to address national security risks that its reviews and investigations identify. By law, CFIUS must base these agreements and conditions on its analysis of the transaction's effects on national security and, in general, must determine that the agreement or condition effectively mitigates the national security risk posed by the transaction. CFIUS must also take into consideration whether the agreement is reasonably calculated to be effective, verifiable, and monitorable over the long term.

The CFIUS statute, as amended by FIRRMA, describes three scenarios in which CFIUS can use its mitigation authority<sup>21</sup>:

- CFIUS can negotiate an agreement with parties to mitigate the national security risks posed by a transaction and, once the risks are resolved, can clear the transaction.
- CFIUS can impose conditions on parties to a completed transaction to mitigate any interim risks until CFIUS concludes its review of the transaction or, as appropriate, the President determines to suspend or prohibit the transaction.
- CFIUS can enter into an agreement or impose conditions to facilitate the voluntary withdrawal and abandonment of a transaction.<sup>22</sup>

Of CFIUS's nine members, Treasury, DOD, DOE, DHS, and DOJ monitor and enforce most mitigation agreements. Agency officials attributed this to the departments' substantive expertise in the areas that the mitigation agreements cover. As CFIUS's chair, Treasury is responsible for designating one or more member agencies to lead the review of the transaction, including, where appropriate, discussions with the transaction parties about potential mitigation. Once a mitigation agreement is signed, Treasury designates one or more agencies to be responsible for monitoring and enforcing compliance with its terms.<sup>23</sup>

CFIUS members refer to the lead agencies designated to monitor and enforce compliance with mitigation agreements as CFIUS monitoring agencies (CMA). CFIUS members distinguish between the "lead CMA" and "co-lead CMA" when more than one member is responsible for a

---

<sup>21</sup>See 50 U.S.C. § 4565(l)(3)(A).

<sup>22</sup>Transaction parties may abandon a transaction for commercial reasons or because they do not accept the mitigation measures CFIUS proposes.

<sup>23</sup>See 50 U.S.C. § 4565(k)(5).

---

mitigation agreement. Although both the lead CMA and co-lead CMA have responsibility to monitor and enforce compliance, the lead CMA is generally the primary point of contact for the transaction parties and coordinates monitoring activities.

For most mitigation agreements, Treasury is generally a co-lead CMA and another agency serves as the lead CMA. In 2019, Treasury began serving as a co-lead CMA for all new mitigation agreements in order to, according to Treasury officials, enable it as chair to more effectively oversee and coordinate the monitoring and enforcement of mitigation agreements.<sup>24</sup>

---

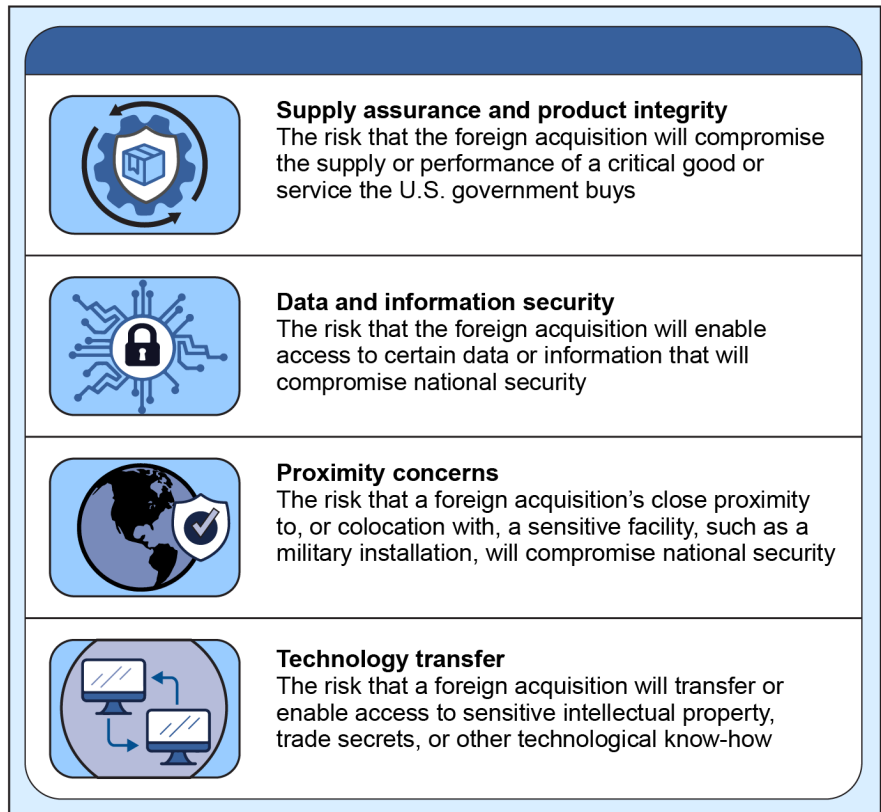
## National Security Risks Addressed by Mitigation Agreements

CFIUS may enter into mitigation agreements to address a range of national security risks. These risks broadly encompass issues related to supply assurance and product integrity, data and information security, proximity concerns, and technology transfer. Figure 3 shows examples of risks that CFIUS mitigation agreements address.

---

<sup>24</sup>Pursuant to the CFIUS regulations implementing FIRRMA and other statutory authorities, Treasury designates itself as a co-lead agency for the assessment, review, investigation, negotiation, or monitoring of a mitigation agreement or order. See 31 C.F.R. §§ 800.230, 802.225.

**Figure 3: Examples of National Security Risks Addressed by CFIUS Mitigation Agreements**



Source: Committee on Foreign Investment in the United States (CFIUS) documents (data); GAO (icons). | GAO-24-107358

To address national security risks, agreements can require the transaction parties to implement various mitigation measures. According to CFIUS's annual report to Congress for 2022, mitigation measures can include:

- requiring assurances of continuity of supply to the U.S. government for defined periods as well as notification and consultation prior to taking certain business decisions;
- requiring implementation of security protocols to ensure the integrity of products or software sold to the U.S. government;
- ensuring that only authorized persons have access to certain technology, systems, facilities, or sensitive information;

- 
- ensuring that certain facilities, equipment, and operations are located only in the United States;
  - prohibiting or limiting the transfer or sharing of certain intellectual property, trade secrets, or technical information; and
  - excluding certain sensitive U.S. assets from the transaction.<sup>25</sup>

According to officials, CFIUS mitigation agreements generally do not contain an end date. However, the law requires Treasury and the lead CMA to periodically review each mitigation agreement with respect to its continued appropriateness and to terminate, phase out, or amend the agreement if a threat no longer requires mitigation.<sup>26</sup>

---

## Mitigation Agreements Nearly Quadrupled in Last Decade, Monitored Primarily by Two Agencies

Number of Agreements Rose from 2000 through 2022, Quadrupling after 2012

From December 2000 through December 2022, the cumulative total number of active mitigation agreements increased significantly, from about five to almost 230. From December 2012 through December 2022, the number of active mitigation agreements roughly quadrupled as continuing mitigation agreements accumulated and new ones were signed (see fig. 4). For the purpose of this analysis, active mitigation

---

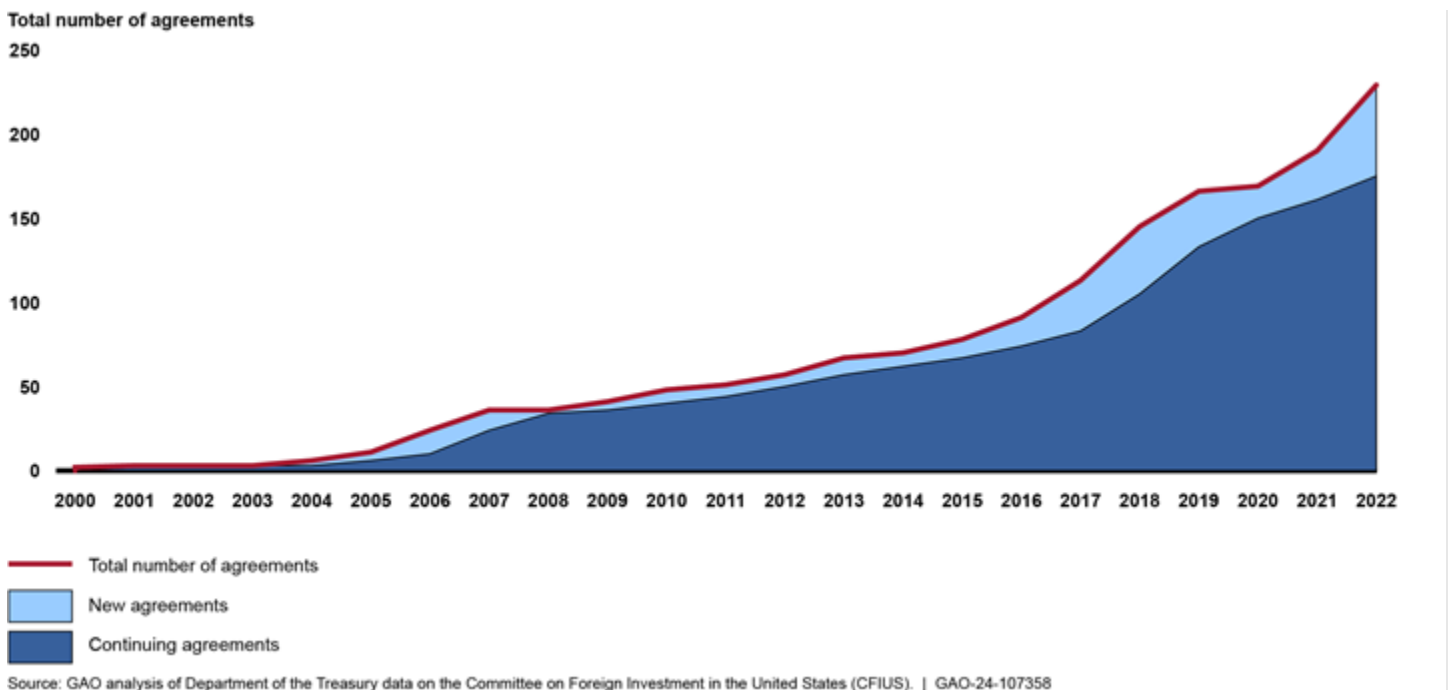
<sup>25</sup>Department of the Treasury, *Committee on Foreign Investment in the United States. Annual Report to Congress. Report Period: CY 2022.*

<sup>26</sup>50 U.S.C. § 4565(l)(3)(B).



agreements include those for transactions CFIUS has cleared as well as certain transactions it has not cleared.<sup>27</sup>

**Figure 4: Number of Active CFIUS Mitigation Agreements, Including New and Continuing Agreements, Dec. 2000–Dec. 2022**



Note: For the purpose of our analysis, “mitigation agreements” includes CFIUS agreements, national security agreements, letters of assurance, orders, and CFIUS-imposed conditions on withdrawn notices and abandoned transactions.

The data shown reflect the number of active mitigation agreements at the end of each calendar year—that is, the sum of any new mitigation agreements (i.e., signed that year) and continuing mitigation agreements (i.e., active at the end of the prior year) minus those terminated during the year.

<sup>27</sup>Transactions not cleared include those that are subject to interim orders as well as certain transactions for which the parties withdrew their notice to CFIUS and abandoned the transaction. CFIUS may impose conditions or enter into an agreement with the parties to an abandoned transaction and may monitor their compliance. For example, according to CFIUS’s 2022 Annual Report to Congress, CFIUS imposed conditions in 2022 on the withdrawal of five of the 87 notices that were withdrawn after CFIUS commenced a national security investigation. CFIUS adopted mitigation agreements for three other withdrawal and abandonments. See Department of the Treasury, *Committee on Foreign Investment in the United States. Annual Report to Congress. Report Period: CY 2022*. According to Treasury officials, most mitigation agreements for transactions that CFIUS has not cleared have a defined end (such as the date of full abandonment of the transaction) or otherwise entail less ongoing monitoring than mitigation agreements for cleared transactions. Transactions that were abandoned but did not have CFIUS-imposed conditions subject to ongoing monitoring are not counted in the data on active mitigation agreements that we reviewed.

---

Our analysis of Treasury data found that the number of mitigation agreements began to grow after remaining largely static from 2000 to 2003, as figure 4 shows. According to Treasury officials, increases in the number of mitigation agreements after 2007 reflect in part the Foreign Investment and National Security Act of 2007's establishment of CFIUS's authority to include mitigation of national security risks arising from covered transactions.<sup>28</sup>

According to Treasury officials, the increased number of active mitigation agreements since 2015 reflects growth in the number of transaction notices filed. Specifically:

- Trends in the number of notices of mergers and acquisitions in strategic sectors—for example, a growing number of notices of foreign investments in firms related to supply chain issues—contributed to growth in the number of transaction notices filed, according to officials.
- FIRRMA's expansion of CFIUS's jurisdiction—including its establishment of CFIUS's authority to review potential national security concerns related to noncontrolling investments as well as real estate transactions—contributed to growth in the number of notices filed after FIRRMA took full effect in 2020, according to officials.<sup>29</sup>

---

## DOD and Treasury Monitor and Enforce the Largest Numbers of Active Agreements

At the end of 2022, DOD was a lead or co-lead CMA for the largest number of active mitigation agreements and Treasury was a lead or co-lead CMA for the second largest number of mitigation agreements. The relative shares of mitigation agreements for which DOD, Treasury, and the other selected agencies—DOE, DHS, and DOJ—were serving as a

---

<sup>28</sup>See Pub. L. No. 110-49, § 5. CFIUS's original authority—established by the 1988 Exon-Florio amendment that added section 721 to the Defense Production Act of 1950—did not include mitigation authority, according to Treasury officials. Consequently, according to the officials, CFIUS previously entered into mitigation agreements based on the government's overall authority to enter into contracts.

<sup>29</sup>We have omitted information, as well as a related graphic, about the countries and national security risks associated with current active mitigation agreements, because Treasury identified that information as sensitive.

---

lead or co-lead CMA at the end of each year evolved from December 2000 to December 2022.<sup>30</sup>

According to Treasury officials, changes in the relative number of mitigation agreements for which certain agencies served as lead or co-lead CMA reflect the evolving nature of foreign investment trends. In addition, officials said that the increased number of mitigation agreements for which DOD has served as a lead or co-lead CMA reflects an increased number of mitigation agreements to address risks to supply assurance, which our analysis showed constituted almost half of the mitigation agreements it was monitoring at the end of 2022. Treasury officials attributed the recent increase in the number of mitigation agreements for which Treasury is a lead or co-lead CMA primarily to its decision to serve as a co-lead CMA on all new mitigation agreements after April 2019.<sup>31</sup>

---

## CFIUS Is Developing Guidance for Monitoring Compliance but Does Not Have Documented Processes for Enforcing and Reviewing Agreements

---

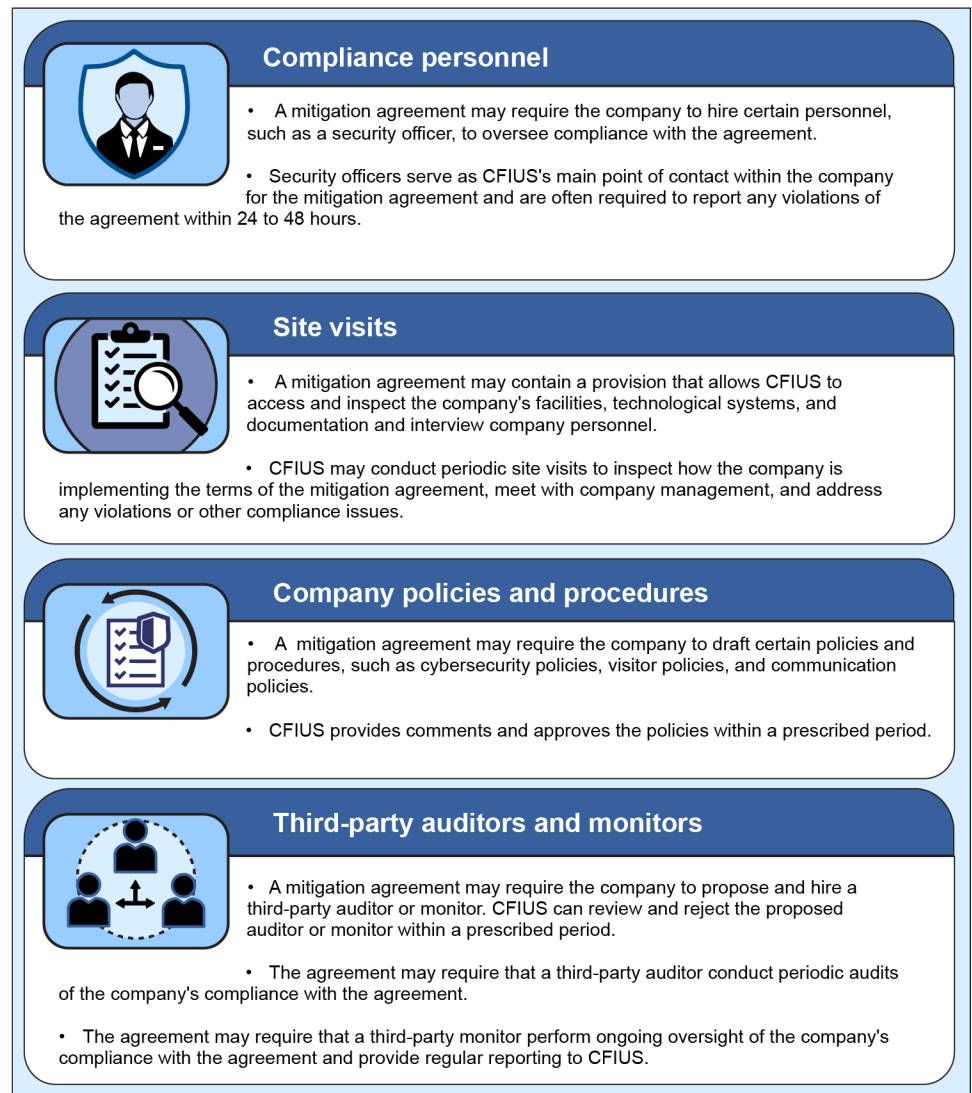
<sup>30</sup>We have omitted information, as well as a related graphic, about the number of active mitigation agreements for which each selected agency served as a lead or co-lead CMA, because Treasury identified that information as sensitive.

<sup>31</sup>According to Treasury officials, before it determined to serve as co-lead CMA on all new mitigation agreements, Treasury had a minor role in monitoring compliance because it often did not have the substantive expertise or the necessary resources to actively participate in monitoring.

## CMA Use Various Techniques to Monitor Compliance with Mitigation Agreements

CMA use multiple techniques to monitor transaction parties' compliance with mitigation agreements. Our review of selected agencies' procedures found that their primary monitoring techniques include requiring companies to hire compliance personnel such as security officers; conducting site visits; requiring companies to develop certain policies and procedures; and working with third-party entities such as monitors and auditors (see fig. 5).

**Figure 5: Examples of CFIUS Monitoring Agency Techniques for Monitoring Mitigation Agreements**



Source: GAO analysis of CFIUS documents and interviews with agency officials (data); GAO (icons). | GAO-24-107358

---

## Compliance Personnel

According to internal Treasury guidance, mitigation agreements often require the company to nominate and appoint personnel to oversee its compliance with the mitigation agreement and to report any instances of noncompliance or suspected noncompliance to the CMAs. The appointed personnel may include security officers, who are responsible for ensuring routine compliance with the mitigation agreement, such as the implementation of any required policies and procedures. Appointed personnel may also include security directors, who sit on the company's board of directors and ensure that the company's strategic decisions are consistent with the mitigation agreement. Treasury officials said that mitigation agreements typically include a timeline for the U.S. business to identify and nominate candidates for these positions. According to the officials, the CMAs are responsible for interviewing and approving the nominated candidates before they are appointed.

Our nongeneralizable review of 19 mitigation agreements found that 17 included a provision requiring the company to hire personnel who could meet specific criteria.<sup>32</sup> For example, one mitigation agreement required the company to nominate a candidate for security officer, subject to the CMAs' approval, within 14 days of the mitigation agreement's effective date. The mitigation agreement specified that the candidate should be a resident, non-dual-national U.S. citizen and eligible for a Secret-level security clearance. According to Treasury officials, the specific qualifications for a security officer vary depending on the individual transaction.

## Site Visits

Mitigation agreements generally include a provision giving the CMAs the authority to access and inspect company facilities, review records and systems, and interview personnel. Our nongeneralizable review of 19 mitigation agreements found that 16 contained a provision for U.S. government access and inspection. CMAs may use this authority to conduct periodic in-person or virtual site visits to the company at their discretion. According to agency officials, because site visits can be time intensive, CMAs prioritize them according to the type of security risk identified in the mitigation agreement, the complexity of the mitigation agreement, and the company's compliance history, among other factors.

---

<sup>32</sup>Because our review of the mitigation agreements was not generalizable, the characteristics we observed may not reflect those of other mitigation agreements. Treasury officials emphasized that each mitigation agreement is tailored to address the transaction's unique circumstances and stated that CMAs take varied approaches to monitor and enforce mitigation agreements.

---

According to internal Treasury guidance, before conducting a site visit, the CMAs coordinate with the company and develop an agenda for the visit. During a site visit, the CMAs may inspect facilities and review records and systems for compliance with the mitigation agreement; meet with company management and, when applicable, the security officer and the security director; interview selected nonmanagement personnel; and follow up on any previously identified compliance issues. Representatives of the third-party monitor and auditor also may participate, when applicable, in the site visit. In addition, CMA officials said they often bring subject matter experts from their own agencies—for example, Navy engineers, Army chemists, or Department of Energy (DOE) physicists—to ensure they can assess any technical aspects of the company’s compliance with the mitigation agreement. After a site visit, the CMAs document the visit and provide any relevant feedback to the company, including requiring additional actions to address findings from the visit. For example, documentation from one site visit shows that the CMAs instructed the company to update a required policy and training on the basis of findings from the visit.

#### Company Policies and Procedures

Mitigation agreements can require a company to develop policies and procedures—related, for example, to cybersecurity, communications, or physical security—that are subject to CMA approval. CMAs might request changes to policies during their reviews, which the company must address within a timeframe specified in the mitigation agreement, if applicable.

Our nongeneralizable review of 19 mitigation agreements found that 11 required the company to develop and implement specific policies or procedures. For example, to restrict the U.S. company’s information sharing with the foreign acquirer, one mitigation agreement required the U.S. company to develop a communications policy governing the type of information that could be shared. To restrict a foreign parent company’s access to certain protected data, another mitigation agreement required the parties to develop a security plan to safeguard company systems that contained protected data.

#### Third-Party Auditors and Monitors

The mitigation agreement may require the company to hire a third-party auditor or monitor to support the CMAs’ compliance monitoring. According to Treasury’s internal guidance, third-party auditors conduct audits to determine whether the parties have complied with the mitigation agreement during a defined period. In contrast, third-party monitors work with the parties on an ongoing basis to ensure compliance and provide reporting to the CMAs. According to Treasury officials, the government is

---

not responsible for the costs associated with third-party auditors or monitors, because the contract for third-party services is between the company and the third-party entity. The CMAs can review nominees' qualifications, approve or reject nominees, and provide input on audit and monitoring plans required under the mitigation agreement.

Our nongeneralizable review of 19 mitigation agreements found that eight required the company to hire one or more third-party entities. For example, one mitigation agreement required the company to hire a third-party auditor to conduct an initial audit of compliance with the agreement and also provided the CMAs with discretion to require subsequent annual audits. Another mitigation agreement, which required the company to replace certain software, also required it to hire a third-party monitor to conduct on-site reviews of the replacement process and report periodically to the CMAs. According to Treasury officials, companies can also benefit from third-party monitors' expertise in compliance.

---

### CMAs Have Taken Steps to Document Their Monitoring Procedures, and Treasury Is Developing Committee-Wide Guidance

CMAs have taken steps to document their respective monitoring procedures, including developing compliance plans, and Treasury officials reported that they are working to develop committee-wide guidance that harmonizes the CMAs' approaches. All five of the agencies we selected for our review have developed or are developing documentation, such as guidance, checklists, and interview questions, for various internal procedures that they use to monitor compliance with mitigation agreements. For example:

- Treasury has internal guidance for selecting third-party monitors, reviewing third-party audit reports, and reviewing company policies, such as policies on physical security, information security, and background screening.
- DOD has internal guidance for planning and implementing site visits, including checklists to use during the visits.
- DOE has a script for its officials' use when interviewing security officer candidates.
- DHS has internal guidance for periodically reassessing its mitigation agreements for possible termination.
- DOJ is developing internal guidance for training staff to monitor compliance with mitigation agreements, according to officials.

Officials from the five agencies also described taking steps to meet the FIRRMA requirement that CFIUS develop mitigation agreement

---

compliance plans as appropriate.<sup>33</sup> The law requires the committee or CMAs to formulate, adhere to, and keep updated a plan for monitoring compliance with each mitigation agreement.<sup>34</sup> The plan should identify the committee member with primary responsibility for the mitigation agreement as well as how and with what frequency that member will monitor compliance, whether a third-party entity will be used, and what actions will be taken if the transaction parties fail to cooperate with efforts to monitor compliance with the mitigation agreement.<sup>35</sup>

The officials we interviewed reported various approaches to developing compliance plans. For example, Treasury officials said they maintain a tracker with summary details about each mitigation agreement, including the CMAs, type of risk, and mitigation measures and monitoring techniques that apply to each mitigation agreement. DOD also maintains a tracker that identifies details such as CMAs and type of risk. DOE officials said they develop a detailed plan for each mitigation agreement, identifying the CMAs, describing measures contained in the mitigation agreement, documenting monitoring activities, and listing dates when certain deliverables are due to the CMAs. DHS officials said that they do not develop a specific plan but that the measures in the mitigation agreements, together with existing internal guidance and procedures, meet the compliance plan requirement. DOJ officials said they understood that Treasury maintains compliance plans for the committee and that CMAs generally develop their own guidance for monitoring compliance with mitigation agreements.

Treasury officials said that CMAs generally develop their own internal guidance on monitoring but share best practices with each other. For example, according to DOD officials, Treasury convened a workshop with other CMAs in 2023 to discuss best practices for monitoring compliance with mitigation agreements. DOD officials said that in the workshop, they shared DOD's site visit procedures and checklists with CMAs and Treasury shared its procedures for conducting interviews with company employees during site visits.

According to Treasury officials, Treasury is working with other CMAs to harmonize monitoring approaches by developing committee-wide

---

<sup>33</sup>See Pub. L. No. 115-232, § 1718.

<sup>34</sup>See 50 U.S.C. § 4565(l)(6)(C)(i).

<sup>35</sup>See 50 U.S.C. § 4565(l)(6)(C)(ii).



---

guidance.<sup>36</sup> Treasury officials told us they are currently working on committee-wide guidance related to site visits and the use of third-party entities to monitor compliance with mitigation agreements. The officials also said they plan to develop and propose committee-wide guidance for other monitoring procedures. In addition, the officials said they have worked with committee members to establish standard wording to use in mitigation agreements, such as wording for provisions requiring a company to hire a security officer to ensure routine compliance.

---

## CFIUS Can Take Enforcement Actions to Address Violations

CMAAs, and CFIUS as a committee, have the authority to take enforcement actions to address noncompliance with the terms of mitigation agreements.<sup>37</sup> Treasury officials said that violations of mitigation agreements occur but are usually minor. According to the officials, violations typically occur during the initial implementation of a new mitigation agreement, when the parties are developing policies and procedures and incorporating them into their business processes. CMAAs may use techniques such as site visits and required and voluntary company reporting to identify suspected violations.

CMAAs may take action to determine whether a violation has occurred and, if it has, gauge the severity of the violation, relying on information from the transaction parties, third-party entities, and other U.S. government sources, among others. At any point during this process, the CMAAs may issue a letter to the transaction parties, documenting the facts and circumstances of the potential violation and indicating whether the CMAAs intend to pursue additional inquiry and possible enforcement.<sup>38</sup>

If CFIUS identifies a violation, it has the authority to take enforcement action by establishing remediation plans and imposing monetary

---

<sup>36</sup>Treasury officials said they are developing a mitigation database to manage information, including transaction information from the original case; the parties' deliverables and their due dates; identities of third-party monitors and auditors; reports and other documents, such as site visit records; interview notes; points of contact; compliance incidents; and enforcement actions. Officials said the database will be available to other CMAAs to use and is built on the larger Case Management System through which parties file transaction notices and declarations to CFIUS. Treasury officials anticipate the mitigation database will be operational by the end of 2023.

<sup>37</sup>See 50 U.S.C. § 4565(l)(6)(D).

<sup>38</sup>We have omitted the number of letters CMAAs issued in response to potential violations, because Treasury identified that information as sensitive.

---

penalties.<sup>39</sup> Treasury officials said that the CMAs responsible for a mitigation agreement are authorized to assess the severity of any violation and to develop and implement remediation plans; however, all CFIUS members must reach consensus to impose penalties when appropriate. In 2022, Treasury posted enforcement and penalty guidelines online. The guidelines describe factors CFIUS weighs in determining whether a penalty is warranted and the scope of the penalty and also describe the process CFIUS follows in imposing penalties.<sup>40</sup> Treasury officials said the guidelines serve to increase public awareness of how CFIUS approaches potential enforcement actions and determines the amount of penalties.

Violations may range from minor or technical noncompliance, such as a missed reporting deadline, to serious violations that could impair national security, such as the release of sensitive or protected data, according to Treasury officials. The officials said that tracking the number of violations across all mitigation agreements has been challenging because of the range in violations' severity, variation in CMAs' recordkeeping practices, and difficulty of counting violations. For example, according to the officials, a company may self-report a single violation that the ensuing investigation determines to constitute multiple violations or no violation. Treasury officials said they are developing a proposal to standardize how CMAs track and report violations. According to Treasury officials, the majority of violations to date have been minor or technical in nature.

**Remediation plans.** CMAs often coordinate with parties to develop remediation plans that establish measures to prevent recurrence of violations, particularly minor or technical ones, according to agency officials. For example, DOE officials said they had established remediation plans requiring additional company training and internal controls to address violations of a mitigation agreement that were unintentional in nature but nonetheless concerning.

Treasury officials told us that after a violation is identified, remediation is generally the first step to address any potential national security risks

---

<sup>39</sup>See 50 U.S.C. § 4565(l)(6)(D). Additionally, CFIUS can unilaterally review a transaction again if it determines there is no other appropriate enforcement mechanism to address a violation of a mitigation agreement or condition. See 50 U.S.C. § 4565(b)(1)(D)(iii). The second review could result in a different disposition of the transaction than resulted from the initial review.

<sup>40</sup>Department of the Treasury, "CFIUS Enforcement and Penalty Guidelines," accessed October 18, 2023, <https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-enforcement-and-penalty-guidelines>.

---

arising from the violation, even if the CMAs are considering whether to pursue further formal enforcement action such as a monetary penalty. According to officials, if the violation is time sensitive, the CMAs develop a remediation plan as soon as possible to address any immediate national security risks. For example, DOD officials told us that after they were notified of a serious violation, they worked with the company to engage a third-party auditor to assess the violation's scope. The officials said they also asked the company to preserve records related to the incident while DOD and other CMAs explored further enforcement action.

Treasury officials said that CMAs exercise their judgment to determine how best to remediate a violation and whether further action is appropriate. For example, if the company self-reports a violation, cooperates fully in remediating the risk, and has committed few or minor violations in the context of the mitigation agreement's full scope, the CMAs may be more likely to address the violation through a remediation plan or a letter outlining the facts of the violation and informing the company that it may be subject to future enforcement action. On the other hand, if the company is uncooperative and has committed numerous or significant violations of the mitigation agreement, the CMAs may be more likely to pursue a committee-wide enforcement action such as a penalty, according to Treasury officials.<sup>41</sup>

**Monetary penalties.** For more serious violations, CFIUS has imposed monetary penalties, subject to approval by the full committee. As a general matter, penalties may not exceed \$250,000 per violation or the transaction's value, whichever is greater, and are based on the nature of the violation.<sup>42</sup>

The CFIUS enforcement and penalty guidelines describe factors that the committee considers when determining whether to pursue a penalty and, if so, the amount of the penalty. These factors include whether the violation could harm national security and whether the company disclosed the violation in a timely manner and cooperated with CMA efforts to investigate and remediate it. According to the guidelines, CFIUS also considers whether the penalty holds the company accountable for its conduct and incentivizes future compliance.

---

<sup>41</sup>The committee's published enforcement and penalty guidelines provide additional detail regarding the relevant aggravating and mitigating factors it considers.

<sup>42</sup>31 C.F.R. §§ 800.901 and 802.901.

---

Internal Treasury guidance describes the process Treasury follows with CMAs and other committee members to justify and agree on penalty actions.<sup>43</sup> If committee members reach consensus on a proposed penalty, CFIUS notifies the company. The company can then petition CFIUS to reconsider the penalty.

As of October 2023, CFIUS had publicly reported two penalties for violations of mitigation measures:<sup>44</sup>

- In 2018, CFIUS imposed a \$1 million penalty for repeated breaches of a 2016 mitigation agreement, including failure to establish required security policies and failure to provide adequate reports to the committee.
- In 2019, CFIUS imposed a \$750,000 penalty for violations of a 2018 interim order, including failure to restrict and adequately monitor access to protected data.

In June 2023, Treasury officials told us that CFIUS had imposed additional penalties during 2023 but had not yet reported them publicly. The officials also said that CFIUS was considering other enforcement actions, including penalties, that it had not yet finalized.

---

### Officials Reported Challenges Reaching Consensus on Enforcement Actions because CFIUS Does Not Have a Documented Process

CMA officials reported challenges to reaching consensus among committee members and finalizing certain enforcement actions. Officials attributed these challenges to the lack of a documented committee-wide process. Officials also noted that these challenges strained agency resources and delayed enforcement action in response to violations.

Although Treasury officials described a process for making CFIUS enforcement decisions, including those involving penalties, the CFIUS enforcement and penalty guidelines do not document this process. For example, the guidelines do not explain the steps in the process, including steps that members should take to resolve disagreements. The guidelines also do not define a timeframe for each step or identify agencies' officials who must concur on an enforcement action. Treasury officials said that because each enforcement action is context specific, they cannot provide

---

<sup>43</sup>We have omitted further details of this process because Treasury identified that information as sensitive.

<sup>44</sup>Treasury may publish on its website certain information related to specific enforcement actions, consistent with statutory confidentiality requirements. See 50 U.S.C. § 4565(c). Treasury officials said they may delay public reporting to maintain the confidentiality of the transaction and the parties.

---

criteria for when enforcement is required. However, Treasury officials agreed that the decision-making process should be clarified. Moreover, officials of other member agencies told us that they would like to participate in documenting a committee-wide process.

The CFIUS enforcement guidelines underscore the committee's recent focus on enforcement. Treasury, as chair of CFIUS, is responsible for coordinating committee decisions on enforcement actions, and its strategic plan identifies timely remediation and appropriate enforcement of apparent breaches of mitigation agreements as a measure of its success.<sup>45</sup> In addition, *Standards for Internal Control in the Federal Government* calls for management to respond to risks related to achieving its objectives and to document its internal controls.<sup>46</sup> Further, leading practices for interagency collaboration state that collaborating agencies should work together to agree on their respective roles and responsibilities and a process for making decisions, and should develop written guidance.<sup>47</sup>

Working with the other member agencies to document a committee-wide process for CFIUS enforcement decisions would strengthen Treasury's ability, as chair, to ensure the committee's timely response to violations that may threaten national security. Even if CFIUS declines to pursue enforcement, a documented process would clarify the steps for reaching that consensus and help avoid the diversion of agency resources in protracted negotiations.

---

### Officials Reported the Process for Reviewing Agreements for Continued Relevance Is Unclear because CFIUS Does Not Have a Documented Process

Treasury and the lead CMA are required to review mitigation agreements for continued relevance, but CMA officials told us the process is unclear because CFIUS lacks a documented process. Specifically, CMA officials said it is not clear what evidence is required to justify terminating a mitigation agreement or how to resolve interagency disagreements about termination decisions. Partly as a result, according to the officials, termination requests typically take many months to address and can burden staff.

Treasury has developed internal guidance that describes its own procedures for reviewing termination requests and notifying the rest of the committee about its reviews. According to Treasury's internal guidance,

---

<sup>45</sup>Department of the Treasury, *Treasury: Strategic Plan 2022-2026*.

<sup>46</sup>[GAO-14-704G](#).

<sup>47</sup>[GAO-23-105520](#).

---

CMAAs may consider terminating a mitigation agreement if a change in circumstances warrants such action. For example, CMAAs may consider termination if the foreign acquirer sells its interest in the U.S. company or if the U.S. company ceases production of a technology that was covered or protected under the mitigation agreement.<sup>48</sup> DOD officials said that if a particular DOD program office no longer uses a product covered by a mitigation agreement addressing supply assurance, they may consider terminating the mitigation agreement. CMAAs may also consider amending mitigation agreements. For example, DHS officials said they decided to amend a mitigation agreement containing a sunset clause and to renew mitigation measures pertaining to certain risks that still concerned them.

However, Treasury has not worked with the other member agencies to develop committee-wide guidance for conducting periodic reviews of mitigation agreements and for evaluating proposals to terminate, phase out, or amend mitigation agreements, according to Treasury officials. Treasury officials said they had started drafting guidance on termination for the committee's input and that they encourage CMAAs to conduct periodic reviews of mitigation agreements. However, no specific frequency or criteria for these reviews has been established, according to officials of one CMA.

Treasury and the lead CMA are responsible for periodically reviewing the continued relevance of each mitigation agreement and for terminating, phasing out, or amending it if the threat it addresses no longer requires mitigation.<sup>49</sup> According to Treasury's internal guidance, reviewing mitigation agreements for potential termination or amendment is both legally required and important for the efficient use of CFIUS resources. *Standards for Internal Control in the Federal Government* states that management should document its internal controls.<sup>50</sup> Further, leading practices for interagency collaboration state that collaborating agencies should work together to agree on their respective roles and

---

<sup>48</sup>For example, one mitigation agreement we reviewed was a result of CFIUS's review of a change in ownership and the termination of a prior mitigation agreement.

<sup>49</sup>50 U.S.C. § 4565(l)(3)(B). The law requires Treasury and the lead agency to periodically review each mitigation agreement with respect to its continued relevance and to terminate, phase out, or otherwise amend the mitigation agreement if a threat no longer requires mitigation.

<sup>50</sup>[GAO-14-704G](#).

---

responsibilities and on a process for making decisions, and should develop written guidance.<sup>51</sup>

A documented CFIUS process for periodically assessing mitigation agreements for their continued relevance and taking any appropriate actions would help ensure that Treasury and lead CMAs regularly and consistently reconsider whether each mitigation agreement remains relevant and adequately addresses risks. A documented process would also help Treasury and other member agencies ensure the efficient use of their resources.

---

## Opportunities Exist to Better Support CFIUS Staffing for Monitoring and Enforcement

---

### Agencies Have Dedicated Staff to Monitor and Enforce Compliance with Agreements

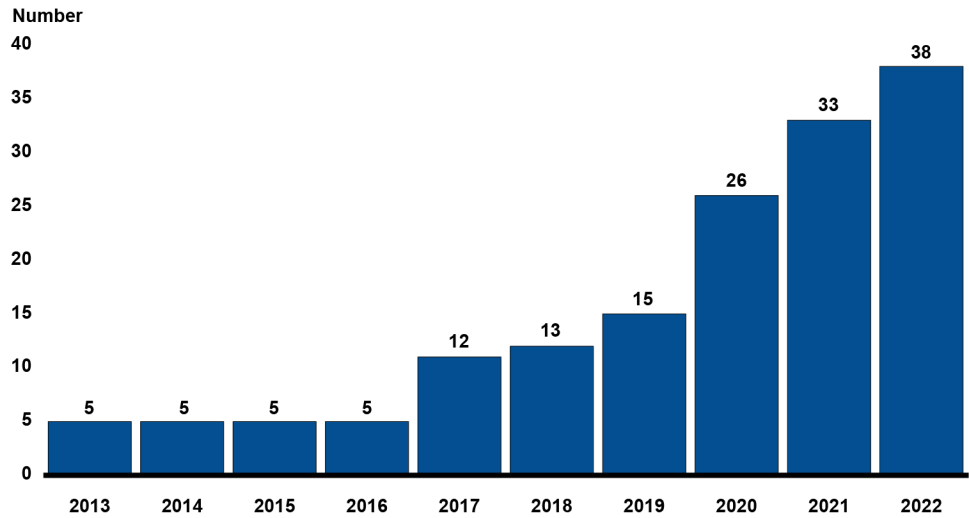
We found that the five selected CFIUS agencies all have dedicated personnel to monitor and enforce compliance with mitigation agreements. In fiscal years 2016 through 2022, the five agencies added more staff to monitor and enforce compliance with mitigation agreements (see fig. 6).<sup>52</sup>

---

<sup>51</sup>[GAO-23-105520](#).

<sup>52</sup>According to agency-reported staffing estimates, agencies have added monitoring and enforcement staff at varying rates. We have omitted information about the number of staff at each agency because Treasury identified that information as sensitive.

**Figure 6: Total Number of Staff at Five Selected CFIUS Agencies Who Dedicated at Least Half of Their Time to Monitoring and Enforcing Compliance with Mitigation Agreements, Fiscal Years 2013–2022**



Source: GAO analysis of staffing estimates reported by selected Committee on Foreign Investment in the United States (CFIUS) member agencies. | GAO-24-107358

Note: For the purpose of our analysis, “mitigation agreements” includes CFIUS agreements, national security agreements, letters of assurance, orders, and CFIUS-imposed conditions on withdrawn notices and abandoned transactions.

Officials from the selected agencies said they have added more staff to address the increased volume and complexity of mitigation agreements. For example, DHS officials said their recent increase in staffing had allowed the department to ensure that each mitigation agreement has the appropriate level of monitoring support. DOD officials said they had hired a cybersecurity expert to review company policies and procedures related to data security, given the rise in mitigation agreements addressing data security risks. DOD officials also said they had added business operations support to manage and coordinate DOD’s site visits and other operations. Treasury officials told us they had set a target of approximately doubling the number of Treasury staff dedicated to CFIUS monitoring and enforcement by the end of fiscal year 2024.

In addition to hiring monitoring staff, four of the five selected agencies have established dedicated offices for monitoring and enforcing compliance with mitigation agreements. For example, Treasury officials said that since 2018, when FIRRMA was enacted, Treasury has expanded its CFIUS-dedicated staff from one to three offices, including an office for monitoring and enforcement. DOD, DHS, and DOJ also have



---

dedicated monitoring and enforcement offices, according to officials. Conversely, DOE has one office dedicated to all CFIUS activities and relies extensively on DOE stakeholders with relevant experience to provide input about the monitoring of particular mitigation agreements, according to officials.

The agencies' CFIUS monitoring and enforcement offices take various approaches to assigning responsibility for certain mitigation agreements to their staff. For example, DOD officials said their goal is to assign approximately 15 mitigation agreements to each case officer. DOJ and DOE officials said they do not designate target caseloads. DOJ officials said that they instead conduct internal managerial assessments before assigning responsibility for mitigation agreements.

In addition, agency officials said that they consult with stakeholders across their respective agencies to support monitoring and enforcement efforts, particularly when a mitigation agreement involves a specialized expertise. For example, DOE officials said they regularly seek stakeholder consultation on site visits and often draw on the science and technology expertise of the National Nuclear Security Administration and the National Laboratories. Similarly, DOD officials said they work with subject matter experts at DOD and other agencies to support site visits. For example, DOD officials said they engaged multiple technical experts on a site visit involving the semiconductor industry. DHS officials said they regularly consult with internal stakeholders, such as the Cybersecurity and Infrastructure Security Agency, U.S. Customs and Border Protection, and the Coast Guard, to support monitoring and enforcement efforts. According to DOJ and Treasury officials, the Federal Bureau of Investigation assists DOJ and other CMAs in reviewing and vetting personnel, vendors, and policies.

---

## Various Factors Affect Agencies' CFIUS Monitoring and Enforcement Workload

### Complexity and Risk Type

According to agency officials, various factors affect their workload for monitoring CFIUS mitigation agreements. These factors include each mitigation agreement's complexity and risk type, its phase, and any violations.

Agency officials told us that the type of risk a mitigation agreement addresses, as well as the associated mitigation measures, often affects the complexity of the mitigation agreement with respect to monitoring and enforcement. For example, according to DOD officials, mitigation agreements addressing supply assurance risks are generally less complex and require fewer resources to manage, while those addressing

---

data and information security risks tend to be more complex, requiring more resources.<sup>53</sup>

Our review of mitigation agreements included four that addressed supply assurance and five that addressed data or information security.<sup>54</sup> We found that the mitigation agreements addressing supply assurance all contained the same two general mitigation measures—requiring the transaction parties to maintain production of the covered product and to notify the CMAs about certain developments, such as a decision to change the production of a covered product. On the other hand, the mitigation agreements addressing data or information security generally contained additional measures, including requirements for the transaction parties to implement technical restrictions on certain sensitive data or information.

According to Treasury officials, growth in the number of mitigation agreements addressing data and information risks, as well as the complex nature of measures to mitigate such risks, has contributed to a general increase in the complexity of mitigation agreements and the associated monitoring.<sup>55</sup>

More generally, Treasury officials said that geopolitical changes have led to increased scrutiny of international investment transactions, requiring CFIUS mitigation agreements to be more detailed and complex. DOD and DHS officials also said that mitigation agreements have been becoming increasingly complex in recent years. According to DHS officials, although mitigation agreements used to have broad, simple language with measures that were easily met and monitored, recent mitigation agreements include more detailed and specific measures, making monitoring more complex. Treasury officials said that the more detailed mitigation agreements are intended to address the increasing complexity

---

<sup>53</sup>DOD officials also said that the level of resources required to monitor compliance with a mitigation agreement is not necessarily related to the level of risk that the mitigation agreement is intended to address. For example, DOD officials said a mitigation agreement addressing supply assurance might be considered very high risk because the covered product is critically important to national security, but the workload associated with the mitigation agreement might consist of simply verifying that the company is still making the specified product.

<sup>54</sup>We selected and reviewed a nongeneralizable sample of 19 mitigation agreements to understand and illustrate how the selected CFIUS agencies monitor and enforce compliance.

<sup>55</sup>We have omitted the number of mitigation agreements addressing data and information security risks, because Treasury identified that information as sensitive.

---

of transactions and associated risks and to help make the mitigation agreements more enforceable. However, DOD officials stressed that the complexity of a mitigation agreement does not necessarily correlate to its enforceability or effectiveness in addressing the national security risk.

Phase

Agency officials said that the initial phase of a mitigation agreement requires the most staff resources to manage. According to the officials, during this phase, the transaction parties implement mitigation measures such as nominating personnel, developing policies and procedures, hiring third-party entities, and performing other implementation tasks that require review and approval by CMAs. DOD officials said that mitigation agreements often specify that CMAs must review these implementation tasks within a set period or risk missing the opportunity to approve or deny the U.S. transaction party's proposals. Agency officials also said that once these mitigation measures are in place, the monitoring workload becomes less labor intensive.

Violations

Agency officials said that violations of mitigation agreements increase the CMAs' workload because they necessitate prompt action to remediate the risk and, if serious, may require additional enforcement actions. According to Treasury officials, violations occur more often during the initial phase of a mitigation agreement, as companies may be implementing mitigation measures for the first time in response to the mitigation agreement.

---

Treasury Did Not Document Objectives or Assess Staffing to Inform Efforts to Increase Its CFIUS Monitoring Staff

Although Treasury is taking steps to increase its CFIUS monitoring staff, it has not documented its objectives for this effort and did not conduct an assessment of its staffing needs before beginning to hire additional staff. Treasury officials said they are taking steps to approximately double their monitoring staff by the end of fiscal year 2024.<sup>56</sup>

Officials described Treasury's objectives for increasing its monitoring staff. Specifically, the officials told us that the additional staff would enable Treasury to take a more proactive role as CFIUS's chair by increasing the agency's capacity to develop and propose more committee-wide guidance for CFIUS's consideration. Officials also said the additional staff would enable Treasury to assume more compliance monitoring responsibilities as a co-lead CMA, such as by conducting more frequent and rigorous site visits. Further, Treasury officials said the

---

<sup>56</sup>We have omitted the number of Treasury's CFIUS monitoring staff because Treasury identified that information as sensitive.

---

additional staff would decrease CFIUS's reliance on third-party monitors.<sup>57</sup>

However, Treasury officials were unable to provide documentation of Treasury's objectives for the increased staffing. *Standards for Internal Control in the Federal Government* calls for management to define objectives clearly and to develop and maintain documentation to retain organizational knowledge.<sup>58</sup> Documenting its objectives for its targeted increase in monitoring staff would provide Treasury a means of assessing the extent to which the staffing increase, once completed, enables it to achieve these objectives.

Moreover, according to Treasury officials, Treasury did not conduct an assessment of its staffing needs before beginning to increase its CFIUS monitoring staff. Instead, according to officials, Treasury estimated the number of staff it would need, because it does not know the number of mitigation agreements that will require monitoring. Officials said that they intend to assess the sufficiency of the increase once staffing reaches the targeted number.

*Standards for Internal Control in the Federal Government* calls for management to periodically evaluate the organizational structure necessary to achieve its objectives.<sup>59</sup> Moreover, federal guidance for workforce planning calls for agencies to conduct analysis of current and future staffing needs, such as identifying any gaps in staffing or staff competencies needed to achieve the agencies' objectives.<sup>60</sup> Conducting a staffing analysis in accordance with this guidance would assist Treasury in determining the extent to which the targeted staffing level, once it is reached, enables Treasury to achieve its documented objectives. It would also assist Treasury in planning for future staffing needs.

---

<sup>57</sup>According to DOD officials, the decision about whether to rely more or less on third-party monitors as a means to monitor compliance with mitigation agreements should be a committee-wide decision.

<sup>58</sup>[GAO-14-704G](#).

<sup>59</sup>[GAO-14-704G](#).

<sup>60</sup>Office of Personnel Management, *Workforce Planning Guide*.

---

## CFIUS Has Not Coordinated on Staffing to Address Resource Levels and Anticipated Growth in Workload

### CMA's Say Current Monitoring Resource Levels Are Insufficient

Officials from three of the five selected agencies told us their current resource levels were insufficient to meet demand for, or expand the scope of, their agencies' monitoring and enforcement efforts. For example, DOE officials said that because of resource levels, they sometimes decline to act as lead CMA on mitigation agreements involving their areas of responsibility and expertise. In these cases, they may defer to a CMA that has comparable interests in the transaction but more resources.<sup>61</sup> DOD officials said that their goal is to assign no more than 15 mitigation agreements to each case officer but that each officer is currently responsible for about 27 mitigation agreements. DOD officials also said that budgetary constraints make hiring additional case officers difficult and that, instead, they frequently redistribute cases among case officers to alleviate workload.

Further, although officials acknowledged that site visits are a critical tool for monitoring compliance with some mitigation agreements, officials from two agencies said their monitoring teams do not have enough resources to complete their targets for site visits. For example, Treasury officials said they believe site visits should generally occur at least annually; however, Treasury currently conducts site visits about once every 3 years for many mitigation agreements because of the large number of active agreements.<sup>62</sup> Similarly, according to DOD officials, they currently do not have enough staff to complete their target of one to two site visits per year for each case and instead must prioritize their monitoring efforts.

Agency officials said they are currently in the process of increasing their staffing levels to address the increased demand for monitoring and enforcement of compliance with mitigation agreements. However, Treasury officials noted that the security clearance process can lead to a

---

<sup>61</sup>According to a 2008 executive order, the lead CMA for a mitigation agreement should seek to ensure it has adequate resources available for monitoring risk mitigation measures. Exec. Order No. 13456, 73 Fed. Reg. 4677 (Jan. 23, 2008).

<sup>62</sup>Treasury officials stated that the frequency of site visits is unique to each mitigation agreement. Those that are complex or have potential compliance issues may require several site visits per year, while those that are simpler to monitor may require infrequent or no site visits, according to the officials.

---

---

CFIUS Does Not Regularly Discuss and Coordinate on Staffing for Monitoring and Enforcement

lengthy hiring process; in particular, denial of provisional security clearances limits their ability to hire new staff quickly. DOD officials said that although all new staff still undergo the security clearance process after onboarding, the department recently eased its security clearance requirements for its prospective CFIUS staff, thus widening its applicant pool.

Although CFIUS staffing needs are expected to grow, the committee does not, despite members' shared responsibilities, regularly discuss and coordinate on the staffing levels needed to monitor and enforce compliance with mitigation agreements. Officials from all five selected agencies said that the number and complexity of mitigation agreements have recently increased, leading to larger workloads. Moreover, some officials expressed concern that limitations in their current staffing resources will affect their ability to monitor compliance.

Officials from three of the five selected agencies said that forecasting their specific CFIUS staffing requirements is difficult. For example, although DOE officials said that the increase in mitigation agreements will require more monitoring staff, they stated that it is nearly impossible to accurately predict the number and complexity of mitigation agreements DOE will be responsible for monitoring in the future. Similarly, Treasury officials said that although they consider a mitigation agreement's risk type an indicator of potential workload, forecasting workload on this basis is difficult because trends in risk types vary from year to year. The officials said that it is easier to prioritize the existing mitigation agreements that will require the most work and that they sometimes adjust Treasury staff's ongoing case workloads.

However, according to CFIUS agency officials, they do not regularly hold committee-wide discussions to coordinate CFIUS staffing needs. DOD officials said they have informal conversations about staffing levels with officials of other CFIUS agencies before submitting budget requests. According to DOD officials, during these conversations they ask about the other agencies' current staffing levels and the numbers of additional staff they plan to request. The officials said that these conversations help shape their budget requests for adequate monitoring and enforcement resources and that they are aware of other agencies' holding similar informal discussions. Yet, according to the officials, these discussions do not occur committee-wide or with any regular frequency. Additionally, Treasury officials said they had not informed the committee about Treasury's plan to take a more proactive monitoring role as CFIUS's chair

---

or discussed with the committee any potential effects of Treasury's plan on other agencies' staffing needs.<sup>63</sup>

According to Treasury officials, Treasury has not, as CFIUS's chair, worked with the other members to establish a scheduled and regularly occurring committee-wide process for discussing and coordinating members' staffing needs for monitoring mitigation agreements. Officials stated that Treasury cannot direct CFIUS agencies to change their staffing.

However, leading practices in interagency collaboration call for collaborating agencies to look for opportunities to address needs by assessing the resources and capacities that each agency can contribute to the collaborative effort.<sup>64</sup> Further, *Standards for Internal Control in the Federal Government* calls for management to establish the organizational structure necessary to achieve its objectives and to periodically evaluate this structure.<sup>65</sup> A scheduled and regularly occurring committee-wide process for CFIUS members to discuss and coordinate their staffing needs would help them ensure that they have adequate resources to effectively monitor and enforce mitigation agreements.

---

## Conclusions

CFIUS has adapted over time to meet the evolving national security threats posed by foreign investment into the United States. In 2018, Congress expanded CFIUS's jurisdiction to encompass additional investment types, which, according to agency officials, contributed to an increase in the number of transactions CFIUS reviewed. In response to these events and certain foreign investment trends, CFIUS has been negotiating an increasing number of mitigation agreements to address national security risks and preserve benefits to the U.S. economy. In addition, CFIUS member agencies—including Treasury, the committee's chair—have recognized the need to standardize their approaches to monitoring and enforcing compliance with the growing number of mitigation agreements and to bolster their resources to carry out the attendant workload.

---

<sup>63</sup>Officials of three of the five selected agencies stated that staff availability is not a determining factor when they sign onto a new mitigation agreement, because each agency generally prefers to address national security risks related to its area of responsibility and expertise, regardless of resources.

<sup>64</sup>[GAO-23-105520](#).

<sup>65</sup>[GAO-14-704G](#).

---

However, as Treasury officials acknowledged, CFIUS lacks documented processes for reaching consensus on enforcement decisions and determining whether and when to terminate outdated mitigation agreements. Working with the other member agencies to document a committee-wide process for deciding on enforcement actions would strengthen Treasury's ability, as chair, to help ensure timely responses to serious violations. Similarly, a documented committee-wide process for regularly reviewing mitigation agreements would help Treasury and the other members ensure the continued relevance of each mitigation agreement and efficiently allocate their resources for monitoring and enforcement.

Moreover, although Treasury intends to double its CFIUS monitoring staff to support a planned expansion of its role as chair, it has not documented its objectives for the targeted staffing increase, which it based on an estimate rather than an assessment of its staffing needs. Documenting these objectives would allow Treasury to assess the extent to which the increased staffing, once it reaches the targeted level, can enable Treasury to achieve them. Moreover, conducting a staffing analysis in accordance with federal workforce planning guidance, such as by identifying any gaps in current or future staffing and staff competencies, would help Treasury determine the extent to which the targeted increase enables it to achieve its documented objectives. Such an analysis would also assist Treasury in planning for future staffing needs.

Finally, officials of the five agencies we selected for our review said that the number and complexity of mitigation agreements have recently increased, raising questions about their ability to sustain effective monitoring and enforcement of compliance with these mitigation agreements. A committee-wide process for regularly discussing and coordinating member agencies' future CFIUS staffing needs would help ensure the committee's continued capacity to review and address national security risks arising from certain transactions involving foreign investment in the United States.

---

## Recommendations for Executive Action

We are making the following five recommendations to Treasury:

The Secretary of the Treasury, as CFIUS's chair, should work with member agencies to document a committee-wide process for considering and making timely decisions on enforcement actions related to mitigation agreements. (Recommendation 1)



---

The Secretary of the Treasury, as CFIUS's chair, should work with member agencies to document a committee-wide process for periodically assessing the relevance of mitigation agreements and amending, phasing out, or terminating them when appropriate. (Recommendation 2)

The Secretary of the Treasury should document Treasury's objectives for increasing its staff for monitoring and enforcing compliance with CFIUS mitigation agreements. (Recommendation 3)

The Secretary of the Treasury should, once the targeted staffing increase is completed, analyze its CFIUS monitoring and enforcement staffing in accordance with federal workforce planning guidance, to determine the extent to which the targeted increase enables Treasury to achieve its documented objectives. (Recommendation 4)

The Secretary of the Treasury, as CFIUS's chair, should work with member agencies to establish a committee-wide process to regularly discuss and coordinate the staffing levels needed to address the projected increase in workload associated with monitoring and enforcing CFIUS mitigation agreements. (Recommendation 5)

---

## Agency Comments

We provided a draft of our sensitive report to Treasury, DOD, DOE, DHS, and DOJ for review and comment. Treasury's comments about the sensitive report are reproduced in appendix II. Treasury and DHS also provided technical comments, which we incorporated as appropriate. DOD, DOE, and DOJ did not provide comments.

In its comments, Treasury agreed with all five of our recommendations, stating that they underscore the need to document and strengthen certain interagency processes and enhance documentation of objectives for staffing resources. Treasury stated that in 2024 it plans to seek committee-wide adoption of standard procedures for enforcing and reviewing existing mitigation agreements. Treasury also noted that the rapid growth in CFIUS's monitoring workload emphasizes the need for greater communication among the committee's member agencies regarding staffing needs.

---

We are sending copies of this report to the appropriate congressional committees, the Secretary of the Treasury, the Secretary of Defense, the Secretary of Energy, the Secretary of Homeland Security, and the Attorney General. The report is also available at no charge on GAO's website at <http://www.gao.gov>.

---

If you or your staff have any questions about this report, please contact Kimberly Gianopoulos at (202) 512-8612 or [gianopoulosk@gao.gov](mailto:gianopoulosk@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Staff who made key contributions to this report are listed in appendix III.

A handwritten signature in black ink that reads "Kimberly M. Gianopoulos". The signature is written in a cursive style with a large initial 'K'.

Kimberly M. Gianopoulos  
Director, International Affairs and Trade

---

# Appendix I: Objectives, Scope, and Methodology

---

This report (1) describes trends in the Committee on Foreign Investment in the United States' (CFIUS) mitigation agreements from 2000 through 2022, (2) evaluates selected CFIUS member agencies' approaches to monitoring and enforcing compliance with mitigation agreements and reviewing them for their continued relevance, and (3) assesses selected member agencies' staffing for monitoring and enforcement.

This report is a public version of a sensitive report that we issued on January 22, 2024.<sup>1</sup> This public version of that report addresses the same objectives and uses the same methodology. However, this report omits certain information that Treasury identified as sensitive, requiring protection from public disclosure. Specifically, this report omits information related to, in the first objective, characteristics of mitigation agreements that were active in 2023, including the country and the type of national security risk; in the second objective, Treasury's internal guidance and processes for enforcement of mitigation agreements; and in the third objective, the number of selected agencies' staff who monitor and enforce mitigation agreements.

To address these objectives, we reviewed relevant laws, executive orders, regulations, and CFIUS public reports. In addition, to describe trends in mitigation agreements, we analyzed Department of the Treasury data on mitigation agreements that were active or terminated between 2000 and 2022. We assessed the reliability of these data by reviewing them for errors and inconsistencies, interviewing agency officials about the data, and reviewing trends in the data with the officials. We also compared the Treasury data with equivalent data from another CFIUS member agency. We determined that these data were sufficiently reliable to describe trends in mitigation agreements since 2000.

We selected five CFIUS agencies—Treasury and the Departments of Defense, Energy, Homeland Security, and Justice—on the basis of the number of active mitigation agreements each managed as of March 2023.<sup>2</sup> To evaluate selected member agencies' approaches to monitoring and enforcing compliance with mitigation agreements and reviewing them for their continued relevance, we reviewed internal agency guidance documents and interviewed agency officials. We assessed agency

---

<sup>1</sup>GAO, *Foreign Investment in the U.S.: Efforts to Mitigate National Security Risks Can Be Strengthened*, GAO-24-106259SU (Washington, D.C.: Jan. 22, 2024).

<sup>2</sup>We have omitted the number of mitigation agreements each agency managed, because Treasury identified that information as sensitive.

processes against internal control principles related to responding to risks and implementing control activities<sup>3</sup> and against leading practices in interagency collaboration.<sup>4</sup>

We also selected and reviewed a nongeneralizable sample of 19 mitigation agreements to understand and illustrate how the five selected CFIUS agencies monitor and enforce compliance. For four of the selected agencies, we randomly selected four mitigation agreements led by each agency—two agreements that were entered into before, and two that were entered into after, the implementation of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA).<sup>5</sup> For the fifth agency, Treasury, we randomly selected two mitigation agreements that were entered into before the act’s implementation; we also selected one case that was entered into after the act’s implementation. Because our review of the mitigation agreements was not generalizable, the characteristics we observed may not reflect those of other mitigation agreements. We also reviewed additional mitigation agreements during in-person meetings with agency officials.

To assess the selected CFIUS members’ staffing for monitoring and enforcement, we obtained agency estimates of the number of staff who dedicated at least 50 percent of their time to monitoring and enforcing mitigation agreements in fiscal years 2013 through 2022. To determine the reliability of the data, we reviewed the data for errors and inconsistencies and interviewed agency officials. We determined that the data were sufficiently reliable for assessing the agencies’ staffing for monitoring and enforcement. We interviewed agency officials regarding staffing processes and workload issues. We assessed agency staffing processes against internal control principles related to defining objectives and establishing the organizational structure to achieve objectives;<sup>6</sup>

---

<sup>3</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

<sup>4</sup>GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, [GAO-23-105520](#) (Washington, D.C.: May 24, 2023).

<sup>5</sup>John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, §§ 1701-1728, 132 Stat. 1636, 2173-2208 (Aug. 13, 2018) (codified as amended at 50 U.S.C. § 4565).

<sup>6</sup>[GAO-14-704G](#).

against federal guidance on workforce planning;<sup>7</sup> and against leading practices for interagency collaboration.<sup>8</sup>

The performance audit on which this report is based was conducted from September 2022 to January 2024 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 Treasury from February 2024 to April 2024 to prepare this version of the original sensitive report for public release. This public version was also prepared in accordance with generally accepted government auditing standards.

---

<sup>7</sup>Office of Personnel Management, *Workforce Planning Guide* (November 2022).

<sup>8</sup>[GAO-23-105520](#).

# Appendix II: Comments from the Department of the Treasury



DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

ASSISTANT SECRETARY

December 21, 2023

Kimberly Gianopoulos  
Director, International Affairs and Trade  
Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Ms. Gianopoulos,

The Department of the Treasury (Treasury) appreciates efforts over the past year by the Government Accountability Office (GAO) in preparing the report, "Foreign Investment in the U.S.: Efforts to Mitigate National Security Risks Can Be Strengthened." As Chair of the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee"), Treasury is continuously seeking to ensure the Committee operates as effectively and efficiently as possible and welcomes GAO's insights and recommendations.

In particular, GAO's report highlights the importance of the Committee's compliance, monitoring, and enforcement work – a growing responsibility that is integral to the Committee's ability to fulfill its critical national security mission. When a covered transaction raises national security risks, the Committee can mitigate the risk by requiring transaction parties to undertake certain measures that are typically formalized in what is called a National Security Agreement, or "mitigation agreement." But the Committee's work does not stop once the mitigation agreement is signed.

The Committee routinely conducts site visits, collects documents and information, and engages with security personnel, third-party monitors, and auditors to ensure that transaction parties uphold the terms of these agreements. While preventing violations from occurring is the Committee's primary focus, the availability of robust remediation and enforcement tools in the event of non-compliance is necessary because a breach could harm national security. Under the Defense Production Act, the Committee has its own enforcement authority — including subpoena authority — and can impose monetary penalties and seek other remedies for violations of its statute, regulations, mitigation orders, conditions, or agreements. The Committee does not hesitate to take enforcement action when necessary to protect national security.

Treasury accepts all of GAO's recommendations, which underscore the need to further document, and in some cases strengthen, certain interagency processes as well as enhance documentation of objectives for staffing resources devoted to CFIUS monitoring and enforcement. Treasury is pleased that GAO acknowledges Treasury's ongoing efforts to document best practices and develop new CFIUS-wide guidance and processes, including the

**Appendix II: Comments from the Department  
of the Treasury**

convening of interagency knowledge-sharing workshops and the development of standard templates as a starting point for mitigation agreement terms. Additionally, the Committee has already made significant progress toward strengthening and documenting its processes in two specific areas addressed in the recommendations:

- In October 2022, Treasury publicly released CFIUS enforcement and penalty guidelines for holding transaction parties accountable if they fail to comply with mitigation agreements or fail to uphold their obligations to mitigate national security risk. In addition, Treasury continues to revise the internal enforcement procedures it has shared with GAO and plans to seek Committee-wide adoption of standard enforcement procedures in 2024.
- In reviewing mitigation agreements for revision or termination, CFIUS is guided by both the relevant statutory language and the internal procedures of Treasury's monitoring and enforcement team and of the other CFIUS Monitoring Agencies. Treasury continues to revise the internal procedures it has shared with GAO and in 2024 plans to seek Committee-wide adoption of standard procedures for reviewing existing mitigation agreements.

Finally, Treasury continues to assess its CFIUS monitoring and enforcement staffing needs, given the difficulty of predicting future caseloads, and concurs that documenting our objectives with greater specificity will be helpful. We are pleased that GAO acknowledges the rapid growth of the Committee's – and especially Treasury's – monitoring workload since the 2018 enactment of the Foreign Investment Risk Review Modernization Act. We concur that this rapid workload expansion – and the demand for additional staffing that comes with it – emphasize the need for greater communication among CFIUS member agencies on staffing needs. Such communication will also improve our coordination with Congress to ensure that CFIUS has the funding it needs to complete its critical national security mission.

While we are proud of the Committee's efforts to protect national security, the work of CFIUS remains unfinished, and there are always ways to improve. As Chair, Treasury remains focused on leading the Committee to maximize its effectiveness, and we look forward to continuing our work in this regard. CFIUS remains committed to using every available authority to protect the national security of the United States.

Sincerely,



Paul Rosen  
Assistant Secretary for Investment Security

---

# Appendix III: GAO Contact and Staff Acknowledgments

---

## GAO Contact

Kimberly Gianopoulos, (202) 512-8612 or [GianopoulosK@gao.gov](mailto:GianopoulosK@gao.gov)

---

## Staff Acknowledgments

In addition to the contact named above, Christina Werth (Assistant Director), Adam Peterson (Analyst in Charge), Marc Rockmore, Kevin Lyman, Alejandro Coste-Sanchez, Reid Lowe, Chris Keblitis, Terry Richardson, and Miranda Riemer made key contributions to this report.



---

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).  
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).  
Visit GAO on the web at <https://www.gao.gov>.

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

---

## Congressional Relations

A. Nicole Clowers, Managing Director, [ClowersA@gao.gov](mailto:ClowersA@gao.gov), (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

---

## Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, [spel@gao.gov](mailto:spel@gao.gov), (202) 512-4707  
U.S. Government Accountability Office, 441 G Street NW, Room 7814,  
Washington,

