United States Government Accountability Office

Report to Congressional Requesters

August 2021

DOD FRAUD RISK MANAGEMENT

Actions Needed to Enhance Department-Wide Approach, Focusing on Procurement Fraud Risks

Accessible Version

GAO@100

A Century of Non-Partisan Fact-Based Work

GAO-21-309

GAO Highlights

Highlights of GAO-21-309, a report to congressional requesters

August 2021

DOD FRAUD RISK MANAGEMENT

Actions Needed to Enhance Department-Wide Approach, Focusing on Procurement Fraud Risks

Why GAO Did This Study

GAO was asked to review issues related to DOD's fraud risk management. DOD obligated $421.8 billion in fiscal year 2020 on contracts. GAO has long reported that DOD's procurement processes are vulnerable to waste, fraud, and abuse. In 2018, DOD reported to Congress that from fiscal years 2013-2017, over $6.6 billion had been recovered from defense-contracting fraud cases. In 2020, the DOD Office of Inspector General reported that roughly one-in-five of its ongoing investigations are related to procurement fraud. This report assesses the steps DOD took in fiscal year 2020 (1) to combat department-wide fraud risks and (2) to conduct a fraud risk assessment and ensure that DOD's component organizations reported procurement fraud risks.

GAO analyzed applicable DOD policy and documents and compared them with Fraud Risk Framework leading practices, interviewed DOD officials, and reviewed fiscal year 2020 fraud risk assessments from six DOD components. GAO selected the six based primarily on fiscal years 2014-2018 contract obligations.

What GAO Recommends

GAO makes five recommendations, including that DOD fill all Task Force positions, update its policy to require fraud risk assessments, and ensure that components assess procurement fraud risks. DOD agreed with some, but not all of the recommendations. GAO continues to believe all the recommendations are warranted and should be implemented.

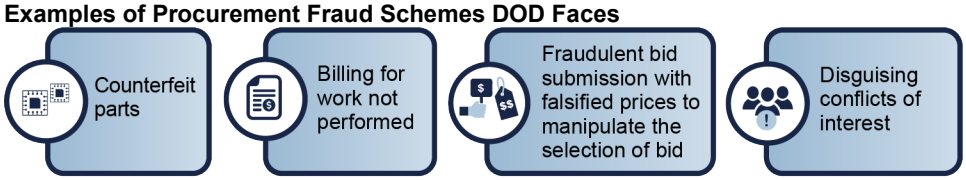
View GAO-21-309. For more information, contact Seto J. Bagdoyan at (202) 512-6722 or bagdoyans@gao.gov.

What GAO Found

The Department of Defense (DOD) faces numerous types of procurement fraud schemes (see figure). For example, in January 2015, the owner of a contracting firm pleaded guilty to bribing DOD officials and defrauding DOD of tens of millions of dollars by overbilling for goods and services. To combat department-wide fraud risks, DOD has taken initial steps that generally align with GAO's *Fraud Risk Framework*. However, DOD has not finalized and implemented a comprehensive approach. For example:

- DOD created a Fraud Reduction Task Force—a cross-functional team represented by subject matter experts across the department—to prioritize fraud risks and identify solutions. But its membership is incomplete. A year after formation, 11 of DOD's 59 component organizations, including the Army, had not designated a Task Force representative. Filling vacant Task Force positions would further strengthen DOD's ability to manage its fraud risks.
- DOD uses its risk management program to assess and report fraud risks. But the policy governing the risk management program does not specifically require fraud risk assessments. As a result, DOD may not be identifying all fraud risks, and its control activities may not be appropriately designed or implemented.
- DOD officials told GAO that they share fraud risk information with agencies' risk management officials, but documentation of stakeholders' roles and responsibilities remains incomplete. Such documentation can help ensure these stakeholders understand their responsibilities.

Examples of Procurement Fraud Schemes DOD Faces



Source: GAO presentation of information from Department of Defense Fiscal Year 2020 Statement of Assurance Execution Handbook. | GAO-21-309

Text of Examples of Procurement Fraud Schemes DOD Faces

- Counterfeit parts
- Billing for work not performed
- Fraudulent bid submission with falsified prices to manipulate the selection of bid
- Disguising conflict of interest

Source: GAO presentation of information from Department of Defense Fiscal Year 2020 Statement of Assurance Execution Handbook. | GAO-21-309

DOD has taken steps to ensure components plan for and assess fraud risks. But some selected components did not report procurement fraud risks, as required

by DOD. DOD provides guidance, tools, and training to its components to conduct fraud risk assessments and to assess procurement fraud risks. However, GAO found that three of six selected components reported procurement fraud risks in their fiscal-year-2020 risk assessments, and that three—which obligated $180.1 billion in fiscal year 2020—did not. Because DOD consolidates reported procurement risks from the components' fraud risk assessments and uses this information to update the department-wide fraud risk profile, it cannot ensure that its fraud risk profile is complete or accurate.

Contents

Tables

Figures

Abbreviations

2021 NDAA	William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021
CAGE	Commercial and Government Entity
DCAA	Defense Contract Audit Agency
DOD	Department of Defense
DOD OIG	Department of Defense Office of Inspector General
DUNS	Data Universal Numbering System
ERM	Enterprise Risk Management
FPDS	Federal Procurement Data System
FRA	Fraud Risk Assessment
Fraud Risk Framework	*A Framework for Managing Fraud Risks in Federal Program*
FRTF	Fraud Reduction Task Force
NDAA	National Defense Authorization Act
OCMO	Office of the Chief Management Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
RMIC	Risk Management Internal Control
SOA	Statement of Assurance

441 G St. N.W.
Washington, DC 20548

August 19, 2021

The Honorable Bernard Sanders
Chairman
Committee on the Budget
United States Senate

The Honorable Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform
House of Representatives

The Department of Defense (DOD), the largest contracting agency in the federal government, typically accounts for about two-thirds of all federal contracting activity. According to data from the Federal Procurement Data System (FPDS), the government's procurement database, DOD obligations increased from about $320 billion in fiscal year 2016 to roughly $422 billion in fiscal year 2020 on contracts for goods and services, including major weapon systems and information technology. The scope and scale of this activity makes DOD procurement inherently susceptible to fraud.

We have identified long-standing issues associated with DOD procurement. Specifically, in 1990, we placed DOD acquisitions on our inaugural High-Risk List, and in 1992, we added DOD's contract management to the list due to challenges in its operational contract support and a fragmented approach to acquiring service contracts. In 2005, we placed DOD's approach to business transformation on our High-Risk List because weaknesses in operations intended to support the warfighter—including processes related to the management of contracts and weapon systems acquisitions—render DOD's operations vulnerable

to fraud, waste, and abuse.[1] These three areas remain on our High-Risk List, which was most recently updated in March 2021. DOD has made some progress addressing weaknesses in these areas but needs to do more work to fully address them. For example, we reported that DOD has continued to demonstrate leadership and show momentum in transforming its business operations but should formalize key officials' responsibilities.

The DOD Office of Inspector General (OIG) has also long reported contracting fraud as a major management challenge and, in fiscal year 2020, identified acquisitions and contract management as a major management challenge.[2] In fiscal year 2021, the DOD OIG reiterated that fraud and acquisition reforms continue to be enduring management challenges.[3] Relatedly, procurement fraud investigations comprise a major portion of DOD OIG cases. For example, in 2020, the DOD OIG reported that 395 of its 1,716 ongoing investigations—or approximately one in five—are related to procurement fraud.[4]

Fraud poses a significant risk to program integrity and erodes public trust in the government. In July 2015, we issued *A Framework for Managing Fraud Risks in Federal Programs (Fraud Risk Framework)* to help federal managers combat fraud and preserve integrity within government

[1]GAO, *High Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas,* GAO-21-119SP (Washington, DC: Mar. 2, 2021). We update the High-Risk List every 2 years with programs and operations that are 'high risk' due to vulnerabilities to fraud, waste, abuse, and mismanagement, or needing broad reform. To determine which federal government programs and functions should be designated high risk, we employ a guidance document with relevant criteria: GAO, *Determining Performance and Accountability Challenges and High Risks*, GAO-01-159SP (Washington, D.C.: Nov. 2000). This document outlines the qualitative and quantitative risks such as whether the risk involves national defense or could significantly impair services, or if at least $1 billion is at risk including the potential evidence of improper payments or a major asset being wasted. We also consider corrective measures planned or under way to resolve the challenge. Key elements needed to make progress in high-risk areas include leadership commitments and an action plan.

[2]OIG, DOD, *Fiscal Year 2020, Top DOD Management Challenges,* (Alexandria, VA: Oct. 15, 2019).

[3]OIG, DOD, *Fiscal Year 2021, Top DOD Management Challenges,* (Alexandria, VA: Oct. 15, 2020).

[4]OIG, DOD, *Semiannual Report to the Congress: October 1, 2019 through March 31, 2020* (Alexandria, VA). This is the most recent DOD OIG report that presents detailed numbers on types of cases.

agencies and programs.[5] We identified leading practices for managing fraud risks and organized these practices into a framework. For example, the first component of the *Fraud Risk Framework* calls for managers to commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management. One case—considered by the DOD OIG to be one of the largest and most complex corruption scandals in the Department's history—underscores the importance of ethical culture. Specifically, in January 2015, the owner of a DOD contracting firm pleaded guilty to bribing "scores" of U.S. Navy officials and defrauding the Navy of tens of millions of dollars by routinely overbilling for various goods and services.[6] Over more than a decade, the owner bribed Navy officials in exchange for classified and confidential information, as well as preferential treatment in the contracting process.

You asked us to review issues related to DOD's fraud risk, specifically those related to contracting.[7] This report assesses the steps DOD took in fiscal year 2020:

- to combat department-wide fraud risks, and
- to conduct a fraud risk assessment and ensure that DOD's component organizations reported procurement fraud risks.

To assess the steps DOD has taken to combat department-wide fraud risks, we analyzed DOD policy and guidance documents related to DOD fraud risk management and compared those documents with leading practices contained in the *Fraud Risk Framework*.[8] Specifically, we assessed these documents against the leading practices relevant to the

[5]GAO, *A Framework for Managing Fraud Risks in Federal Programs,* GAO-15-593SP (Washington, D.C.: July 28, 2015).

[6]Department of Justice, *Defense Contractor and its CEO Plead Guilty to Corruption Conspiracy Involving "Scores" of Navy Officials*, 15-054 (Jan. 15, 2015).

[7]Fraud and fraud risk are distinct concepts. Fraud involves obtaining something of value through willful misrepresentation and is a determination to be made through the judicial or other adjudicative system. According to the DOD OIG, procurement fraud damage can extend beyond financial losses. It also threatens DOD's ability to achieve its objectives and can undermine the safety and operational readiness of the warfighter. Fraud risk exists when individuals have an opportunity to engage in fraudulent activity, have an incentive or are under pressure to commit fraud, or are able to rationalize committing fraud. Fraud risk can exist even if actual fraud has not occurred. When fraud risks can be identified and mitigated, fraud may be less likely to happen.

[8]GAO-15-593SP.

first component of the *Fraud Risk Framework:* commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.[9] In addition, we assessed the information gathered to determine the extent to which DOD's activities align with relevant federal internal control standards contained in the *Standards for Internal Control in the Federal Government (Federal Internal Control Standards)*—such as those relating to demonstrating oversight and enforcing accountability.[10] We also interviewed officials from the Under Secretary of Defense (Comptroller) and the Office of the Chief Management Officer to discuss their roles in fraud risk management.

To assess the steps DOD has taken to conduct a fraud risk assessment and ensure that DOD component organizations reported procurement fraud risks, we reviewed applicable guidance and interviewed officials from the Comptroller and the Office of the Chief Management Officer. We compared DOD's guidance to relevant leading practices related to the second component of the *Fraud Risk Framework:* plan regular fraud-risk assessments and assess risks to determine a fraud risk profile. We selected six DOD components for review of their fraud risk assessments to determine the extent to which they reported on the high-risk focus area of procurement fraud. We selected five components—the Departments of the Air Force, Army, and Navy; the Defense Logistics Agency; and the Washington Headquarters Services—based on contract obligations during fiscal years 2014 through 2018, the 5 most recent years available at the time of our selection.[11] The Departments of the Air Force, Army, and Navy obligate a majority of DOD's contracting dollars. The Defense Logistics Agency manages the global supply chain—from raw materials to end-user to disposition—for the Air Force, Army, and Navy, among other

[9]The *Fraud Risk Framework* contains four components: (1) commit; (2) assess; (3) design and implement; and (4) evaluate and adapt. Within the four components, there are overarching concepts and leading practices. To assess the steps DOD took to combat department-wide fraud risks, we selected the first component—commit—because DOD formalized its fraud risk management approach in fiscal year 2020 and is in the initial stages of implementation.

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

[11]During fiscal years 2014 through 2018, 23 DOD components reported contract obligations in Federal Procurement Data System (FPDS). We determined that FPDS is sufficiently reliable for purposes of determining DOD contract obligations from fiscal years 2014 through 2018 overall and across select DOD components. We primarily selected components with the largest contract obligations whose main functions were not national intelligence or health care, which were outside our scope.

components. Washington Headquarters Services has a broad scope of responsibilities, including facility management and centralized contracting and procurement. We selected the sixth component—the Defense Contract Management Agency—based on its role in providing contract administration services for DOD, including the military services. Our findings from the six selected components cannot be generalized to the remaining DOD components.

Our review was limited to DOD's fraud-risk management activities for fiscal year 2020. Therefore, this engagement does not examine the effects of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021's (2021 NDAA) repeal of the Chief Management Officer position.[12] For further discussion about our scope and methodology, see appendix I.

We conducted this performance audit from January 2019 to August 2021 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.

Background

DOD Contracting

During fiscal year 2020, DOD's appropriations amounted to approximately $712.6 billion[13] and it obligated $421.8 billion for contracting activity.[14] As shown in figure 1, DOD generally accounts for about two-thirds of federal contracting activity, obligating more than all civilian federal agencies

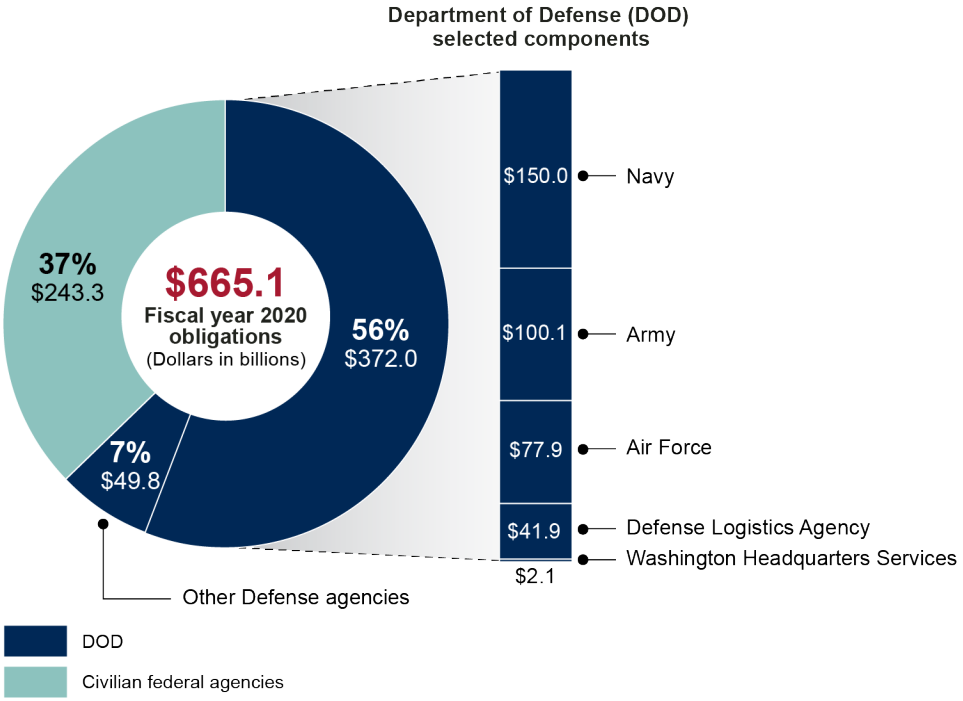
[12]Pub. L. No. 116-283, Div. A, § 901, 134 Stat. 3388, 3794 (2021).

[13]DOD, *United States Department of Defense Fiscal Year 2021 Budget Request,* (Washington, D.C.: May 2020).

[14]As mentioned earlier, DOD contract management has been on the High-Risk List since 1992. We identified three major areas of challenges: Acquisition Workforce, Service Acquisitions, and Operational Contract Support. In 2021, we reported that DOD has significantly mitigated some key contract management risks, particularly risks involving its acquisition workforce, but it should do more to address risks involving contracted services and operational contract support.

combined, and in fiscal year 2020 was led by the Navy in terms of obligations.

Figure 1: Fiscal Year 2020 Department of Defense's and Selected Components' Obligations for Contracting Activity Compared to Civilian Federal Agencies



Source: GAO analysis of Federal Procurement Data System. | GAO-21-309

Data tables for Figure 1: Fiscal Year 2020 Department of Defense's and Selected Components' Obligations for Contracting Activity Compared to Civilian Federal Agencies

$665.1 Fiscal year 2020 obligations (Dollars in billions)		
37%	$243.3	Civilian federal agencies
7%	$49.8	Other Defense agencies
56%	$372.0	Department of Defense (DOD) components

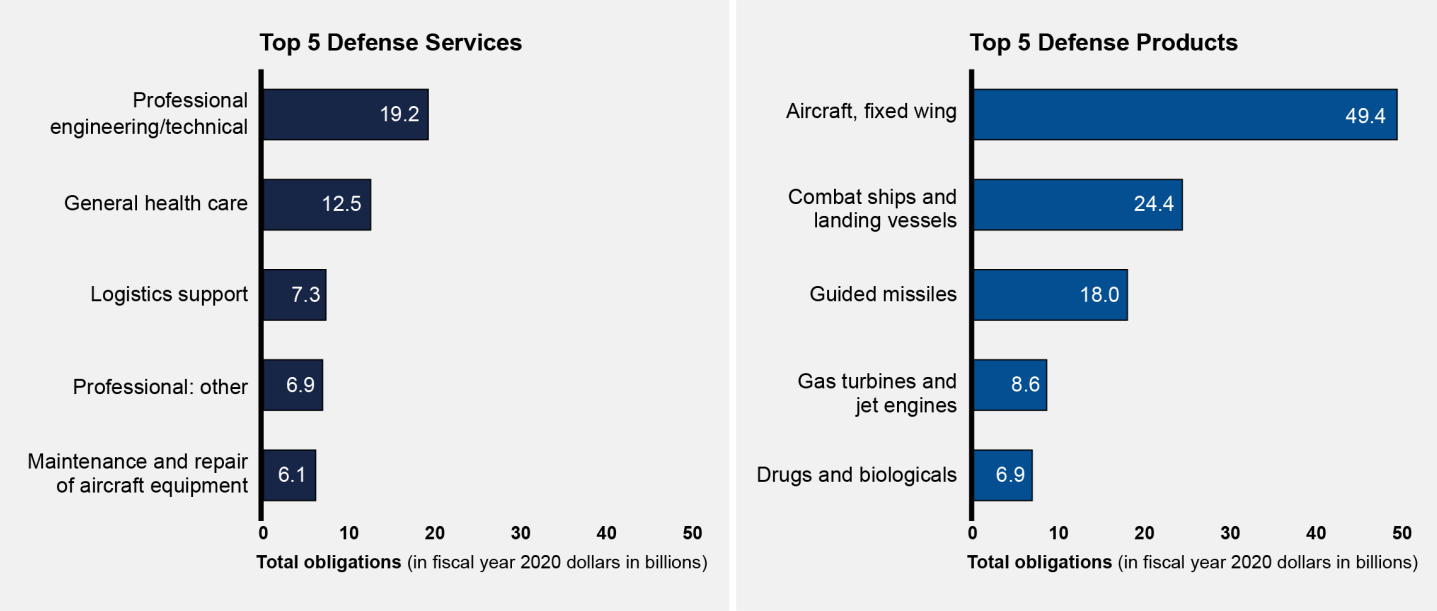
Department of Defense (DOD) selected components	
$150.0 billion	Navy
$100.1 billion	Army
$77.9 billion	Air Force
$41.9 billion	Defense Logistics Agency
$2.1 billion	Washington Headquarters Services

Source: GAO analysis of Federal Procurement Data System. | GAO-21-309

Note: We also selected a sixth component not included here—the Defense Contract Management Agency—based on its role in providing contract administration services for DOD, including the military services. We did not include this component in this figure because the agency had negative obligations for fiscal year 2020 due to de-obligating funds during the contract closeout process. Closing a contract includes tasks such as verifying that the goods and services were provided and making final payment to the contractor.

DOD awards contracts to companies in the private sector to provide a wide variety of products and services for U.S. military forces. In fiscal year 2020, DOD obligated funds to roughly 47,000 contractors. As indicated in figure 2, DOD obligated funds for products and services including aircraft, combat ships, professional engineering, and health care.

Figure 2: Department of Defense Obligations for Top 5 Products and Services in Fiscal Year 2020



Source: GAO analysis of Federal Procurement Data System. | GAO-21-309

Data table for Figure 2: Department of Defense Obligations for Top 5 Products an

Top 5 Defense Services		Top 5 Defense Products	
Professional engineering/technical	$19.2	Aircraft, fixed wing	$49.4
General health care	$12.5	Combat ships and landing vessels	$24.4
Logistics support	$7.3	Guided missiles	$18.0
Professional, other	$6.9	Gas turbines and jet engines	$8.6

Top 5 Defense Services		Top 5 Defense Products	
Maintenance and repair of aircraft equipment	$6.1	Drugs and biologicals	$6.9
Total obligations (in fiscal year 2020 dollars in billions)		**Total obligations** (in fiscal year 2020 dollars in billions)	

Source: GAO analysis of Federal Procurement Data System. | GAO-21-309d Services in Fiscal Year 2020

DOD Contracting Fraud

According to DOD, there are numerous contracting fraud schemes DOD may face—including bid rigging, inflated prices, counterfeit parts, conflicts of interest, false documentation for contractor payments, and overbilling by contractors.[15] Additionally, in November 2019, we reported that DOD faces several types of financial and nonfinancial fraud risks, as well as national security risks posed by contractors with opaque ownership.[16] An opaque ownership structure conceals other entities or individuals who own, control, or financially benefit from the company and can facilitate fraud and other unlawful activity. We concluded that DOD faces challenges with identifying and verifying a contractor's ownership(s). For example, we found that the General Services Administration's integrity and performance database provides limited ownership information to contracting officials, including those in DOD. We recommended that DOD assess risks related to a contractor's ownership(s) as part of its ongoing efforts to assess fraud risk. DOD agreed with our recommendation, and starting in fiscal year 2021, is requiring components to report on fraud risks related to opaque contractor ownership. Also, based on our November 2019 report, the 2021 NDAA requires the General Services Administration to include, for certain corporations including those with a federal contract in excess of $500,000, the identification of the corporation's beneficial owner as part of its integrity and performance database.[17]

The extent of fraud associated with DOD's contracting has not been determined. One of the many challenges is that because of fraud's

[15]DOD, *Fiscal Year 2020 Department of Defense Statement of Assurance Execution Handbook* (January 30, 2020).

[16]GAO, *Defense Procurement, Ongoing DOD Fraud Risk Assessment Efforts Should Include Contractor Ownership,* GAO-20-106 (Washington, D.C.: Nov. 25, 2019).

[17]Pub. L. No. 116-283, Div. A, § 885, 134 Stat. 3388, 3791 (2021).

deceptive nature, programs can incur financial losses related to fraud that are never identified and such losses are difficult to reliably estimate. However, the most recent data available on recovered funds provide some indication of the scale of defense contracting fraud. These amounts were made available in DOD's response to a requirement of the NDAA for fiscal year 2018.[18] At that time, DOD reported to Congress that from fiscal years 2013 through 2017, over $6.6 billion had been recovered from defense contracting fraud cases, as shown in table 1.[19]

Table 1: Recovered Funds from Department of Defense (DOD) Contracting Fraud Cases from Fiscal Years 2013-2017, as Reported in 2018

	Number of DOD's contracting fraud cases resulting in monetary judgments	Amount of recoveries
Criminal Conviction	1,059	$792,226,115
Civil Judgments and Settlements	443	$5,858,180,290
Total	**1,502**	**$6,650,406,405**

Source: Department of Defense 2018 Report to Congress on Defense Contracting Fraud. | GAO-21-309

DOD also reported that, as a result of its criminal investigations, DOD OIG does not recommend specific penalties for contractors involved in fraud on contracts or other transactions. However, DOD OIG's audit and evaluation reports consistently recommend improvements in areas such as seeking refunds for contract overpayments and determining if DOD received fair and reasonable pricing, among other things. See appendix II for examples of contract management requirements, processes, and tools that may help DOD prevent, detect, and respond to fraud.

Fraud Risk Management

The objective of fraud risk management is to ensure program integrity by continuously and strategically mitigating the likelihood and effects of fraud. Effectively managing fraud risk helps to ensure that federal programs' services fulfill their intended purpose, that funds are spent effectively, and that assets are safeguarded. Executive-branch agency managers are responsible for managing fraud risks and implementing practices for combating those risks. The *Fraud Risk Framework* provides

[18]National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Div. A, § 889, 131 Stat. 1283, 1508 (2017).

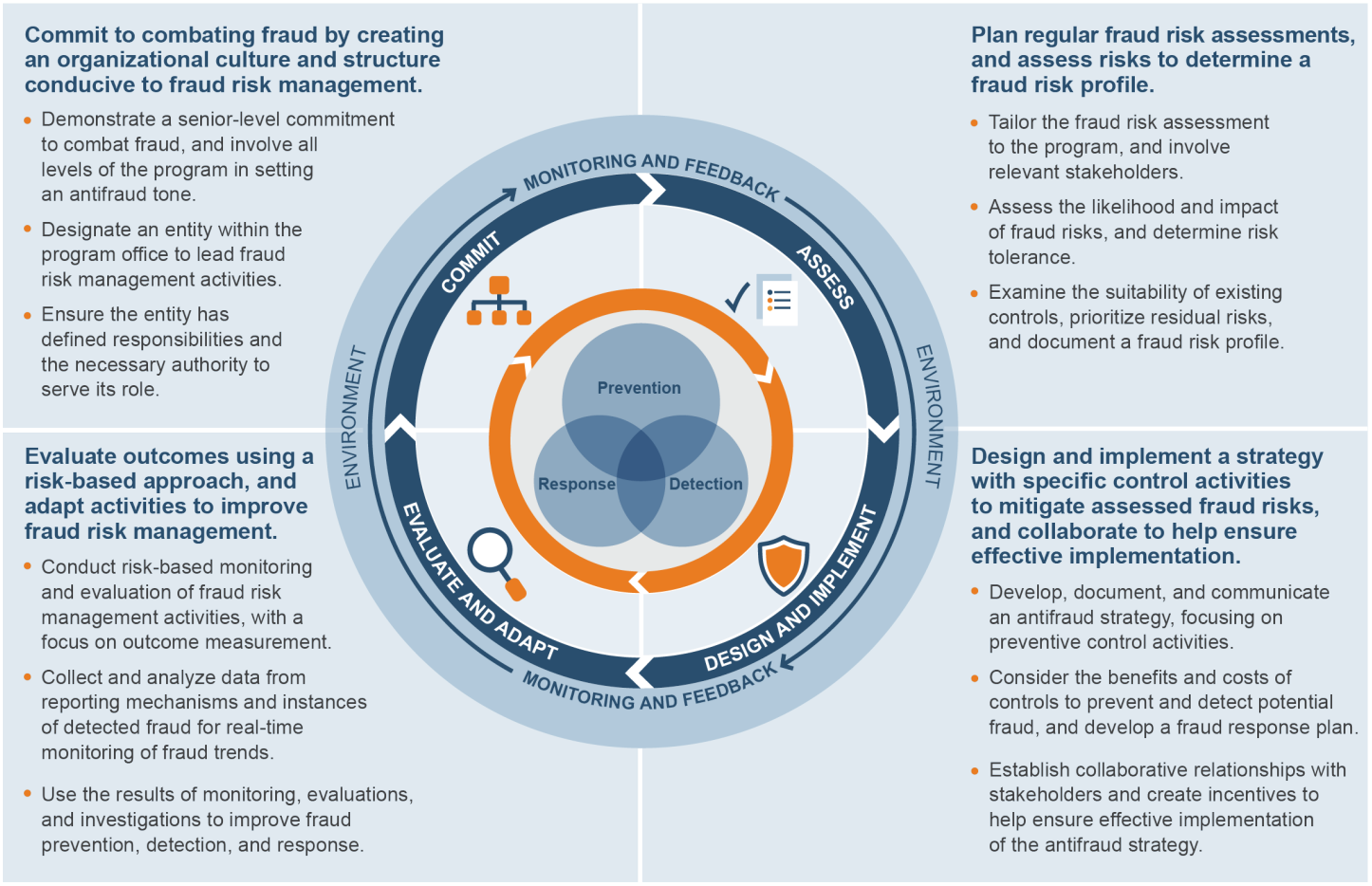
[19]Recovered funds include monies received in fines, penalties, restitution, and forfeiture of property in criminal convictions of fraud and also through civil judgments and settlements.

a comprehensive set of key components, overarching concepts, and leading practices that serve as a guide for agency managers to use when developing efforts to combat fraud in a strategic, risk-based way.[20] As required under the Fraud Reduction and Data Analytics Act of 2015 and its successor provisions in the Payment Integrity Information Act of 2019, the leading practices of the *Fraud Risk Framework* are incorporated into Office of Management and Budget's (OMB) guidelines and agency controls.[21] As depicted in figure 3, the Fraud Risk Framework describes leading practices within four components: commit, assess, design and implement, and evaluate and adapt.

[20]GAO-15-593SP.

[21]The Fraud Reduction and Data Analytics Act of 2015, enacted in June 2016, required OMB to establish guidelines for federal agencies to create controls to identify and assess fraud risks and to design and implement antifraud control activities. Pub. L. No. 114-186, 130 Stat. 546 (2016). The act further required OMB to incorporate the leading practices from the *Fraud Risk Framework* in the guidelines. Although the Fraud Reduction and Data Analytics Act of 2015 was repealed in March 2020, the Payment Integrity Information Act of 2019 requires these guidelines to remain in effect, subject to modification by OMB as necessary, and in consultation with GAO. Pub. L. No. 116-117, § 2(a), 134 Stat. 113, 131 - 132 (2020), codified at 31 U.S.C. § 3357.

Figure 3: The Four Components of the Fraud Risk Management Framework and Selected Leading Practices



Source: GAO. | GAO-21-309

Text of Figure 3: The Four Components of the Fraud Risk Management Framework and Selected Leading Practices

Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management. • Demonstrate a senior-level commitment to combat fraud, and involve all levels of the program in setting an antifraud tone. • Designate an entity within the program office to lead fraud risk management activities. • Ensure the entity has defined responsibilities and the necessary authority to serve its role.
Plan regular fraud risk assessments, and assess risks to determine a fraud risk profile. • Tailor the fraud risk assessment to the program, and involve relevant stakeholders. • Assess the likelihood and impact of fraud risks, and determine risk tolerance. • Examine the suitability of existing controls, prioritize residual risks, and document a fraud risk profile.

Design and implement a strategy with specific control activities to mitigate assessed fraud risks, and collaborate to help ensure effective implementation. • Develop, document, and communicate an antifraud strategy, focusing on preventive control activities. • Consider the benefits and costs of controls to prevent and detect potential fraud, and develop a fraud response plan. • Establish collaborative relationships with stakeholders and create incentives to help ensure effective implementation of the antifraud strategy.
Evaluate outcomes using a risk-based approach, and adapt activities to improve fraud risk management. • Conduct risk-based monitoring and evaluation of fraud risk management activities, with a focus on outcome measurement. • Collect and analyze data from reporting mechanisms and instances of detected fraud for real-time monitoring of fraud trends. • Use the results of monitoring, evaluations, and investigations to improve fraud prevention, detection, and response.

Source: GAO. | GAO-21-309

As mentioned above, the first component of the *Fraud Risk Framework*—commit—calls for program managers to commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management. This includes designating an antifraud entity to manage the fraud-risk assessment process. The second component—assess—calls for program managers to plan regular fraud risk assessments and provides leading practices for planning and conducting regular fraud risk assessments. This process includes identifying and assessing risks and documenting the results in the program's fraud risk profile.[22]

OMB plays a key role in issuing guidance to assist managers with combating government-wide fraud, waste, and abuse. In 2016, OMB established guidance for federal agencies' enterprise risk management, an approach for addressing the full spectrum of risks and challenges related to achieving the agencies' missions, in OMB's Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control.* This guidance requires executive agencies, including DOD, to:

- evaluate risks to accomplishing strategic, operations, reporting, and compliance objectives, and

[22]According to GAO's *Fraud Risk Framework,* a fraud risk profile is the summation of effectively assessing fraud risks. The profile includes the analysis of the types of internal and external fraud risks facing the program, their perceived likelihood and impact, managers' risk tolerance, and the prioritization of risks.

- provide an annual Statement of Assurance (SOA) that represents the agency head's informed judgment as to the overall adequacy and effectiveness of the agency's internal control.[23]

The Circular No. A-123 guideline further specifies that agencies should:

- adhere to the *Fraud Risk Framework's* leading practices as part of their efforts to effectively design, implement, and operate an internal control system that addresses fraud risks, and
- use GAO's *Federal Internal Control Standards* to annually evaluate the effectiveness of internal controls.[24]

DOD's Risk Management Internal Control (RMIC) Program

In 2013, in response to OMB's requirements for an annual SOA, DOD implemented its RMIC program. DOD's RMIC program culminates annually with a report on the design and effectiveness of key control activities compiled through components' SOA submissions.[25] According to DOD's 2020 *Agency Financial Report*, its RMIC program subsumes the responsibilities of the previous Enterprise Risk Management and Internal Control Program.[26] The Comptroller oversees the year-round RMIC program efforts by monitoring compliance to DOD Instruction 5010.40, which:

- establishes DOD's RMIC program,
- assigns responsibilities and prescribes procedures for the execution of the Managers' Internal Control Program within DOD,

[23]OMB required an annual statement of assurance starting in fiscal year 2006. See OMB, *Management's Responsibility for Internal Control,* Circular No. A-123 (Washington, D.C.: Dec. 21, 2004).

[24]The *Fraud Risk Framework* acknowledges that agencies may use initiatives like enterprise risk management efforts to assess their fraud risks, but the *Fraud Risk Framework* does not eliminate the separate and independent fraud risk management requirements.

[25]Formerly referred to as the Managers' Internal Control Program of the Department of Defense, Managers' Internal Control Program Procedures, DOD Instruction 5010.40 (Washington, D.C.: May 30, 2013).

[26]DOD, *Agency Financial Report: Fiscal Year 2020* (Washington, D.C.: Nov. 16, 2020).

- provides guidance for preparation and submission of the annual SOA to the Secretary of Defense, and
- instructs DOD managers to report annually on material weaknesses, which can affect financial audits and weaken safeguards against fraud, waste, and abuse.

To implement DOD Instruction 5010.40, the Comptroller issues the *SOA Execution Handbook* annually. This guidance:

- updates requirements to assist each component with its annual SOA submissions,
- focuses on the objective of obtaining an unqualified audit opinion,[27]
- instructs components to implement the *Fraud Risk Framework* as an integral part of risk management,
- provides guidance to assist components in balancing an internal controls program with risk management efforts that effectively and efficiently provide monitoring and oversight, and
- outlines assessment and reporting requirements for DOD officials at all levels, such as Senior Accountable Officials and their Action Officers, providing oversight and consistency in the identification of department-wide material weaknesses to strengthen the financial audit posture.[28]

DOD Has Taken Initial Steps to Combat Department-Wide Fraud Risks but Has Not

[27]An unqualified opinion is given when the auditor is reasonably assured that the financial statements are free of material misstatements.

[28]Senior Accountable Officials and their Action officers provide component level oversight for designated assessable units, including identification of department-wide material weaknesses, consider department-wide impact, and present recommendations to the Defense Business Council and Financial Improvement and Audit Remediation Governance Board. A material weakness is a deficiency, or combination of deficiencies, in internal controls over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

Finalized and Implemented a Comprehensive Approach

DOD took initial steps in fiscal year 2020 to combat department-wide fraud risks, and these steps generally align with *Fraud Risk Framework* leading practices; however, DOD has not finalized a comprehensive approach. Among the steps taken, DOD created a Fraud Reduction Task Force to prioritize fraud risks, but the task force's membership is incomplete. DOD has also used other risk management programs to meet new fraud risk assessment and reporting requirements, but the documentation of these requirements and stakeholder roles' and responsibilities has not been finalized.

DOD Has Taken Initial Steps to Demonstrate Commitment to Fraud Risk Management

The first component of the *Fraud Risk Framework—commit*—calls for managers to create an organizational culture to combat fraud at all levels of the agency and a structure with a dedicated entity to lead fraud-risk management activities. As a part of our assessment, we considered relevant leading practices. Specifically, we assessed whether DOD:

- Demonstrated senior-level commitment to integrity and combating fraud. As discussed in the *Fraud Risk Framework,* one way managers effectively manage fraud risks includes to develop, to document, and to communicate an antifraud strategy that describes the program's approach to combating fraud.
- Designated a dedicated entity that has defined responsibilities and the necessary authority across the program, serves as the repository of knowledge on fraud risks and controls, manages the fraud risk-assessment process, leads or assists with trainings and other fraud-awareness activities.[29]

In July 2020, the Comptroller's Office issued guidance that describes DOD's fraud-risk management approach, thereby providing an initial framework for combating fraud risks. The guidance, which generally aligns with *Fraud Risk Framework* leading practices, identifies a lead entity and some stakeholder roles and responsibilities. However, officials

Fraud Risk Framework Component

Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management

Source: GAO. | GAO-21-309

[29]GAO-15-593SP.

with the Comptroller's Office acknowledged to us that DOD's fraud-risk management efforts are in the infancy stage.

Specifically, DOD's July 2020 fraud-risk management guidance designated the Comptroller as the lead entity to oversee department-wide fraud-risk management activities.[30] The Comptroller's fraud-risk management roles and responsibilities include:

- Develop and maintain DOD's fraud-risk management documentation in compliance with applicable laws and regulations and serve as the repository for fraud controls and risks.
- Conduct an annual fraud-risk assessment process, including evaluation of component reported fraud risks to identify trends and risks that may have a department-wide effect, manage DOD's fraud risks, maintain its fraud risk profile, and support components in managing priority fraud risks.
- Lead the Chief Financial Officer's data analytics efforts for DOD and fraud risk management trainings, and co-lead the Fraud Reduction Task Force.

In its July 2020 guidance, DOD also demonstrated commitment to combating fraud by identifying stakeholder roles and responsibilities throughout the department. Fraud-risk management stakeholders include:

Chief Management Officer Position Repealed

The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 repealed the position of the Chief Management Officer of the Department of Defense (DOD) effective January 1, 2021.[a] In January 2021, the Secretary of Defense delegated responsibility for improving accountability and performance in the DOD to the Comptroller. In February 2021, officials from the Comptroller's office told us that they are in the process of determining how to implement these new responsibilities and that there is not an implementation timeframe. In March 2021 Comptroller officials told us these responsibilities include fraud risk management.

[30]These responsibilities are assigned to three Comptroller Offices, specifically to: (1) the Office of the Deputy Chief Financial Officer, (2) the Financial Improvement and Audit Readiness Directorate, and (3) the Chief Financial Officer Data Transformation Office.

For the purposes of this report, we discuss the Chief Management Officer's roles and responsibilities related to DOD's fraud risk management through 2020. We did not assess the effect of the repeal of the Chief Management Officer position on DOD's fraud risk management efforts.

Source: GAO. | GAO-21-309

[a]Pub. L. No. 116-283, Div. A, § 901, 134 Stat. 3388, 3794 (2021).

- **The Financial Improvement and Audit Readiness Governance Board** is a cross-component senior management council—co-chaired by the Comptroller and the former Chief Management Officer—that serves as the Risk Management Council. It facilitates discussion at the enterprise level on priority fraud-risk focus areas and oversees all assessments of fraud risks and internal controls.[31]
- **The Chief Management Officer,** prior to this position's repeal in 2021, collaborated with the Comptroller to support DOD leadership in determining how to best address department-wide risks and allocate resources to mitigate those risks (see side bar). The Chief Management Officer also incorporated prioritized fraud risks in DOD's Enterprise Risk Management risk register and risk profile. The Comptroller and Chief Management Officer co-chaired the Financial Improvement and Audit Readiness Governance Board, among other things. According to DOD's fiscal year 2020 *SOA Execution Handbook,* the Chief Management Officer and the Comptroller also served as the oversight bodies for DOD's RMIC Program, which included providing guidance for the annual SOA via policies, training, tools, and templates.
- **Fraud Reduction Task Force,** which was established in February 2020, includes subject matter experts and senior leaders from relevant components to reduce fraud risk determined to be high priority across components. The Task Force—co-led by the Comptroller and Chief Management Officer before its repeal in 2021—is to review and approve high-priority risks consolidated and categorized by the Comptroller and commits resources to improve fraud controls. See further discussion below.
- **Components**—which may include Military Departments, Defense agencies, DOD Field Activities, and Combatant Commands—are to implement the fraud-risk-management guidance. They are also to report to the Comptroller (and, prior to its elimination, the Chief Management Officer) on aggregated fraud risk assessment and fraud control assessments results that may have a department-wide effect.
- **Principal Staff Assistants** are subject matter experts in specific program areas, such as acquisitions. These experts are able to identify and communicate fraud schemes and trends to the

[31]The Financial Improvement and Audit Readiness Governance Board provides vision, leadership, oversight, and accountability for DOD's effort to achieve full financial auditability, in line with congressional mandates, including the Federal Financial Management Improvement Act of 1996 and GPRA Modernization Act of 2010.

Comptroller, Chief Management Officer (prior to its elimination), and the Fraud Reduction Task Force.[32] For example, officials within the Comptroller's Office told us they partner with the Under Secretary of Defense for Acquisition and Sustainment's office, which has experts in contracting, to discuss procurement fraud risks. The officials also said that Acquisition and Sustainment works across DOD components to identify and mitigate contracting risks. According to DOD's fiscal year 2020 *SOA Execution Handbook*, Principal Staff Assistants are to coordinate and meet at least quarterly with Components to review and prioritize identified risks and internal control evaluation results.

Membership of DOD's Fraud Reduction Task Force Is Incomplete

In February 2020, DOD's Deputy Chief Financial Officer issued a memorandum forming the Fraud Reduction Task Force. According to the memorandum and July 2020 guidance, the Task Force is intended to:

- support establishing and implementing DOD's fraud risk management approach, including review and approval of high priority risks consolidated and categorized by the Comptroller;
- develop internal controls for business activities that present the highest potential for fraud, help make fraud risk management a priority, sustain program integrity, and ensure mission accomplishment; and
- help design and implement activities for a successful fraud-risk management program, including conducting analytics to understand the scope of the fraud risks, such as likelihood and potential impact, and implementing activities to reduce fraud.

According to DOD's July 2020 fraud-risk-management guidance, the Comptroller's Office is also to share priority risk categories with the Task Force for review and approval before they are included in DOD's risk profile and considered for DOD's Enterprise Risk Management risk profile. Officials within the Comptroller's Office told us the Task Force reviews high priority risks to corroborate, not approve, the Comptroller's categorization. These officials also told us they plan to clarify the Task

[32]The Principal Staff Assistants are the Under Secretaries of Defense; the DOD Deputy Chief Management Officer; the General Counsel of DOD; the Inspector General of DOD; and those Assistant Secretaries of Defense, Assistants to the Secretary of Defense, and Office of the Secretary of Defense Directors, and equivalents who report directly to the Secretary or Deputy Secretary of Defense.

Force's roles in the fiscal year 2022 update of DOD's fraud-risk-management documentation.

A year after its formation, the Task Force's membership remains incomplete. When the Task Force was announced on February 18, 2020, DOD requested that components identify representatives by February 25, 2020. According to the DOD memorandum, the component representative must be able to provide subject matter expertise to help shape and strengthen fraud analysis tests and corrective actions to significantly reduce fraud, among other tasks. Members of the Task Force include officials from the RMIC program, auditors, accounting and finance, as well as management and program analysts and budget analysts.[33] We initially determined that as of August 2020, 26 of 59 components had not designated a representative for the Task Force, including 2 of the 6 components we selected—the Air Force and Army. In September 2020, the Air Force's policy and contracting-oversight officials told us they were aware of the Task Force and were looking into how they can contribute. However, in October 2020, these officials told us they were unaware of an Air Force official designated to serve as Task Force representative. The Army's policy and contracting-oversight officials we met with in April 2020 stated that they were unaware of the Task Force.

In October 2020, Comptroller officials told us the Task Force was in the initial stages of piloting department-wide data analytics efforts assessing timecard and purchase card fraud. In January 2021, officials within the Comptroller's Office told us that participation in the Task Force by the components was voluntary during its first year of implementation. In February 2021, these officials explained that the voluntary status was due to delays they experienced distributing DOD's July 2020 fraud-risk-management guidance. However, the officials could not provide documentation indicating that Task Force participation was voluntary. Officials within the Comptroller's Office told us they do not have concerns about components not participating during the first year of the Task Force, although they said they are taking steps to better ensure participation. For example, these officials told us they plan to include the requirement for components to identify a Task Force representative in the fiscal year 2021 *SOA Execution Handbook*. However, Comptroller

[33]In January 2021, Comptroller officials told us that the Task Force is a high-level position with members who have a broad reach in their components to assist with fraud risk efforts. These officials told us they meet informally with the Task Force every 2 weeks.

officials also told us that issuance of this guidance is on hold due to the recent repeal of the Chief Management Officer's position.[34]

Filling Task Force vacancies would further strengthen DOD's ability to effectively prioritize fraud risk management. As of February 2021, membership on the Task Force had increased but remained incomplete. According to documentation provided by the Comptroller, 11 of the 59 components had not designated a representative. Comptroller officials told us they are working with the remaining components, including the Army, to identify representatives. The Army, 1 of our 6 selected components, accounts for 24 percent ($100.1 billion) of DOD's fiscal year 2020 obligations.

DOD Incorporated Fraud Risk Requirements in Its Risk Management Program, but Policy and Guidance Are Inconsistent with Relevant Federal Fraud-Reporting Requirements

DOD incorporated fraud risk assessment and reporting requirements in guidance but thresholds are inconsistent with federal fraud-reporting requirements. DOD has also not fully updated related policy, resulting in inconsistencies between policy and guidance. Additionally, DOD officials explained that they share information with oversight officials—Department-wide Assessable Unit Senior Accountable Officials, their Action Officers, and the Defense Business Council—but that process has not been documented.

DOD Uses Its Risk Management Program to Assess and Report Fraud Risks, but Inconsistencies in Governing Policy and Implementing Guidance Remain

[34]In March 2021, DOD issued its fiscal year 2021 *SOA Execution Handbook*, which requires components to identify a Task Force representative. An assessment of the fiscal year 2021 *SOA Execution Handbook* is outside of the scope of this report.

Trade-offs for Risk Management and Internal Control and Antifraud Approaches

The Fraud Risk Framework recognizes that agencies have flexibility in how they set up their antifraud activities and structures, and that fraud-risk-management activities may be incorporated or aligned with other program-risk-management activities. However, integrating antifraud efforts into a broader risk management and internal control approach may pose trade-offs. This structure may provide a broad view of potentially aberrant behaviors from unintentional errors to sophisticated bribery or corruption schemes, which could inform the development of control activities that serve multiple risk management and internal functions, including fraud risk management. However, without careful planning, integrating fraud risk management into a larger risk management and internal control approach could limit the amount of resources and attention focused specifically on fraud prevention, detection, and response. Additionally, fraud's deceptive nature makes it harder to detect potentially requiring control activities that are specifically designed to prevent and detect criminal intent.

Source: GAO. | GAO-21-309

DOD uses its RMIC program to collect information from DOD components to meet relevant executive agency requirements, such as those contained in OMB Circular No. A-123. DOD Instruction 5010.40 addresses these requirements and identifies responsibilities for the Comptroller and DOD components, among others. As mentioned above, the Comptroller is responsible for ensuring adherence to annual-reporting requirements and issuing guidance for proper execution of DOD's RMIC program, such as DOD's annual *SOA Execution Handbook*.

Policy. DOD Instruction 5010.40 establishes RMIC program structure and requirements for DOD and components to identify, assess, and report on the effectiveness of internal controls.[35] As discussed above, OMB Circular No. A-123 requires executive agencies, in this case DOD, to evaluate risks to accomplishing strategic, operations, reporting, and compliance objectives and to provide an annual SOA.

To meet these requirements, DOD uses its RMIC program, which it also uses to meet financial-reporting requirements (see sidebar).[36] The Instruction assigns implementation responsibilities to DOD components. In March 2021, Comptroller officials told us that based on their interpretation of the OMB Circular No. A-123's reporting requirement, components must include all fraud risks regardless of a risk's materiality or weakness as part of their SOA. However, Instruction 5010.40 does not direct the components to include all fraud risks as part of their SOAs. Instead, the instruction requires that DOD components report significant

[35]According to DOD Instruction 5010.40, DOD and components must establish a RMIC program with three distinct internal control assessments: (1) operations, (2) financial reporting, and (3) financial systems to assess inherent risks in mission-essential processes, among other things. Department of Defense, *Managers' Internal Control Program Procedures,* DOD Instruction 5010.40 (Washington, D.C., May 30, 2013) (Incorporating Change 1, effective June 30, 2020). According to DOD's Fiscal Year 2020 *Agency Financial Report*, its RMIC program holds both operational and financial managers accountable for ensuring they are effectively managing risks and internal controls in their areas of responsibility.

[36]Since 1995, GAO has designated DOD financial management as high risk because of pervasive deficiencies in the department's financial management systems, business processes, internal controls, and financial reporting. These deficiencies have adversely affected DOD's ability to prepare auditable financial statements, and this lack of ability is one of three major impediments preventing us from expressing an audit opinion on the U.S. government's consolidated financial statements.

deficiencies and material weaknesses in internal controls that weaken fraud safeguards in their SOAs, among others.

Guidance. The Comptroller and the Chief Management Officer had oversight roles for the fiscal year 2020 SOA process and were responsible for updating the corresponding *SOA Execution Handbook.* Specifically, the *SOA Execution Handbook* identifies program requirements, including fraud risks, and stakeholder roles and responsibilities. Further, the Comptroller and the Chief Management Officer updated DOD's fiscal year 2020 *SOA Execution Handbook* guidance to include a requirement for components to conduct fraud risk assessments, including identifying, assessing, and reporting procurement fraud risks. However, the *SOA Execution Handbook* does not direct the components to report all fraud risks identified in these assessments as part of their SOAs. Instead, the *SOA Execution Handbook* requires that components report significant deficiencies and material weaknesses identified in their risk and internal control assessments. The Comptroller's Office explained that this reporting requirement is related to material weaknesses collected for the SOA process and does not pertain to the fraud risk assessment that components conduct. However, the *SOA Execution Handbook* is not clear that this reporting requirement is not applicable to component's fraud risk assessments.

The *SOA Execution Handbook* also prioritizes remediating material weaknesses and improving financial management; this process includes a risk-based approach that focuses on the remediation of audit findings aligned to the audit priority areas and the sustainment of business process improvements to advance the achievement of a clean audit opinion. As mentioned above, integrating fraud risk management into a larger risk-management and internal-control approach can pose trade-offs without careful planning. Specifically, this approach could limit the amount of resources and attention focused specifically on fraud prevention, detection, and response, such as fraud risks that are not material weaknesses or significant deficiencies. See discussion of selected components' fraud risk assessments below.

According to DOD's fiscal year 2016 SOA guidance, the Comptroller's Office planned to update DOD Instruction 5010.40 to incorporate relevant OMB Circular No. A-123 and *Federal Internal Control Standards* requirements. In February 2019, officials within the Comptroller's office told us the Instruction 5010.40 was being updated to reflect OMB Circular No. A-123 fraud-risk-reporting requirements. In October and December 2020, officials within the Comptroller's and Chief Management Officer's

offices further told us they were collaborating to update that Instruction and the fiscal year 2021 *SOA Execution Handbook* to reflect fraud-risk-reporting requirements and that the draft documents were under internal review.

As of March 2021, Comptroller officials had not updated DOD Instruction 5010.40 to explicitly include fraud-risk-reporting standards and distinguish them from financial reporting requirements. Comptroller officials explained that the recent repeal of the Chief Management Officer's position and reassignment of its responsibilities has halted issuance of the instruction.[37] These officials told us their leadership is determining how to reassign the Chief Management Officer's responsibilities and do not have an issuance timeline for DOD Instruction 5010.40. Under DOD's current approach, components may not be reporting all fraud risks, including those that are not categorized as a material weakness or significant deficiency, because the current policy and guidance does not explicitly state that they are required to do so.

Federal Internal Control Standards' Principle 12 states that management should implement control activities through policies. Specifically, documentation of responsibilities through policies and periodic review of control activities contribute to the design, implementation, and operating effectiveness of control activities. In addition, *Federal Internal Control Standards'* Principle 1 requires the oversight body (in this case the Comptroller) and management to reinforce the commitment to doing what is right, not just maintaining a minimum level of performance necessary to comply with applicable laws and regulations, so that these priorities are understood by all stakeholders, such as regulators, employees, and the general public.

Without policies and guidance that explicitly state that a component's fraud risk assessment must include all fraud risks regardless of materiality, DOD's design, implementation, and operating effectiveness of control activities may be limited. For example, fraud risk identification may be incomplete; risk responses may be inappropriate; control activities may not be appropriately designed or implemented; information and communication may falter; and results of monitoring may not be understood or acted upon to remediate deficiencies and fraud risks.

[37]In March 2021, DOD issued its fiscal year 2021 *SOA Execution Handbook*, which noted it is in the process of revising DOD Instruction 5010.40. An assessment of the fiscal year 2021 *SOA Execution Handbook* is outside of the scope of this report.

DOD Shares Information with Internal Control Oversight Officials but Does Not Reference Them in Its Fraud Risk Management's Documentation

Officials within the Comptroller's Office told us they share fraud risk information with department-wide RMIC oversight officials—including department-wide Assessable Unit Senior Accountable Officials, Action Officers, and the Defense Business Council—to keep stakeholders informed of risk management activities to enhance department-wide progress. However, the roles and responsibilities for these officials are not referenced in DOD's July 2020 fraud-risk-management guidance. Comptroller officials noted that this omission is to ensure Assessable Unit Senior Accountable Officials and their Action Officers are able to support remediating department-wide financial audit material weaknesses, not necessarily fraud risks. These officials explained they have not yet determined what the Defense Business Council's roles and responsibilities should be. Figure 4 illustrates selected roles and responsibilities of stakeholders involved in DOD's fraud risk management activities, including stakeholders not referenced in program documentation, as well as examples of related responsibilities identified during our review of DOD documentation.

Figure 4: Selected Roles and Responsibilities of Stakeholders Engaged in Department of Defense's (DOD) Fraud Risk Management Activities as of Fiscal Year 2020

Designated Lead DOD Fraud Risk Management Oversight Entity	**Under Secretary of Defense Comptroller/Chief Financial Officer (the Comptroller)**	Leads DOD's Fraud Risk Management activities, provides guidance to components, and incorporates fraud risks in DOD's fraud risk register and prioritized fraud risks in its risk profile. Manages DOD fraud risks via the Fraud Risk Management program, serves as a repository of fraud risk and controls knowledge, and leads Chief Financial Officer data analytics efforts and supports effort to streamline analytics department-wide.	$
Department-wide Fraud Risk Management Stakeholders	**Chief Management Officer[a]**	Led DOD's Enterprise Risk Management activities, including incorporating prioritized fraud risks in DOD's Enterprise Risk Management risk register and risk profile.	⚙$
	Financial Improvement and Audit Remediation Governance Board	Cross-component council that that oversees financial audit remediation related to internal control over financial reporting and financial systems and shares information on prioritized fraud risks, controls, and remediation.	$
	Financial Improvement and Audit Remediation Committee	Cross-component leadership group that advises and makes recommendations to the Chief Management Officer and Comptroller to prioritize, integrate, and manage efforts to improve financial management and achieve audit readiness.	$
	Principal Staff Assistants	Implements DOD's Fraud Risk Management guidance and reports identified fraud schemes and trends to the Fraud Reduction Task Force, Comptroller, and Chief Management Officer.	👤
	Fraud Reduction Task Force	Cross-component team of subject-matter experts and senior leaders who lead DOD's analytics activities for high-priority fraud risks.	🔍
Department-wide Risk Management Internal Control Oversight Officials	**Department-wide Assessable Unit Senior Accountable Officials and Action Officers**	Provides component level oversight for designated assessable unit, including identification of department-wide material weaknesses, considers DOD impact, and presents recommendations to the Defense Business Council and Financial Improvement and Audit Remediation Governance Board	⚠
	Defense Business Council	Governance body that oversees operational audit remediation related to internal controls over operations, including non-financial systems; and vets issues related to management, improvement of defense business operations, and other issues.	⚠
Component Fraud Risk Management Stakeholders	**Component Risk Management Internal Control Coordinator and Program Managers**	Identifies fraud risks, implements adequate controls, reports aggregated fraud risk assessment results that may have a department-wide impact to the Comptroller, and coordinates with the Fraud Reduction Task Force, Chief Management Officer, and Comptroller on the review and mitigation of potential fraud cases	👤$

$ Authority related to financial reporting and systems

⚙ Authority related to business operations and internal controls

👤 Subject matter experts in specific program areas

🔍 Senior assessment team

👤$ Officials from component level financial and program offices

⚠ Entity with internal control program oversight responsibilities that is omitted from DOD's fraud risk management documentation

Source: GAO analysis of DOD information. | GAO-21-309

Text of Figure 4: Selected Roles and Responsibilities of Stakeholders Engaged in Department of Defense's (DOD) Fraud Risk Management Activities as of Fiscal Year 2020

	Stakeholder	Responsibility	Role
Designated Lead DOD Fraud Risk Management Oversight Entity	Under Secretary Of Defense/Chief Financial Officer (the Comptroller)	Leads DOD's Fraud Risk Management activities, provides guidance to components, and incorporates fraud risks in DOD's fraud risk register and prioritized fraud risks in its risk profile. Manages DOD fraud risks via the Fraud Risk Management program, serves as a repository of fraud risk and controls knowledge, and leads Chief Financial Officer data analytics efforts and supports effort to streamline analytics department-wide.	Authority related to financial reporting and systems
Department-wide Fraud Risk Management Stakeholders	Chief Management Officer[a]	Led DOD's Enterprise Risk Management activities, including incorporating prioritized fraud risks in DOD's Enterprise Risk Management risk register and risk profile.	Authority related to business operations and internal controls
Department-wide Fraud Risk Management Stakeholders	Financial Improvement and Audit Remediation Governance Board	Cross-component council that that oversees financial audit remediation related to internal control over financial reporting and financial systems and shares information on prioritized fraud risks, controls, and remediation.	Authority related to financial reporting and systems
Department-wide Fraud Risk Management Stakeholders	Financial Improvement and Audit Remediation Committee	Cross-component leadership group that advises and makes recommendations to the Chief Management Officer and Comptroller to prioritize, integrate, and manage efforts to improve financial management and achieve audit readiness.	Authority related to financial reporting and systems
Department-wide Fraud Risk Management Stakeholders	Principal Staff Assistants	Implements DOD's Fraud Risk Management guidance and reports identified fraud schemes and trends to the Fraud Reduction Task Force, Comptroller, and Chief Management Officer.	Subject matter experts in specific program areas
Department-wide Fraud Risk Management Stakeholders	Fraud Reduction Task Force	Cross-component team of subject-matter experts and senior leaders who lead DOD's analytics activities for high-priority fraud risks.	Senior assessment team
Department-wide Risk Management Internal Control Oversight Officials	Department-wide Assessable Unit Senior Accountable Officials and Action Officers	Provides component level oversight for designated assessable unit, including identification of department-wide material weaknesses, considers DOD impact, and presents recommendations to the Defense Business Council and Financial Improvement and Audit Remediation Governance Board	Entity with internal control program oversight responsibilities that is omitted from DOD's fraud risk management documentation
Department-wide Risk Management Internal Control Oversight Officials	Defense Business Council	Governance body that oversees operational audit remediation related to internal controls over operations, including non-financial systems; and vets issues related to management, improvement of defense business operations, and other issues.	Entity with internal control program oversight responsibilities that is omitted from DOD's fraud risk management documentation
Component Fraud Risk Management Stakeholders	Component Risk Management Internal Control Coordinator and Program Managers	Identifies fraud risks, implements adequate controls, reports aggregated fraud risk assessment results that may have a department-wide impact to the Comptroller, and coordinates with the Fraud Reduction Task Force, Chief Management Officer, and Comptroller on the review and mitigation of potential fraud cases	Officials from component level financial and program offices

Source: GAO analysis of DOD information. | GAO-21-309

[a]The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 repealed the position of the Chief Management Officer of the DOD in January 2021. Pub. L. No. 116-283, Div. A, § 901, 134 Stat. 3388, 3794 (2021). DOD officials told us the Chief Management Officer's fraud-risk-assessment responsibilities are currently being re-assigned.

Assessable Unit Senior Accountable Officials and Action Officers. Comptroller officials told us that high priority risk areas, including fraud risks, are shared with department-wide Assessable Unit Senior Accountable Officials and their Action Officers. Comptroller officials explained that high priority risk areas are used to keep stakeholders informed of risk management activities to enhance department-wide progress. The roles and responsibilities for these officials are not articulated in DOD's fraud-risk management documentation, however. Officials within the Comptroller's Office told us that they did not identify roles and responsibilities in the fraud-risk-management documentation for Senior Accountable Officials and their Action Officers for two reasons. First, officials told us that their current priority is ensuring Senior Accountable Officials and their Action Officers are able to support remediating department-wide financial audit material weaknesses, not necessarily fraud risks. Second, officials within the Comptroller's Office explained they do not want to place too many responsibilities on Senior Accountable Officials and their Action Officers.

Comptroller officials further explained they are formalizing a new process that would enable them to engage with Senior Accountable Officials and their Action Officers throughout the year to address and track material weaknesses. Comptroller officials also told us they plan to release guidance for Senior Accountable Officials' roles and responsibilities in fiscal year 2021 and later include department-wide Senior Accountable Officials and their Action Officers in the fraud-risk management structure. Officials explained they do not have a specific date when these officials will be incorporated in the fraud-risk management process, a process that depends on the adoption and effectiveness of the Senior Accountable Officials and Action Officers in supporting the fiscal year 2021 RMIC process.

Defense Business Council. In December 2020, officials within the Chief Management Officer's office told us that business operations fraud risks were shared with the Defense Business Council for prioritization. This includes the Defense Business Council's providing input on which risks the Chief Management Officer escalated to the Financial Improvement

and Audit Readiness Governance Board.[38] These officials also told us they planned to work with the Defense Business Council to develop criteria for elevating high risks and how to share this information. Officials within the Comptroller's Office also told us that they had not identified roles and responsibilities in its fraud risk management documentation for the Defense Business Council because they had not yet determined what those roles and responsibilities should be. Officials told us they were collaborating with the Chief Management Officer to determine the role of the Defense Business Council within the SOA and risk assessment process. However, as mentioned above, the repeal of the Chief Management Officer's position has placed these efforts and guidance on hold.

Officials within the Comptroller's Office told us no decisions or guidance have been shared concerning its new role as Co-chair and sharing high priority risk areas, including fraud risks, with the Defense Business Council. These officials told us that they are awaiting guidance from their leadership on how to implement their new responsibilities and determine the effect on the Defense Business Council's role in DOD's fraud risk management. These officials told us there is no timeframe for the release of the guidance on implementing their new responsibilities resulting from the repeal of the Chief Management Officer position.

DOD's fraud-risk-management approach has a direct-reporting line to senior level managers within the agency, an approach that generally aligns with the *Fraud Risk Framework* leading practice.[39] However, DOD's fraud-risk-management documentation does not reference the department-wide Assessable Unit Senior Accountable Officials, their Action Officers, and the Defense Business Council. As such, the

[38]The Defense Business Council is the senior management council for implementing the Secretary's Management Agenda and vetting issues related to management, including oversight of operational audit remediation related to internal controls over operations and non-financial systems. Members consist of the Under Secretary of Defense for Acquisition, Technology, and Logistics; Under Secretary of Defense for Policy; the Comptroller; Under Secretary of Defense for Personnel and Readiness; Under Secretary of Defense for Intelligence; Director, Cost Assessment and Program Evaluation; Joint Staff; and each Military Services' Deputy Chief Management Officer and Chief Information Officer. DOD's Chief Information Officer and Chief Management Officer co-chaired the Defense Business Council, prior to its repeal in 2021. The Secretary of Defense's January 11, 2021, memorandum delegated the Comptroller as new co-chair of the Defense Business Council.

[39]GAO-15-593SP.

documentation does not align with *Federal Internal Control Standards.* Specifically, Principle 2 of the *Federal Internal Control Standards* requires the oversight body, in this case the Comptroller, to work with key stakeholders to understand their expectations and help the entity fulfill these expectations if appropriate. Further, Principle 3 requires management to establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives and also develop and maintain documentation of its internal control system.

Documentation provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors.[40] Documenting the roles and responsibilities of department-wide Assessable Unit Senior Accountable Officials and their Action Officers and the Defense Business Council could enhance the Comptroller's ability to ensure these stakeholders understand their responsibilities and the chain of accountability, use high priority risk areas to strategize at the department level, and remain informed of risk management activities to enhance department-wide progress.

[40]GAO-14-704G.

DOD Has Taken Steps to Conduct a Fraud Risk Assessment, but Some Components Did Not Report Procurement Fraud Risks

DOD Provides Guidance, Tools, and Training for Components to Conduct Fraud Risk Assessments and to Assess Procurement Fraud Risks

Fraud Risk Framework Component:
Plan regular fraud risk assessments and assess risks to determine a fraud risk profile

Source: GAO. | GAO-21-309

The second component of the *Fraud Risk Framework*—assess—calls for federal managers to plan regular fraud risk assessments and to assess risks to determine a fraud risk profile. Specifically, leading practices include tailoring the fraud risk assessment to the program and planning to conduct the assessment at regular intervals. The leading practices also include identifying the tools and data on fraud schemes and involving relevant stakeholders.[41]

The *SOA Execution Handbook* addresses how DOD components are to conduct fraud risk assessments. The guidance in the *SOA Execution Handbook* for how to plan and conduct regular fraud risk assessments generally aligns with leading practices. For instance, the Comptroller and the Chief Management Officer provided oversight on the SOA process, policy guidance, tools, and information for components' use in the risk assessment process, and training.

Oversight. The Comptroller and the Chief Management Officer had oversight roles for the annual SOA process for fiscal year 2020. Officials from the Comptroller's Office consolidated reported risks from the components' fraud risk assessments and updated the Department-wide fraud risk profile. The Chief Management Officer incorporated fraud risks prioritized by the Comptroller into DOD's enterprise-risk-management "risk register" and fraud risk profile.[42] The Chief Management Officer collaborated with the Comptroller to mitigate DOD risks and allocate

[41]GAO-15-593SP.

[42]A "risk register" documents identified risks, often grouped by type or category (e.g., reputational, program, operational, etc.), and helps managers see how risks relate to relevant strategic objectives. According to GAO's *Fraud Risk Framework,* a fraud risk profile is the summation of effectively assessing fraud risks. The profile includes the analysis of the types of internal and external fraud risks facing the program, their perceived likelihood and effect, managers' risk tolerance, and the prioritization of risks.

resources, as appropriate. See figure 5 below for the department-wide fraud-risk-assessment review process.

Figure 5: Department of Defense's (DOD) Fraud Risk Assessment Review Process for Fiscal Year 2020

DOD's fraud risk assessment (FRA) review process		DOD entities involved			
		Components	Office of the Under Secretary of Defense Comptroller (the Comptroller)	Fraud Reduction Task Force (FRTF)	Office of the Chief Management Officer (OCMO)[a]
Complete the FRA	Components report fraud risks identified in highly susceptible areas in their programs and processes to the Comptroller and OCMO using DOD's FRA.	✓	✓		✓
Consolidate risk	The Comptroller reviews the risks submitted by components, aggregates, re-categorizes, revises risk language for clarity and consistency, and groups risks by category.		✓		
Assesses and assign subjective impact and likelihood levels to each risk category	The Comptroller assesses and assigns subjective impact and likelihood measures by risk category to be included in the DOD fraud risk profile and also assigns risk levels.		✓		
Review and approve high risk categories	The priority risk categories identified are presented to the agency leadership for review and approval. The cross-component FRTF approves the priority risks and commits resources to develop action plans for mitigating identified fraud risks.			✓	
Identify opportunities to develop analytics	OCMO and the Comptroller coordinate with the FRTF and components to identify data sources and analytics. Once analytics are developed, OCMO and the Comptroller coordinate with the FRTF and components, as needed, to review and refine analytics tests.	✓	✓	✓	✓
Update and communicate risk profile	The results of the FRA are consolidated into DOD's Fraud Risk Profile. The fraud risks are escalated to the OCMO for consideration for the DOD Enterprise Risk Management Risk Profile.	✓	✓	✓	✓

✓ Involved in DOD's fraud risk management review process

Source: GAO analysis of DOD information. | GAO-21-309

Data table for Figure 5: Department of Defense's (DOD) Fraud Risk Assessment Review Process for Fiscal Year 2020

		DOD entities involved			
	DOD's fraud risk assessment (FRA) review process	**Components**	**Office of the Under Secretary of Defense Comptroller (The Comptroller)**	**Fraud Reduction Task Force (FRTF)**	**Office of the Chief Management Officer (OCMO)[a]**
Complete the FRA	Components report fraud risks identified in highly susceptible areas in their programs and processes to the Comptroller and OCMO using DOD's FRA.	Involved in DOD's fraud risk management review process	Involved in DOD's fraud risk management review process		Involved in DOD's fraud risk management review process
Consolidate risk	The Comptroller reviews the risks submitted by components, aggregates, re-categorizes, revises risk language for clarity and consistency, and groups risks by category.		Involved in DOD's fraud risk management review process		
Assesses and assign subjective impact and likelihood levels to each risk category	The Comptroller assesses and assigns subjective impact and likelihood measures by risk category to be included in the DOD fraud risk profile and also assigns risk levels.		Involved in DOD's fraud risk management review process		
Review and approve high risk categories	The priority risk categories identified are presented to the agency leadership for review and approval. The cross-component FRTF approves the priority risks and commits resources to develop action plans for mitigating identified fraud risks.			Involved in DOD's fraud risk management review process	

	DOD entities involved				
	DOD's fraud risk assessment (FRA) review process	**Components**	**Office of the Under Secretary of Defense Comptroller (The Comptroller)**	**Fraud Reduction Task Force (FRTF)**	**Office of the Chief Management Officer (OCMO)[a]**
Identify opportunities to develop analytics	OCMO and the Comptroller coordinate with the FRTF and components to identify data sources and analytics. Once analytics are developed, OCMO and the Comptroller coordinate with the FRTF and components, as needed, to review and refine analytics tests.	Involved in DOD's fraud risk management review process	Involved in DOD's fraud risk management review process	Involved in DOD's fraud risk management review process	Involved in DOD's fraud risk management review process
Update and communicate risk profile	The results of the FRA are consolidated into DOD's Fraud Risk Profile. The fraud risks are escalated to the OCMO for consideration for the DOD Enterprise Risk Management Risk Profile.	Involved in DOD's fraud risk management review process	Involved in DOD's fraud risk management review process	Involved in DOD's fraud risk management review process	Involved in DOD's fraud risk management review process

Source: GAO analysis of DOD information. | GAO-21-309

[a]The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 repealed the position of Chief Management Officer of the DOD effective January 1, 2021. Pub. L. No. 116-283, Div. A, § 901, 134 Stat. 3388, 3794 (2021). The Deputy Secretary of Defense's January 11, 2021, memorandum delegated the Comptroller responsible for improving accountability and performance in DOD business operations. DOD officials told us that the Chief Management Officer's fraud-risk-assessment responsibilities, as noted in Figure 5 above, are currently being assigned. In March 2021, Comptroller officials told us they are assuming the Chief Management Officer's business operations responsibilities and these responsibilities will include fraud risk-management responsibilities.

The Comptroller uses input collected from the components' fraud risk assessments to develop and maintain DOD's fraud risk profile. Officials within the Comptroller's Office told us they were very dependent upon the SOA process as the initial indicator of identified risks from components.

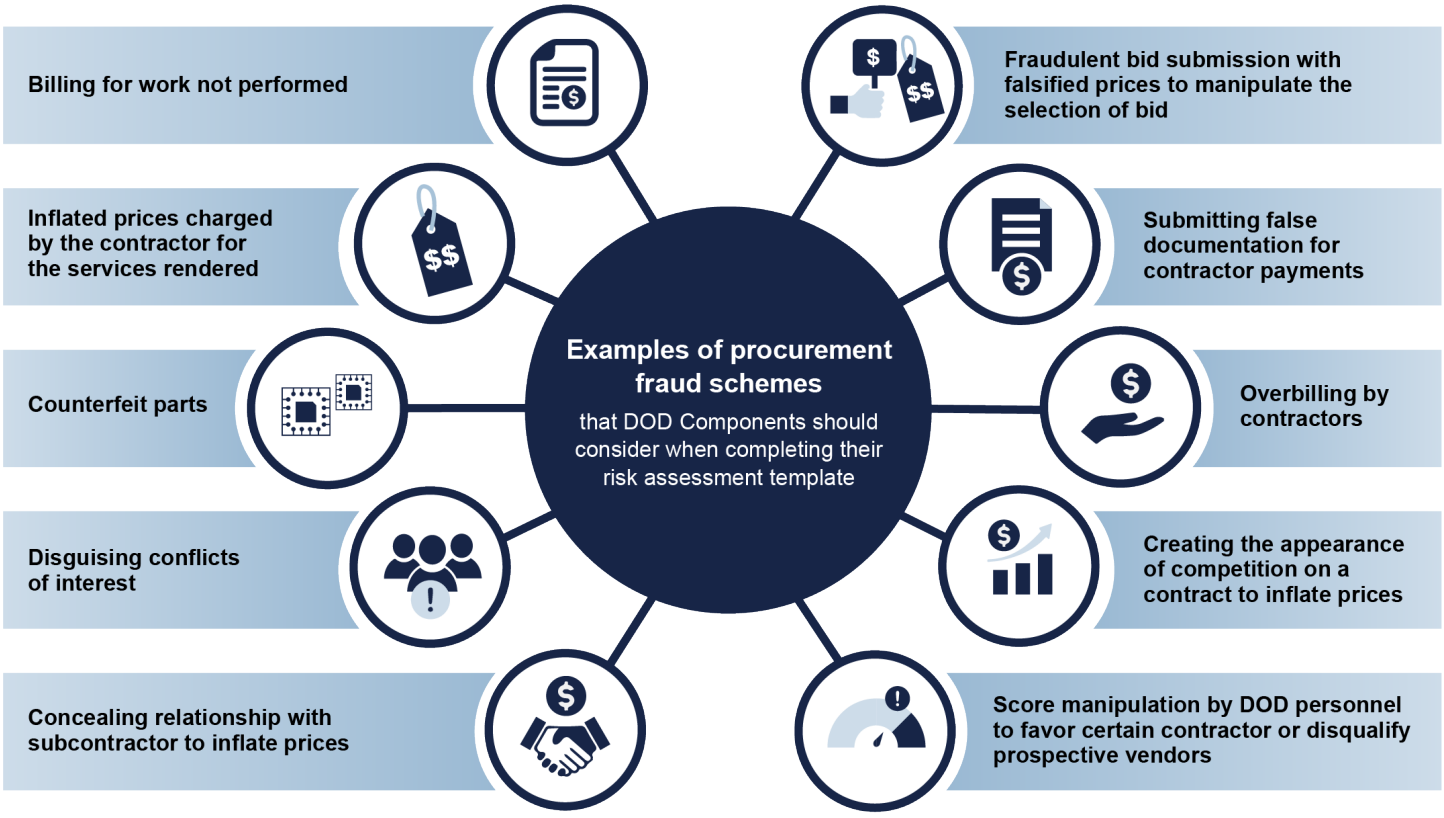
Policy guidance. The Comptroller and the Chief Management Officer were responsible for updating the *SOA Execution Handbook,* which provided guidance for the fiscal year 2020 SOA process. According to the

fiscal year 2020 *SOA Execution Handbook,* it updates requirements to assist each component with its annual SOA submissions, provides guidance to components to maintain the internal control environment, and focuses on the objective of obtaining an unqualified audit opinion. The 2020 *SOA Execution Handbook* also provides guidance to assist components in balancing an internal control program with risk management efforts that effectively and efficiently provide monitoring and oversight. Specifically, the *SOA Execution Handbook* requires that components must annually identify fraud risks related to payroll, beneficiary payments, procurement, grants, information technology and security, asset safeguards, purchase, travel, fleet cards, and commissary.

Tools and information. The Comptroller also provided tools and information to assist components with their own fraud risk assessments. For example, the Comptroller told us they developed a risk assessment template to assist components in compiling significant strategic, operational, reporting, and compliance risks at the component level. The Comptroller also told us they updated the risk assessment template for fiscal year 2020 to include a drop-down menu to assess fraud risk. With this update, the Comptroller required components to report on their fraud risks, including procurement fraud risk, for the first time, officials told us.

The Comptroller also provides examples of procurement fraud schemes within the *SOA Execution Handbook,* as shown in figure 6 below, for components to consider when assessing for procurement fraud risk. According to the 2020 *SOA Execution Handbook,* the list is not meant to be all-inclusive but to help the components get started with their fraud risk assessment. While not an exhaustive list, appendix II shows additional examples of requirements, processes, and tools available to components for consideration during the assessment process.

Figure 6: Examples of Procurement Fraud Schemes That Department of Defense's (DOD) Components Should Consider when Completing Their Risk Assessment Template



Source: GAO presentation of information from Department of Defense Fiscal Year 2020 Statement of Assurance Execution Handbook. | GAO-21-309

Text of Figure 6: Examples of Procurement Fraud Schemes That Department of Defense's (DOD) Components Should Consider when Completing Their Risk Assessment Template

- Billing for work not performed
- Inflated prices charged by the contractor for the services rendered
- Overbilling by contractors
- Counterfeit parts
- Concealing relationship with subcontractor to inflate prices
- Disguising conflicts of interest
- Score manipulation by DoD personnel to favor certain contractor or disqualify prospective vendors
- Submitting false documentation for contractor payments

- Creating the appearance of competition on a contract to inflate prices

Source: GAO presentation of information from Department of Defense Fiscal Year 2020 Statement of Assurance Execution Handbook. | GAO-21-309

Training. Officials within the Comptroller's Office told us they provide training to relevant stakeholders—an approach that is consistent with leading practices—in the fraud risk assessment process. For instance, the Comptroller provides training to component representatives responsible for completing the risk assessment template. One way the Comptroller provides this training is through "Office Hours" where components can receive instruction on how to complete their risk assessment templates for the annual SOA submission process. For instance, in April 2020, the Comptroller held an office hours for risk management representatives from components to explain how to meet *SOA Execution Handbook's* requirements.[43] Officials told us that training invitees include RMIC program representatives from the components and those responsible for completing the risk assessment template.

Some Components Did Not Report Procurement Fraud Risks as Required

As mentioned above, according to DOD's fiscal year 2020 *SOA Execution Handbook,* components were required to conduct risk assessments, including fraud risk assessments, to inform the identification of priorities for testing and remediation. Within their fraud risk assessments, components must annually identify fraud risks related to procurement, among other risks, consistent with leading practices to conduct the assessment at regular intervals. According to the *SOA Execution Handbook,* components were required to report the results of the risk assessments to the Comptroller and Chief Management Officer for the fiscal year 2020 SOA process. Further, components must identify controls currently in place, develop a mitigation plan to implement controls to prevent and detect fraud, and remediate any gaps in high-priority fraud risk areas. Officials within the Comptroller's Office told us the fiscal year 2020 SOA requirements were communicated to components via e-mail distribution and posting to an internal website, with a "What's New"

[43]Comptroller officials told us the office hours are open to members of the RMIC community and to the Fraud Reduction Task Force, who sometimes forward the information to other officials. Officials receive topics for discussion and follow-up questions for future office hours from the RMIC community and the components.

section highlighted. In addition, Comptroller officials told us they held multiple "Office Hours" to engage with components on the *SOA Handbook* requirements.

Comptroller officials said that 40 components reported a total of 386 fraud risks as a part of the fiscal year 2020 SOA risk assessment process. They stated that this information would inform DOD's fraud risk profile, which was completed in May 2021.

Our analysis of the fiscal year 2020 Quarter 4 Fraud Risk Assessments, as submitted to the Comptroller, from the six selected components showed that they all reported on fraud, operational, regulatory-compliance, information-technology and security, and financial risks. We also specifically examined the extent the six selected components' risk assessments reported on procurement fraud risks. As shown in table 3 below, three of the six selected components reported on procurement fraud risks within their risk assessments as required by the fiscal year 2020 *SOA Execution Handbook.* The remaining three selected components did not report on procurement fraud risks as required.

Table 2: Selected Department of Defense (DOD) Components' Fiscal Year 2020 Quarter 4 Risk Assessments Reporting on Fiscal Year 2020 Statement of Assurance (SOA) Execution Handbook Requirement to Report Procurement Fraud Risks

		Fiscal Year 2020 Quarter 4 Fraud-Risk-Assessment Submissions	
DOD Component	**Fiscal Year 2020 Obligations (dollars in billions)**	**Reported High Risk Focus Area of Procurement Fraud (Yes/No)[a]**	**Procurement Fraud Risk Type/ Scheme by Component**
Defense Contract Management Agency	$ -0.11[b]	Yes	• Contractor Fraud • Cost and Pricing • Contract Administration/Payments
Defense Logistics Agency	$41.9	Yes	• Suspected Overpricing • Bid Rigging • Counterfeit Parts • Misuse/abuse of Commercial and Government Entity (CAGE) code[c]
Department of the Navy	$150.0	Yes	• Contract management oversight • Employees exploit the procurement process to ensure an uneven playing field • Counterfeit parts • Manipulation of bid process • Contractors submit false certifications and billings
Department of the Air Force[d]	$77.9	No	None reported

DOD Component	Fiscal Year 2020 Obligations (dollars in billions)	Fiscal Year 2020 Quarter 4 Fraud-Risk-Assessment Submissions: Reported High Risk Focus Area of Procurement Fraud (Yes/No)[a]	Fiscal Year 2020 Quarter 4 Fraud-Risk-Assessment Submissions: Procurement Fraud Risk Type/ Scheme by Component
Department of the Army	$100.1	No	None Reported
Washington Headquarters Services	$2.1	No	None reported

Source: Federal Procurement Data System and GAO analysis of Department of Defense-provided data on fiscal year 2020 Quarter 4 Component-level Fraud Risk Assessments. | GAO-21-309

[a]Denotes a requirement from Department of Defense fiscal year 2020 *Statement of Assurance Execution Handbook*

[b]For fiscal year 2020, Defense Contract Management Agency reported negative obligations because the agency conducts contract closeout for some of its large contracts, and recently reported a large number of contracts that had not been closed within the time frames typically expected under federal regulations.

[c]The Commercial and Governmental Entity (CAGE) code is a unique five-character identifier assigned to contractors located in the United States and its territories to identify a commercial or government entity.

[d]Air Force officials told us they did not report procurement fraud risk in its risk assessment, but they did conduct and submit a fraud control matrix that included procurement fraud controls currently in place. However, according to the *SOA Execution Handbook* and fiscal year 2020 *Fraud Risk Management Strategy*, the components' risk assessments are used to inform the prioritization of risks and update the Department-wide fraud risk profile, while the fraud control matrix helps the Comptroller to create a comprehensive list of controls that are currently in place across the Department and to identify best practices to share with the DOD community.

The three components that reported on procurement fraud varied in the level of detail within their fraud risk assessments. They generally reported on internal opportunities for employees to exploit the procurement process and external procurement fraud schemes. For instance, Navy and the Defense Contract Management Agency reported opportunities for fraud, waste, and abuse due to a lack of oversight in contract management or employees seeking ways to exploit the procurement process in favor of one vendor over another. All three components reported on types of fraud schemes as described in the fiscal year 2020 *SOA Execution Handbook* and in prior OIG reports. For example, the Navy and Defense Logistics Agency reported on counterfeit parts, submitting false documentation, or bid rigging as potential procurement fraud schemes to mitigate within their defense agencies.

As previously noted, three components—Air Force, Army, and Washington Headquarters Services—did not report on procurement fraud within their risk assessment despite the fiscal year 2020 *SOA Execution*

Handbook's requirement to do so.[44] Comptroller officials told us they were aware that these components did not identify any procurement fraud risk in their risk assessments. The Comptroller's Office acknowledged it is a challenge to have a complete DOD fraud risk profile given that the components' fraud risk assessments varied in completeness and information provided. Comptroller officials explained that components—such as the Air Force, Army, and the Washington Headquarters Services—might not have reported on procurement fraud risks because the component experienced staff turnover.[45]

Officials within the Comptroller's Office told us for the fiscal-year-2020 fraud-risk assessment process, there was no requirement for components to explain why they would not report procurement fraud as a risk within their risk assessment template and there were no validation efforts in place. These officials told us they plan to expand their verification and validation efforts for fiscal year 2021 to include the components' fraud risk assessments. They said that they have had general discussions with these components about the 2021 fraud-risk-assessment process and emphasized that components pay close attention to procurement fraud risk and make sure these risks are included in the components' risk assessments going forward. Chief Management Officer officials told us that they rely on risks reported by components; this approach presents a challenge in documenting a complete and accurate picture of department-wide fraud risks. They told us they rely on components to monitor and mitigate risks that do not qualify as a significant or material weakness. That is, if a risk is not reported via the department-wide fraud-risk-assessment process, components are responsible for monitoring and mitigating that risk at the component level.[46]

[44]Officials from the Air Force told us they did not identify and assess procurement fraud risk in its risk assessment, but they did conduct and submit a fraud control matrix that included procurement fraud controls currently in place. However, according to the *SOA Handbook* and fiscal year 2020 *Fraud Risk Management Strategy*, the components' risk assessments are used to inform the prioritization of risks and update the Department-wide fraud risk profile, while the fraud control matrix helps the Comptroller to create a comprehensive list of controls that are currently in place across the Department and to identify best practices to share with the DOD community.

[45]We did not independently verify or corroborate the Comptroller's reason for why components may not have reported such risks.

[46]Chief Management Officer's officials told us this before the 2021 NDAA repealed the position of Chief Management Officer of the DOD effective January 1, 2021.

As mentioned above, the Comptroller's Office told us they interpret OMB Circular No. A-123's requirement that agencies include an evaluation of fraud risk to include all fraud risks, including procurement risks, regardless of risk materiality or weaknesses. Through guidance, DOD has assigned the implementation of this requirement—that is, the identification, assessment, and reporting of fraud risks—to its components. The Comptroller's Office explained that the requirement that components were only to report deficiencies that rise to the level of a significant deficiency or material weakness is related to a separate SOA submission process to identify material weaknesses and significant deficiencies. This process does not pertain to the fraud risk assessment that components conduct.

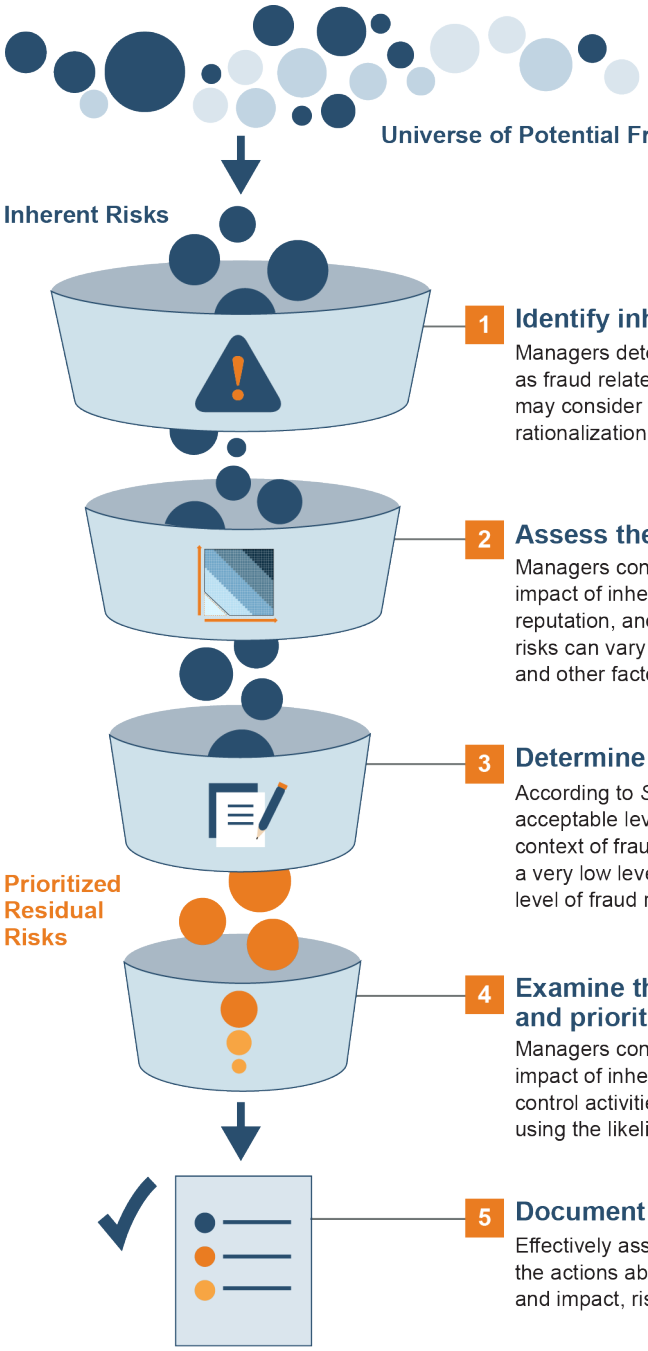
Further, as discussed above, the DOD's SOA process focuses on sustaining a strong internal control environment with the objective of obtaining an unqualified audit opinion, not a comprehensive fraud risk assessment. Not all fraud risks may rise to the level of a material weaknesses or significant deficiency for the purposes of an audit opinion, but that does not mean that such a risk should not be reported. DOD Instruction 5010.40 states that the concept of materiality is not primarily financial. Qualitative factors such as the effect on mission success or failure, health and safety, and threat to image must be considered. The objective of fraud risk management is to ensure program integrity by continuously and strategically mitigating the likelihood and effect of fraud. Further, fraud risks can have an effect on the program's reputation and compliance with laws or regulations. As noted in the *Fraud Risk Framework,* effective managers consider these nonfinancial effects during the risk assessment process. Finally, the Comptroller can consider the materiality of procurement fraud risks once all risks have been reported by components. Officials of the Chief Management Officer's office told us they rely on components to do this reporting due to the sheer size of the department, but they recognized there are opportunities to make improvements.

The *Fraud Risk Framework* identifies leading practices for conducting a fraud risk assessment to identify and assess fraud risks to determine a fraud risk profile. Fraud risk assessments that align with the *Fraud Risk Framework* involve identifying the inherent fraud risks affecting the program, assessing the likelihood and effect of those fraud risks, determining fraud risk tolerance, examining the suitability of existing controls and prioritizing residual fraud risk, and documenting the

program's fraud risk profile.[47] See figure 7 below for key elements of the fraud risk assessment process. According to leading practices, managers who effectively assess fraud risks attempt to fully consider the specific fraud risks the agency or program faces, analyze the potential likelihood and effect of fraud schemes, and then ultimately document prioritized fraud risks. Moreover, managers can use the fraud-risk-assessment process to determine the extent to which controls may no longer be relevant or cost-effective. The Framework also states that a robust fraud risk profile should include information about all fraud risks that may affect a program.

[47]GAO-15-593SP.

Figure 7: Key Elements of the Fraud Risk Assessment Process



1 Identify inherent fraud risks affecting the program

Managers determine where fraud can occur and the types of fraud the program faces, such as fraud related to financial reporting, misappropriation of assets, or corruption. Managers may consider factors that are specific to fraud risks, including incentives, opportunity, and rationalization to commit fraud.

2 Assess the likelihood and impact of inherent fraud risks

Managers conduct quantitative or qualitative assessments, or both, of the likelihood and impact of inherent risks, including the impact of fraud risks on the program's finances, reputation, and compliance. The specific methodology managers use to assess fraud risks can vary by program because of differences in missions, activities, capacity, and other factors.

3 Determine fraud risk tolerance

According to *Standards for Internal Control in the Federal Government*, risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. In the context of fraud risk management, if the objective is to mitigate fraud risks—in general, to have a very low level of fraud—the risk tolerance reflects managers' willingness to accept a higher level of fraud risks, and it may vary depending on the circumstances of the program.

4 Examine the suitability of existing fraud controls and prioritize residual fraud risks

Managers consider the extent to which existing control activities mitigate the likelihood and impact of inherent risks. The risk that remains after inherent risks have been mitigated by existing control activities is called residual risk. Managers then rank residual fraud risks in order of priority, using the likelihood and impact analysis, as well as risk tolerance, to inform prioritization.

5 Document the program's fraud risk profile

Effectively assessing fraud risks involves documenting the key findings and conclusions from the actions above, including the analysis of the types of fraud risks, their perceived likelihood and impact, risk tolerance, and the prioritization of risks.

Source: GAO. | GAO-21-309

Text of Figure 7: Key Elements of the Fraud Risk Assessment Process

1. Identify inherent fraud risks affecting the program
   Managers determine where fraud can occur and the types of fraud the program faces, such as fraud related to financial reporting, misappropriation of assets, or corruption. Managers may consider factors that are specific to fraud risks, including incentives, opportunity, and rationalization to commit fraud.
2. Assess the likelihood and impact of inherent fraud risks
   Managers conduct quantitative or qualitative assessments, or both, of the likelihood and impact of inherent risks, including the impact of fraud risks on the program's finances, reputation, and compliance. The specific methodology managers use to assess fraud risks can vary by program because of differences in missions, activities, capacity, and other factors.
3. Determine fraud risk tolerance
   According to Standards for Internal Control in the Federal Government, risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. In the context of fraud risk management, if the objective is to mitigate fraud risks—in general, to have a very low level of fraud—the risk tolerance reflects managers' willingness to accept a higher level of fraud risks, and it may vary depending on the circumstances of the program.
4. Examine the suitability of existing fraud controls and prioritize residual fraud risks
   Managers consider the extent to which existing control activities mitigate the likelihood and impact of inherent risks. The risk that remains after inherent risks have been mitigated by existing control activities is called residual risk. Managers then rank residual fraud risks in order of priority, using the likelihood and impact analysis, as well as risk tolerance, to inform prioritization.
5. Document the program's fraud risk profile
   Effectively assessing fraud risks involves documenting the key findings and conclusions from the actions above, including the analysis of the types of fraud risks, their perceived likelihood and impact, risk tolerance, and the prioritization of risks.

Source: GAO. | GAO-21-309

Further, the *Fraud Risk Framework* acknowledges that agencies may use initiatives, like enterprise risk management efforts, to assess their fraud risks, but that does not eliminate the need for separate and independent fraud-risk-management efforts. While the existing SOA process could inform a fraud risk assessment, DOD has not used these efforts to comprehensively assess procurement and other fraud risks in accordance with leading practices. In addition, without complete component assessments, the Comptroller cannot analyze the potential likelihood and effect of procurement fraud schemes and then ultimately document prioritized fraud risks.

Three of the six selected components identified procurement fraud risks and assessed the likelihood and effect of such risks during the fiscal-year

2020 fraud-risk-assessment process, but three components did not, as previously noted. The Comptroller consolidates reported procurement risks from the components' fraud risk assessments and uses this information to update the department-wide fraud risk profile. Without complete information on fraud risks from all components, the Comptroller cannot ensure that the fraud risk tolerance, the suitability of existing controls, or prioritization of residual procurement fraud risk in the Department's documented fraud risk profile are complete or accurate, consistent with leading practices that a robust fraud risk profile include information about all fraud risks that may affect a program.

Conclusions

In fiscal year 2020, DOD obligated approximately $422 billion on contracts. The scope and scale of this activity makes DOD procurement inherently susceptible to fraud. In 2020, DOD took steps consistent with leading practices to implement a structure to manage department-wide fraud risks, including those involving procurement, but the effort remains a work in progress. DOD has opportunities to build upon these steps to position itself to better identify and mitigate its fraud risks, including those related to contracting. For instance, with almost 20 percent of the Task Force's positions vacant a year after it was formed, filling the vacancies would further strengthen DOD's ability to effectively make fraud risk a management priority and ensure resources are available to develop action plans for mitigating fraud risks across the department.

DOD's policy and guidance regarding its fraud-risk-management activities remains incomplete. Specifically, OMB Circular No. A-123 requires DOD to evaluate risks to accomplishing strategic, operations, reporting, and compliance objectives. To fulfill these objectives, DOD delegates implementation responsibilities to components and uses its and components' RMIC programs to identify, assess, and report on the effectiveness of internal controls. However, DOD Instruction 5010.40—which governs the RMIC programs—has not been updated to include relevant Circular No. A-123 fraud-risk-reporting requirements. In addition, while the *SOA Execution Handbook* requires that components annually identify, assess, and report fraud risks, the emphasis is on remediating material weaknesses and increased financial statement auditability. As a result, components may not be reporting fraud risks that are not categorized as a material weakness or a significant deficiency because the current guidance does not specify that they are required to do so. Because the Comptroller consolidates procurement risks reported in the

components' fraud risk assessments and uses this information to update the department-wide fraud risk profile, the Comptroller cannot ensure that the Department's documented fraud risk profile is complete or accurate. Without explicit fraud-risk-reporting requirements implemented through policy and guidance, DOD's design, implementation, and operating of control activities' effectiveness in managing fraud risks may be limited.

In addition, officials from the Comptroller's Office told us they share fraud risk information with department-wide RMIC oversight officials—including department-wide Assessable Unit Senior Accountable Officials, Action Officers, and the Defense Business Council—to keep stakeholders informed of risk management activities to enhance department-wide progress. However, the roles and responsibilities for these officials are not referenced in DOD's July 2020 fraud-risk-management guidance. Documenting the roles and responsibilities of department-wide Assessable Unit Senior Accountable Officials and their Action Officers and the Defense Business Council provides an opportunity to enhance the Comptroller's ability to ensure these stakeholders:

- understand their responsibilities and the chain of accountability,
- use high priority risk areas to strategize at the department level, and
- remain informed of risk management activities to enhance department-wide progress.

Given DOD's decentralized approach for identifying and managing fraud risks, documentation provides a means to assure consistent implementation and understanding of requirements and to help mitigate the risk of having that knowledge limited to a few personnel.

DOD relies on its components to identify, assess, and report procurement fraud risks as part of the SOA process. However, our review of selected components' assessments found that three of the six selected components reported procurement fraud risks during the fiscal year 2020 fraud-risk-assessment process, and the other three components did not. Because DOD consolidates reported procurement risks from the components' fraud risk assessments and uses this information to update the Department-wide fraud risk profile, DOD cannot ensure that the Department's documented fraud risk profile is complete or accurate. The SOA process focuses on sustaining a strong internal control environment with the objective of obtaining an unqualified audit opinion, not on a comprehensive fraud risk assessment. The *Fraud Risk Framework* acknowledges that agencies may use initiatives, like enterprise risk

management efforts, to assess their fraud risks, but it does not eliminate the need for separate and independent fraud-risk-management efforts. While the existing SOA process could inform a fraud risk assessment, DOD has not used these efforts to comprehensively assess procurement fraud risks in accordance with leading practices.

While DOD has taken initial steps to better manage its fraud risks—including those related to contracting—ensuring that these efforts are finalized and comprehensive, as well as strategically organized and targeted at prioritized fraud risks could help strengthen the Department's overall approach to fraud risk management. Now that the Chief Management Officer's position has been repealed, it will be critical for the Comptroller to continue efforts to make DOD's fraud-risk-management program more robust and effective, especially through revisions in policy and guidance. Effective fraud risk management would help ensure alignment of DOD's program policy and guidance. In this regard, implementing robust fraud-risk-management processes is vital to help ensure that federal programs, such as those involving DOD procurement, fulfill their intended purpose, funds are spent effectively, and assets are safeguarded. Given the billions of dollars DOD spends annually on procurement, failing to manage and mitigate fraud effectively may ultimately adversely affect DOD's ability to support the warfighter.

Recommendations for Executive Action

We are making the following five recommendations to DOD:

The Deputy Chief Financial Officer should ensure that cognizant DOD components designate representatives to the Fraud Reduction Task Force as expeditiously as possible. (Recommendation 1)

The Comptroller should update DOD Instruction 5010.40 to include fraud-risk-assessment and reporting requirements. Specifically, the instruction should:

- distinguish fraud-risk-assessment and reporting requirements from financial-reporting requirements, and
- clarify that components must report all fraud risks, including fraud risks that are not categorized as a material weakness or a significant deficiency. (Recommendation 2)

The Comptroller should update its *Statement of Assurance Execution Handbook* to clarify that components should report all fraud risks, including fraud risks that are not categorized as a material weakness or a significant deficiency. (Recommendation 3)

The Comptroller should determine and document the fraud-risk-management roles and responsibilities of all oversight officials, including department-wide Assessable Unit Senior Accountable Officials and their Action Officers and the Defense Business Council, and the chain of accountability for implementing DOD's fraud-risk-management approach. (Recommendation 4)

The Comptroller should direct components, as part of the annual statement of assurance process, to plan and conduct regular fraud risk assessments that align with leading practices in the *Fraud Risk Framework.* Specifically, the assessment process should include: (1) identifying inherent procurement fraud risks, (2) assessing the likelihood and effect of these risks, (3) determining fraud risk tolerance, (4) examining the suitability of existing fraud controls, and (5) compiling and documenting the fraud risk profile. (Recommendation 5)

Agency Comments and Our Evaluation

We provided a copy of this report to DOD for review and comment. In its written comments, reproduced in appendix III, DOD concurred with our first and second recommendations, citing actions that it plans to take to address them. However, DOD did not concur with our third and fourth recommendations and partially concurred with our fifth recommendation. We continue to believe that all of the recommendations are warranted as fundamental practices to ensure effective fraud-risk management, as discussed below, and DOD should act to implement all of the recommendations in their entirety. DOD and DOD OIG also provided technical comments, which we incorporated as appropriate.

DOD did not concur with our third recommendation that the Comptroller update its *Statement of Assurance Execution Handbook* to clarify that components should report all fraud risks, including fraud risks that are not categorized as a material weakness or a significant deficiency. In its comments, DOD stated that its fiscal year 2021 *SOA Execution Handbook* requests that components report all fraud risks, including fraud risks that are not categorized as a material weakness or significant deficiency. The fiscal year 2021 *Statement of Assurance Execution*

Handbook states that DOD components must annually identify fraud risks related to grants, procurement, and opaque contractor ownership, among others, in DOD's risk assessment template. However, the guidance does not specify that all fraud risks should be reported, specifically those risks that are not categorized as a material weakness or significant deficiency. Further, according to the fiscal year 2021 *Statement of Assurance Execution Handbook,* the risk assessment template—which the Comptroller uses to compile a department-wide fraud risk profile—was developed to assist DOD components in identifying and compiling the most significant financial and non-financial risks. As discussed in this report, under DOD's current approach, components may not be reporting all fraud risks, including those that are not categorized as a material weakness or significant deficiency, because the guidance does not clearly state they must do so. Not all fraud risks may rise to the level of a material weakness or significant deficiency to be reported on the risk assessment template, the reporting mechanism for fraud risks—which is why we continue to believe this recommendation is warranted.

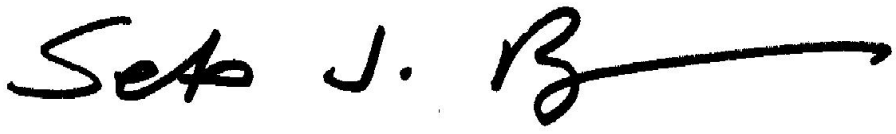
DOD did not concur with our fourth recommendation that the Comptroller should determine and document the fraud-risk management roles and responsibilities of all oversight officials and the implementation of the chain of accountability. In its comments, DOD stated that Assessable Unit Senior Accountable Officials' and Action Officers' primary role is to support driving audit progress and mitigating department-wide material weaknesses. However, DOD stated that Office of the Comptroller will internally discuss any potentially required updates regarding the Assessable Unit Senior Accountable Officials' and Action Officers' roles and responsibilities. As discussed in this report, DOD officials told us fraud risk information is shared with Assessable Unit Senior Accountable Officials and their Action Officers, as well as the Defense Business Council. However, these entities, along with the Procurement Fraud Working Group as DOD noted in its comments, are not referenced in DOD's fraud-risk management guidance. As we found, it is not clear what these entities' roles and responsibilities are as they relate to DOD's fraud-risk management approach and how accountability is maintained. This absence of documentation does not align with *Federal Internal Control Standards.* Specifically, these standards note that documentation provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors. Not documenting all oversight officials' roles and responsibilities may limit DOD's ability:

- to ensure stakeholders understand their responsibilities and the chain of accountability,
- to use high priority risk areas to strategize at the department level, and
- to remain informed of risk management activities to enhance department-wide progress.

DOD partially concurred with our fifth recommendation that the Comptroller direct components to plan and conduct regular fraud risk assessments that align with leading practices in the *Fraud Risk Framework* as part of the annual statement of assurance process. In its comments, DOD stated that it provides a risk assessment template and guidance to assist components in identifying and compiling the most significant financial and non-financial risks relevant to the individual component. However, DOD stated that it will update the language for fiscal year 2022 to specifically call out the inclusion of fraud risks in the statement-of-assurance risk-assessment template. Doing so provides DOD with an opportunity to use the annual statement-of-assurance process to comprehensively assess procurement fraud risks in accordance with leading practices. Further, taking this step may also help ensure that all fraud risks are reported by all components, providing DOD with a complete and accurate basis for the Department's documented fraud risk profile and better positioning it to manage its fraud risks. However, to fully address our recommendation and align with leading practices, DOD will also need to ensure that components are identifying inherent procurement fraud risks and assessing the likelihood and effect of those risks.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the appropriate congressional committees, the Secretary of Defense, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-6722 or bagdoyans@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made contributions to this report are listed in appendix IV.



Seto J. Bagdoyan
Director of Audits, Forensic Audits and Investigative Service

Appendix I: Objectives, Scope, and Methodology

This report assesses the steps the Department of Defense (DOD) took in fiscal year 2020: (1) to combat department-wide fraud risks and (2) to conduct a fraud risk assessment and ensure that DOD's component organizations report procurement fraud risks.

To assess the steps DOD has taken to combat department-wide fraud risks, including demonstrating its commitment to doing so, we analyzed DOD guidance documents—including DOD's July 2020 fraud risk management guidance—and compared those documents with leading practices contained in *A Framework for Managing Fraud Risks in Federal Programs (Fraud Risk Framework)*.[1] Specifically, we compared those documents with leading practices relevant to the first component of the *Fraud Risk Framework*: commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.[2]

We also interviewed officials from the Offices of the Under Secretary of Defense (Comptroller) and the Chief Management Officer to discuss their roles in fraud risk management. In addition, we assessed the information gathered to determine the extent to which DOD's activities align with relevant federal internal control standards contained in the *Standards for Internal Control in the Federal Government (Federal Internal Control Standards)*—such as those relating to demonstrating oversight and enforcing accountability.[3] For example, to assess DOD's commitment to creating an organizational culture conducive to fraud risk management, we reviewed documentation describing DOD's fraud risk management

[1]Department of Defense, *Managers' Internal Control Program Procedures,* DOD Instruction 5010.40 (Washington, D.C., May 30, 2013) (Incorporating Change 1, effective June 30, 2020).

[2]GAO, *A Framework for Managing Fraud Risks in Federal Programs,* GAO-15-593SP (Washington, D.C.: July 2015). The *Fraud Risk Framework* contains four components: (1) commit; (2) assess; (3) design and implement; and (4) evaluate and adapt. Within the four components, there are overarching concepts and leading practices. To assess the steps DOD took to combat department-wide fraud risks, we selected the first component—commit—because DOD formalized its fraud risk management approach in fiscal year 2020 and is in the initial stages of implementation.

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

approach and interviewed Comptroller and Chief Management Office officials to determine whether there was a designated lead entity to oversee fraud risk management activities since this step would be indicative of a senior-level commitment to combat fraud. We also used this information to identify structures potentially conducive to fraud risk management, such as the Fraud Reduction Task Force.

To assess the steps DOD has taken to conduct a fraud risk assessment and ensure that DOD component organizations report procurement fraud risks, we reviewed applicable guidance contained in the *Fiscal Year 2020 DOD Statement of Assurance (SOA) Execution Handbook.* We also reviewed fraud risk assessments from six selected components to determine the extent to which those assessments reported on the high-risk focus area of procurement fraud. In addition, we also interviewed officials from the Offices of the Comptroller and the Chief Management Officer to discuss their roles in compiling the department-wide fraud risk profile. We compared DOD's guidance to selected leading practices relevant to assessing fraud risks as described in the second component of the *Fraud Risk Framework:* plan regular fraud risk assessments and assess risks to determine a fraud risk profile.[4] Specifically, we assessed DOD's actions to relevant leading practices related to planning, conducting, and documenting a comprehensive fraud risk assessment to determine the program's fraud risk profile. For example, we reviewed fraud risk assessments submitted to the Comptroller from the six selected components to determine the extent to which the components complied with the *SOA Execution Handbook's* requirement to identify procurement fraud risks.

Our six selected components were the Departments of the (1) Air Force, (2) Army, and (3) Navy; (4) Defense Contract Management Agency; (5) Defense Logistics Agency; and (6) Washington Headquarters Services. We selected five of these components—the Departments of the Air Force, Army, and Navy; Defense Logistics Agency; and Washington Headquarters Services—based on contract obligations from fiscal year 2014 through 2018, the five most recent years available at the time of our

[4]A robust fraud risk profile would include information about all fraud risks that may affect a program. Documenting fraud risks together can aid managers in understanding links between specific risks.

selection.[5] These five components comprised almost 90 percent of the total DOD contract obligations during this timeframe. The Defense Logistics Agency manages the global supply chain—from raw materials to end user to disposition—for the Air Force, Army, and Navy, among other components. Washington Headquarters Services has a broad scope of responsibilities, including facility management and centralized contracting and procurement. We selected the sixth component—the Defense Contract Management Agency—based on its role in providing contract administration services for DOD, including the military services. Our findings from the six selected components cannot be generalized to the remaining DOD components.

Our review was limited to DOD's fraud risk management activities for fiscal year 2020. Therefore, this engagement does not examine the effects of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021's repeal of the Chief Management Officer position.[6]

As previously mentioned, we conducted this performance audit from January 2019 to August 2021 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.

[5]Although there are components that obligated more funds than Washington Headquarters Services, we did not select them because their primary functions of national intelligence or health care were outside our scope. During fiscal years 2014 through 2018, 23 DOD components reported contract obligations in Federal Procurement Data System (FPDS). We determined that FPDS is sufficiently reliable for purposes of determining DOD contract obligations from fiscal years 2014 through 2018 overall and across select DOD components.

[6]Pub. L. No. 116-283, Div. A, § 901, 134 Stat. 3388, 3794 (2021).

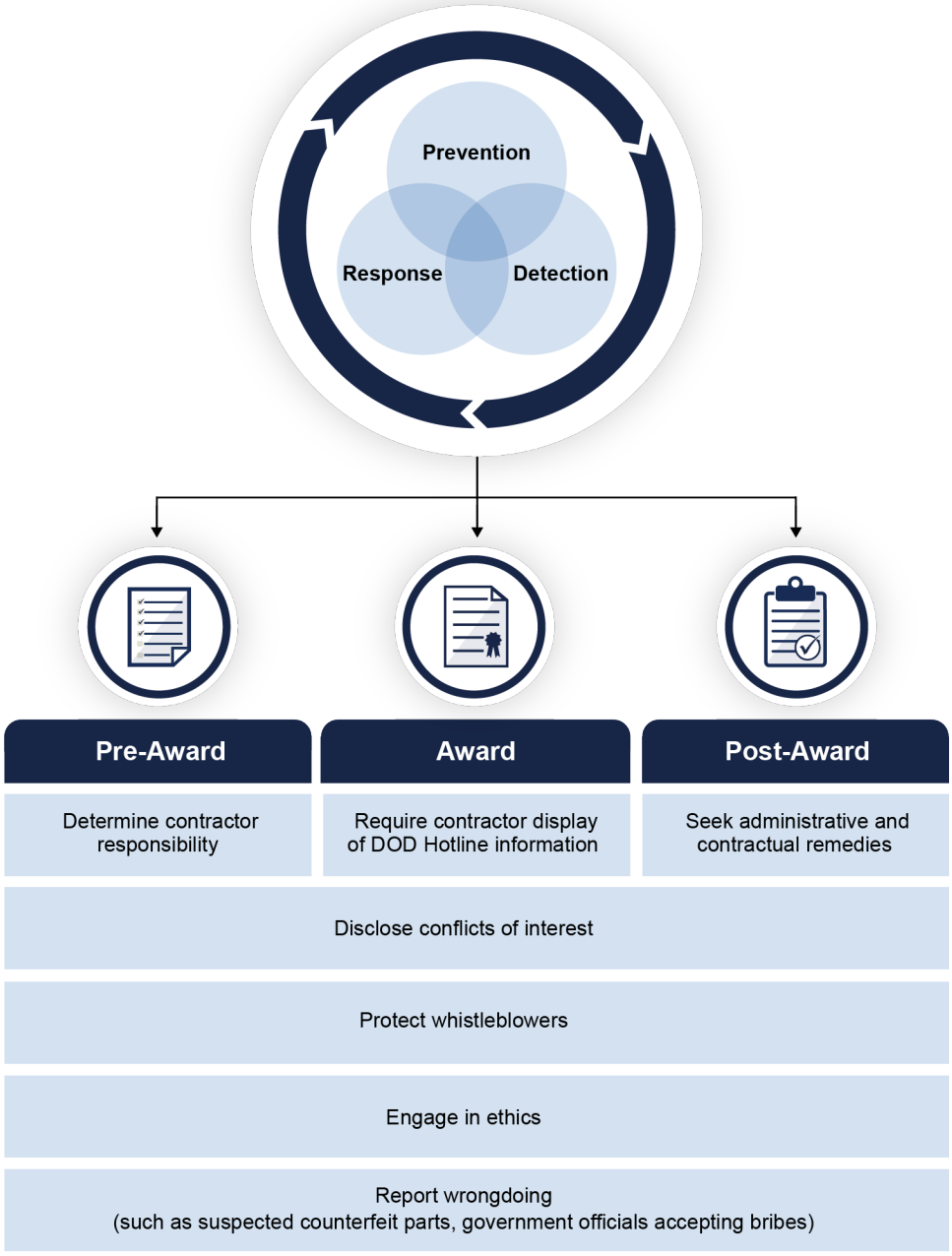
Appendix II: Examples of Activities to Help the Department of Defense (DOD) Manage Contracting Fraud

Activities for managing fraud risk generally fall into three categories of prevention, detection, and response, with each category reinforcing the others. To manage contracting fraud risk, DOD has various requirements, processes, and tools available that are intended to help prevent, detect, and respond to fraud. These requirements, processes, and tools are available throughout the contracting lifecycle, as well as during specific phases. We have identified these phases to include the pre-contract award phase, the contract award phase, and the post-contract award phase.

- Pre-award phase activities generally include defining requirements, planning the acquisition, and preparing the solicitation.
- Award phase activities generally involve evaluating offers, negotiating price, and selecting awardees.
- Post-award phase activities generally involve contract administration, agency oversight of contractor performance, and closeout of the contract.

See figure 8 for examples of requirements, processes, and tools available to DOD to help manage its fraud risk. We did not independently verify the efficacy or ability of any of these requirements, processes, and tools to address fraud or fraud risk.

Figure 8: Examples of Requirements, Processes, and Tools Available to the Department of Defense (DOD) during the Contracting Lifecycle to Help Prevent, Detect, and Respond to Fraud



Source: GAO analysis of the Federal Acquisition Regulation and Department of Defense information. | GAO-21-309

Text of Figure 8: Examples of Requirements, Processes, and Tools Available to the Department of Defense (DOD) during the Contracting Lifecycle to Help Prevent, Detect, and Respond to Fraud

Pre-Award	Award	Post-Award
Determine contractor responsibility	Require contractor display of DOD Hotline information	Seek administrative and contractual remedies
Disclose conflicts of interest	Disclose conflicts of interest	Disclose conflicts of interest
Protect whistleblowers	Protect whistleblowers	Protect whistleblowers
Engage in ethics	Engage in ethics	Engage in ethics
Report wrong doing (such as suspect counterfeit parts, government officials accepting bribes)	Report wrong doing (such as suspected counterfeit parts, government officials accepting bribes)	Report wrongdoing (such as suspect counterfeit parts, government officials accepting bribes)

Source: GAO analysis of the Federal Acquisition Regulation and Department of Defense information. | GAO-21-309

Prevention

The pre-award and award phases of the contracting lifecycle provide opportunities to prevent contracting fraud, such as ensuring that the prospective contractor is determined to be responsible to perform the work.

Contractor Responsibility Determination

According to the Federal Acquisition Regulation, no purchase or award may be made unless the contracting officer makes an affirmative determination that the prospective contractor is responsible.[1] The following tools help prevent contracting fraud because these tools provide various information on contractors, such as whether they have been convicted of fraud:

[1]FAR §§ 9.103 and 9.104-1.

Prevention

Opportunities to prevent contracting fraud

Source: GAO. | GAO-21-309

- The System for Award Management contains government-wide information on contractors. Any entity that wishes to do business with the government must register in the System for Award Management to be eligible to receive a contract award except in certain circumstances.[2] When an agency excludes a contractor—thereby making the contractor ineligible from receiving contracts for a period of time—it must report this information in the System for Award Management.[3] Contracting officers are able to search the System for Award Management for excluded contractors.
- The Federal Awardee Performance and Integrity Information System was designed to significantly enhance the government's ability to evaluate the ethics and quality of prospective contractors competing for federal contracts and to protect taxpayers from doing business with irresponsible contractors. This system provides a prospective contractor "Report Card" that includes information pertaining to the prospective contractor's past performance (if applicable), such as any administrative agreements, contract terminations, nonresponsibility determinations, and exclusions from the System for Award Management, among other things. Before awarding a contract, a contracting officer is generally required to review the prospective contractor's information found in the Federal Awardee Performance Integrity Information System.[4]
- The Dun & Bradstreet database contains business information on all existing and potential government contractors and awardees, linked to the business entity through unique Data Universal Numbering System (DUNS) numbers. A DUNS number is a unique 9-digit number that is assigned to every business entity in Dun & Bradstreet's global business database.[5] Officials from the Army, Defense Logistics Agency, and Washington Headquarters Services told us that contracting officers at these agencies use the Dun & Bradstreet database to obtain information to help them determine responsibility

[2]FAR § 4.1102.

[3]FAR § 9.404.

[4]FAR § 9.104-6.

[5]Dun & Bradstreet is a global provider of data and analytics for business decisions. Specifically, the Dun & Bradstreet data cloud holds millions of records representing companies comprising the vast majority of the world's gross domestic product. In 1963, Dun & Bradstreet introduced its DUNS numbers to identify businesses numerically for data-processing purposes.

of prospective contractors. For example, officials from Washington Headquarters Services told us that information obtained from Dun & Bradstreet allows contracting officers to identify company financial risks and enables the contracting officers to verify that the vendor is a legitimate company. A Dun & Bradstreet report evaluates the company's risk based upon its credit score and financial stressors and predicts the likelihood of its going out of business within the next 12 months.

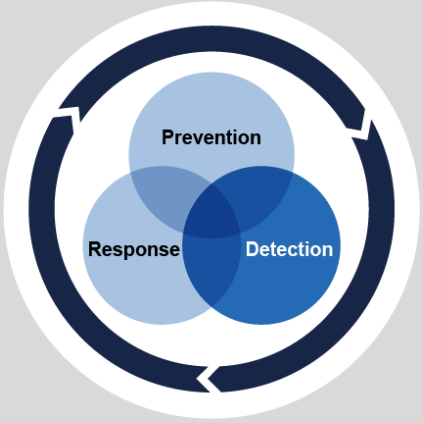
- The Defense Contractor Review List is an enterprise-wide tool for use by contracting officers to identify and communicate contractor performance, capability, and integrity issues for making determinations of responsibility and the effective administration of contracts.

Detection

DOD can take action to detect contracting fraud at any time during the contracting lifecycle through a number of ways, including the DOD Hotline, DOD's Contractor Disclosure Program, audits by the Defense Contracting Audit Agency, and additional tools used by components.

DOD Hotline

Detection
Opportunities to identify contracting fraud

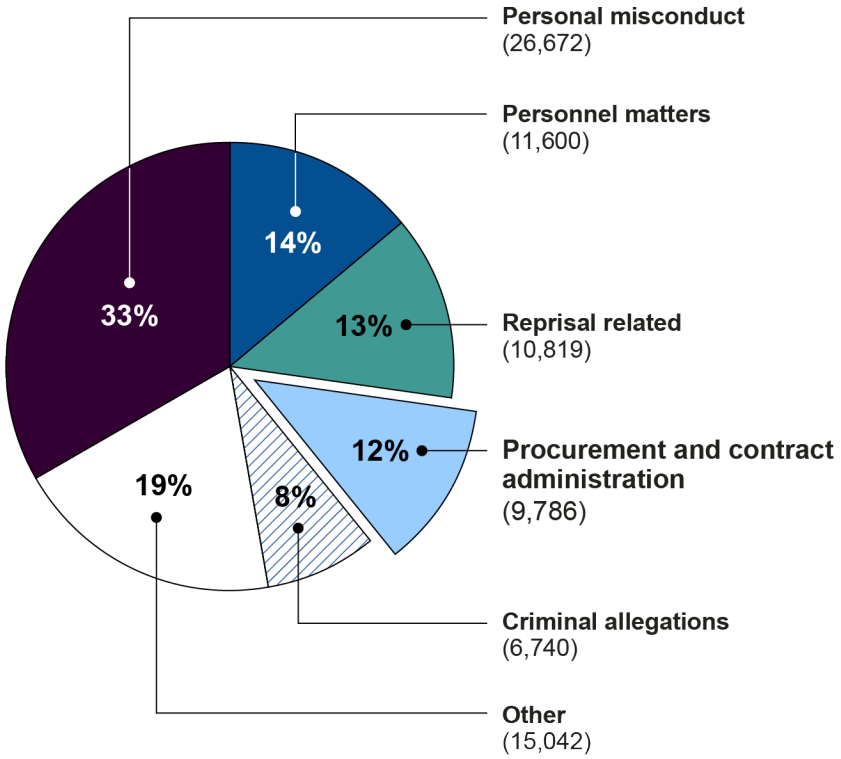


Source: GAO. | GAO-21-309

The DOD Hotline, managed by the DOD Office of Inspector General (OIG), provides a confidential means for anyone to report fraud involving DOD personnel and operations—including contractors—without fear of reprisal. Defense contractors generally must prominently display DOD Hotline information in common work areas within business segments performing work under DOD contracts and, if the contractor maintains a website as a method of providing information to employees, on the

website.[6] In 2019, the DOD OIG reported that the DOD Hotline receives approximately 14,000 complaints annually.[7] As demonstrated in figure 9, complaints regarding procurement and contract administration comprise one of the top five DOD Hotline categories.

Figure 9: Department of Defense Hotline Allegation Types Received from Fiscal Years 2015 through 2019



Source: GAO analysis of DOD OIG Semiannual Reports from fiscal years 2015-2019. | GAO-21-309

Data table for Figure 9: Department of Defense Hotline Allegation Types Received from Fiscal Years 2015 through 2019

Personal Misconduct	26672	33%
Personnel Matters	11600	14%
Reprisal Related	10819	13%
Procurement & Contract Administration	9786	12%

[6]DFARS § 252.203-7004.

[7]Department of Defense Office of Inspector General (DOD OIG), *Fiscal Year 2020, Top DOD Management Challenges,* (Alexandria, VA).

Criminal Allegations	6740	8%
Other	15042	19%

Source: GAO analysis of DOD OIG Semiannual Reports from fiscal years 2015-2019. | GAO-21-309

Note: One semi-annual report from fiscal year 2015 reported DODs Office of Inspector General Hotline cases closed from allegations received. The remaining reports from fiscal years 2015 through 2019 reported cases opened from allegations received.

The DOD Hotline coordinates the receipt and evaluation of fraud, waste, abuse, and mismanagement allegations, including violations of contracting fraud, and refers cases for investigation using a priority referral process. In 2017, DOD OIG issued DOD Hotline Instruction 7050.01 which defines responsibilities, procedures, and quality standards for the DOD Hotline.[8] To protect whistleblowers who report violations, this instruction requires that the confidentiality of the DOD Hotline source must be protected. Whistleblowers play an important role in safeguarding the federal government against fraud. However, whistleblowers also risk reprisal, such as demotion, reassignment, and firing. The DOD OIG is also responsible for investigating allegations of whistleblower reprisals.

DOD Contractor Disclosure Program

DOD's Contractor Disclosure Program provides defense contractors with a method to report contracting fraud violations discovered during self-policing activities. In 2016, DOD OIG updated its DOD Contractor Disclosure Program Instruction 5505.15, which provides a framework for government verification of the information reported.[9] Contractor disclosures are made with no advance agreement regarding possible DOD resolution of the matter and with no promises regarding potential civil or criminal action by the Department of Justice. For certain contracts, regulations require a clause to be inserted into a contract that requires contractors to disclose certain violations of criminal law—including fraud and instances of knowingly making false claims to the government—to the agency's OIG.[10] According to the DOD Contractor's *Guide to Submitting a Disclosure,* the contractor is required to disclose a description of the violation, any safety or operational hazards, and an

[8]DOD Instruction 7050.01, *DOD Hotline Program* (Oct. 17, 2017).

[9]DOD Instruction 5505.15, *DOD Contractor Disclosure Program* (Dec. 22, 2016).

[10]FAR § 52.203-13.

estimated financial effect to the government among other things.[11] DOD's Instruction 5505.15, which establishes policy for the DOD Contractor Disclosure Program, states that upon receipt of a contractor disclosure, the DOD OIG is required to:

- notify the Department of Justice as well as affected DOD Components,
- refer contractor disclosures of a criminal nature to the appropriate Defense Criminal Investigative Organization for investigation, and
- refer non-criminal contractor disclosures to the affected DOD component for appropriate action.[12]

We found that DOD OIG received 1,218 contractor disclosures from fiscal years 2015 through 2019. During this time period, labor mischarges—such as artificially inflated hours—comprised the vast majority (72 percent) of contractor disclosures. However, these disclosures also included instances of bribery, bid-rigging, and counterfeit parts, among other potential violations.[13]

Audits by the Defense Contract Audit Agency

The Defense Contract Audit Agency (DCAA) performs all necessary contract audits for DOD and was established to provide more efficient and consistent contracting audit support by centralizing these duties in a single defense organization. DCAA contract audits help ensure that the government pays fair and reasonable prices for needed goods and services and that contractors charge the government in accordance with applicable laws, regulations, and contract terms. For example, DCAA audits primarily cost-reimbursable and other non-fixed price contracts, which generally pose the highest risk to the government. According to the DOD OIG, using a cost-reimbursement type contract may increase the risk that the contractor will fraudulently overcharge the government.[14]

[11]OIG, DOD, *DOD Contractor's Guide to Submitting a Disclosure* (July 2018).

[12]DOD Instruction 5505.15.

[13]GAO analysis of data reported in DOD OIG semiannual reports from fiscal years 2015-2019.

[14]OIG, DOD, *Contingency Contracting: A Framework for Reform-2015 Update.* DODIG-2015-101 (Alexandria, Va.: Mar. 31, 2015).

To assist auditors with identifying contracting fraud during audits, DOD OIG developed a list of fraud indicators for contract audits. This list includes scenarios such as kickbacks and falsification of documents. DCAA auditors are required to promptly report any instances of suspected fraud discovered during an audit to the DOD OIG.[15] DCAA's Suspected Irregular Conduct Referral form provides a means to report the suspected fraud, including an estimated loss to the government and a classification of the irregularity. The form allows the auditor to classify the irregularity in multiple categories, such as accounting, billing, labor, pricing, materials, false claims, small business fraud, and ethical violations, including kickbacks, gratuities, and bribery. DCAA officials told us that DCAA auditors submitted 229 Suspected Irregular Conduct Referral forms to DOD OIG between fiscal years 2015 through 2019.

Component Tools

Officials from some of our six selected components told us about tools they use to help detect defense-contracting fraud.

- Officials from the Air Force and the Defense Contract Management Agency told us that they use data analytics to help detect contracting fraud. Data analytics enables insights into the operating effectiveness of internal controls and the identification of improper cost charges, potential indicators of fraud, or actual fraudulent payments or activities. For example, the Air Force uses fraud analysts to assess fraud indicators to help identify vulnerabilities to conduct risk assessments on contractors.
- Washington Headquarters Services officials told us that conducting site visits could help detect contractor fraud. Officials provided an example where a site visit determined that the contractor's reports did not match physical evidence found at the site. Ultimately, Washington Headquarters Services did not pay the contractor for the inconsistent work.

[15]DCAA Instruction 7640.15, *Reporting and Monitoring of Suspected Contractor Fraud, DOD Contractor Disclosure Program, and Other Contractor Irregularities* (Mar. 21, 2019).

Response

Response
Opportunities to remediate contracting fraud.

Source: GAO. | GAO-21-309

DOD can take action to respond to contracting fraud which affects all phases of the contracting lifecycle. For example, excluding a current defense contractor due to a fraud conviction will prevent that contractor from winning future government awards. DOD actions include pursuing administrative and contractual remedies, and coordinating with the Department of Justice to pursue criminal and civil remedies.

Administrative Remedies: DOD may take a number of administrative actions that not only respond to fraud that has occurred but to also help prevent additional fraud from occurring, such as removing the contractor from lists of qualified bidders or manufacturers, termination of a contracting officer's appointment, and suspending or debarring contractors.[16] Suspension takes place for a temporary period, pending the completion of an investigation or legal proceeding.[17] Debarred contractors are ineligible to contract with the government for a specified period of time—generally no more than 3 years—unless in certain specified instances or if the government determines that it is necessary to protect the government's interest.[18] Both suspended and debarred contractors that are placed on the excluded parties list within the System for Award Management. Suspension and debarment are not considered punishments but are meant to protect the government. The Interagency Suspension and Debarment Committee reported that in fiscal year 2019, DOD issued 267 suspensions and 442 debarments.[19]

Contractual Remedies: DOD may take a number of contract-based actions to ensure integrity of products or recoup lost dollars. These include requiring the contractor to correct defects in the procured item, refusing to accept nonconforming goods presented by the contractor,

[16]FAR §§ 9.207, 1.603-4, and subpart 9.4.

[17]FAR § 9.407-4.

[18]FAR § 9.406-4.

[19]The Interagency Suspension and Debarment Committee is an interagency body created by Executive Order 12549, 51 Fed. Reg. 6370 (Feb. 18, 1986), consisting chiefly of representatives from executive branch organizations that work together to provide support for suspension and debarment programs throughout the government. The committee reports to Congress annually on the status of the federal suspension and debarment system, pursuant to 31 U.S.C. § 6101 note.

withholding payments to the contractor, or recovering funds from illegal or improper activity.

Civil and Criminal Remedies: The Department of Justice solely handles civil and criminal remedies for contracting fraud. DOD works with the Department of Justice to assist in coordinating these remedies for applicable cases. Both civil and criminal remedies could involve financial penalties such as fines; criminal remedies may also involve imprisonment. In December 2019, the DOD OIG reported that the Department of Justice, based on work performed by DOD OIG's Defense Criminal Investigative Service, prosecuted five contractors for participating in a bid rigging and fraud conspiracy. The contractors were charged more than $155 million in criminal fines and more than $205 million in damages and civil penalties—the largest criminal and civil settlements ever obtained under antitrust laws.[20]

Applicable federal criminal and civil laws allow the Department of Justice to seek convictions or judgments of liability for certain instances of fraud. However, because fraud convictions and judgments generally take years to occur, the government could be vulnerable to additional fraud during this timeframe. Therefore, even before allegations of fraud are fully investigated and prosecuted or litigated, DOD coordinates both internally and with the Department of Justice to apply a range of applicable administrative and contractual remedies used to protect the government during fraud investigations.

In 2014, DOD updated its *Instruction 7050.05 Coordination of Remedies for Fraud and Corruption Related to Procurement Activities.*[21] The purpose of the instruction is to ensure that DOD coordinates internally, and also with the Department of Justice, to efficiently pursue all appropriate remedies—including administrative, contractual, civil, and criminal—in applicable cases. The instruction stresses early engagement of remedies. According to DOD's guidance, during an investigation and before prosecution or litigation and when based in whole or in part on evidence developed during an investigation, administrative and contractual remedies are taken only with the advance knowledge of the responsible defense criminal investigative organization, as well as

[20]Office of Inspector General, DOD, Semiannual Report to the Congress, April 1, 2019, through September 30, 2019 (Alexandria, Va.: Dec. 2, 2019).

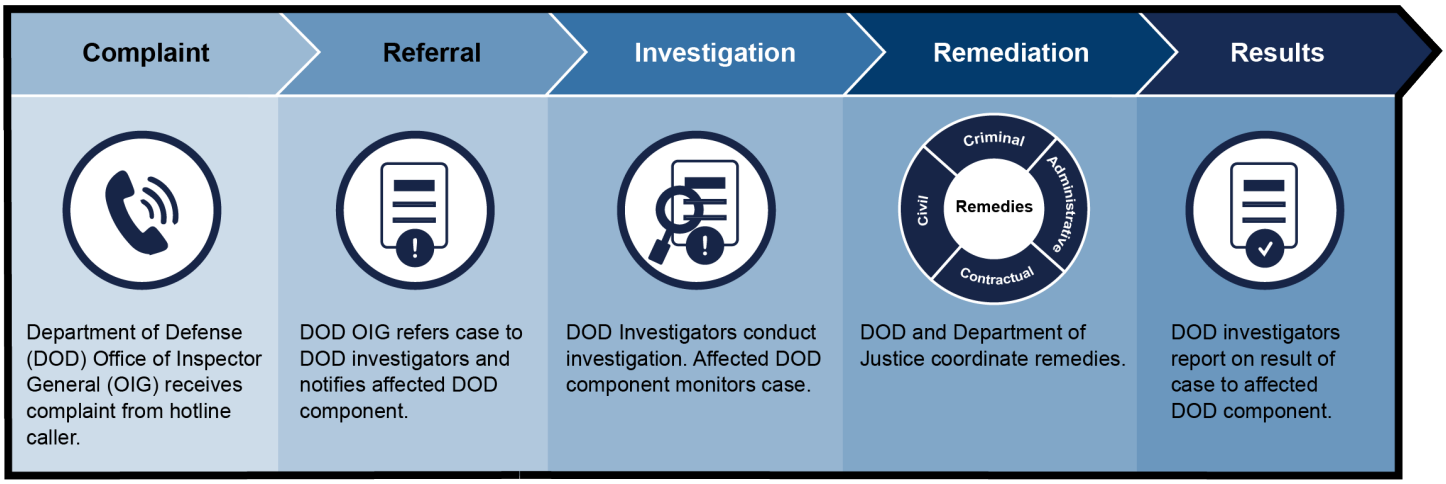
[21]DOD Instruction 7050.05, *Coordination of Remedies for Fraud and Corruption Related to Procurement Activities* (May 12, 2014).

appropriate legal counsel within both DOD and the Department of Justice. Further, these remedies may be taken only after the Department of Justice identifies any potential adverse effect to the ongoing criminal or civil case.

In a hypothetical example of a contractor alleged to have fraudulently provided counterfeit aircraft parts, DOD and the Department of Justice would coordinate to pursue all appropriate remedies. The respective contracting officer at DOD could pursue contractual remedies such as enforcing the contractor to correct the parts and terminating the contract. A DOD Suspension and Debarment official could pursue administrative remedies such as suspension and debarment. Meanwhile, the Department of Justice could pursue a civil remedy—monetary penalties, and a criminal remedy—additional monetary penalties or imprisonment. An official from the U.S. Army Criminal Investigation Command told us that remedies are tools to address fraud and can be used in any sequence, but need to be balanced between options that decrease the effect of the fraud while not compromising the ongoing investigation.

The DOD OIG—central to DOD's response to contracting fraud—monitors the implementation of, and compliance with, the provisions of DOD Instruction 7050.05. DOD OIG's Defense Criminal Investigative Service investigates fraud allegations for contracts awarded by non-military DOD components, and those involving multiple military services, the top 100 companies with revenues from defense contracts, and violations of antitrust laws. The respective military criminal investigative organizations investigate fraud allegations for contracts awarded by the respective service. Figure 10 describes the process for the investigation and coordinated remediation of a hypothetical fraud case, once an allegation is reported to the DOD OIG.

Figure 10: Process for a Fraud Case Based on a Department of Defense Hotline Tip



Source: GAO analysis of DOD documents. | GAO-21-309

Text of Figure 10: Process for a Fraud Case Based on a Department of Defense Hotline Tip

Complaint	Referral	Investigation	Remediation	Results
Department of Defense (DOD) Office of Inspector General (OIG) receives complaint from hotline caller.	DOD OIG refers case to DOD investigators and notifies affected DOD component.	DOD Investigators conduct investigation. Affected DOD component monitors case.	DOD and Department of Justice coordinate remedies.	DOD investigators report on result of case to affected DOD component.

Source: GAO analysis of DOD documents. | GAO-21-309

Appendix III: Comments from the Department of Defense

ACQUISITION AND SUSTAINMENT

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

Mr. Seto Bagdoyan
Director, Forensic Audits and Investigative Services
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Mr. Bagdoyan:

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report, GAO-21-309SU, "DOD FRAUD RISK MANAGEMENT: Actions Needed to Enhance Department-wide Approach, Focusing on Procurement Fraud Risks," dated June 10, 2021 (GAO Code 103252).

The DoD response to each recommendation is enclosed. My point of contact is Mr. Jeff Grover, 703-697-9352 or jeffrey.c.grover.civ@mail.mil.

Sincerely,

CALISTI.SCOTT.R.1028133959 Digitally signed by CALISTI.SCOTT.R.1028133959 Date: 2021.07.16 16:53:16 -04'00'

for John M. Tenaglia
Principal Director,
Defense Pricing and Contracting

Enclosure:
As stated

Enclosure

GAO DRAFT REPORT DATED JUNE 10, 2021
GAO-21-309SU (GAO CODE 103252)

"DOD FRAUD RISK MANAGEMENT: Actions Needed to Enhance Department-wide Approach, Focusing on Procurement Fraud Risks"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The Deputy Chief Financial Officer should ensure that cognizant DOD components designate representatives to the Fraud Reduction Task Force as expeditiously as possible.

DoD RESPONSE: Concur. As discussed during the audit, the Deputy Chief Financial Officer (DCFO) has incorporated identifying Component-level Fraud Reduction Task Force representatives into the Fiscal Year (FY) 2021 Statement of Assurance Execution Handbook. As of June 2021, all but four of the DoD Components have designated representatives to the Fraud Reduction Task Force. The DCFO is working with these remaining DoD Components to designate the appropriate representatives.

RECOMMENDATION 2: The Comptroller should update DOD Instruction 5010.40 to include fraud risk assessment and reporting requirements. Specifically, the instruction should (1) distinguish fraud risk assessment and reporting requirements from financial reporting requirements and (2) clarify that components must report all fraud risks, including fraud risks that are not categorized as a material weakness or significant deficiency.

DoD RESPONSE: Concur, this is part of the ongoing updates we have been working on with regards to DoD Instruction 5010.40.

RECOMMENDATION 3: The Comptroller should update its *Statement of Assurance Execution Handbook* to clarify that components should report all fraud risks, including fraud risks that are not categorized as a material weakness or significant deficiency.

DoD RESPONSE: Nonconcur. The Department does not concur because the FY 2021 Statement of Assurance Handbook currently requests that Components report all fraud risks, including fraud risks that are not categorized as a material weakness or significant deficiency. Per pages 45-46 in the FY 2021 Statement of Assurance Execution Handbook, the following guidance was provided with regard to the Fraud Risks: For the Fraud Risk Category, DoD Components must annually identify fraud risks related to payroll, beneficiary payments, grants, procurement, information technology and security, asset safeguards, purchase, travel, fleet cards, opaque contractor ownership, contingency/emergency programs (e.g., CARES Act related risks), and commissary. These focus areas are listed in the template under the "Fraud Risk Category" column. Fraud risks related to focus areas must be reported under the "Other" Fraud Risk Subcategory.

As such, the DoD Components are already required to submit all fraud risks, not just risks related to significant deficiencies or material weaknesses.

RECOMMENDATION 4: The Comptroller should determine and document the fraud risk management roles and responsibilities of all oversight officials, including department-wide Assessable Unit Senior Accountable Officials and their Action Officers and the Defense Business Council, and the chain of accountability for implementing DOD's fraud risk management approach.

DoD RESPONSE: Nonconcur. As directed by the DCFO, the Assessable Unit Senior Accountable Officials' and Action Officers' primary role is to support driving audit progressand mitigating Department-wide material weaknesses. OUSD(C) will internally discuss any potentially required updates regarding the Assessable Unit Senior Accountable Officials' and Action Officers' roles and responsibilities.

Additionally, the Office of the Under Secretary of Defense for Acquisition and Sustainment established the DoD-wide Procurement Fraud Working Group in January 2005 to develop a closer working relationship among the relevant DoD activities and Agencies involved in the identification, investigation, and prosecution of procurement fraud. Specifically, the DoD-wide Procurement Fraud Working Group provides a forum for information exchange, legislative/policy development, and continuing education with regard to current issues, future national trends, investigative strategies, appropriate remedies, and enforcement problems in the procurement fraud arena. As fraud remediation activities are identified, the Working Group will coordinate efforts to resolve and implement solutions.

RECOMMENDATION 5: The Comptroller should direct components, as part of the annual statement of assurance process, to plan and conduct regular fraud risk assessments that align with leading practices in the *Fraud Risk Framework*. Specifically, the assessment process should include (1) identifying inherent procurement fraud risks, (2) assessing the likelihood and impact of these risks, (3) determining fraud risk tolerance, (4) examining the suitability of existing fraud controls, and (5) compiling and documenting the fraud risk profile.

DoD RESPONSE: Partially concur. The current guidance for the Statement of Assurance Risk Assessment Template (as outlined in the Statement of Assurance Execution Handbook) incorporates fraud, operational, financial, and systems risks. The guidance for the template is on page 44 of the handbook and noted below.

The Risk Assessment Template has been developed to assist the DoD Components in identifying and compiling the most significant financial and non-financial risks relevant to their individual Component as well as those that may have enterprise wide applicability. Identified risks should be prioritized based on an assessment of risks' likelihood and impact, as well as consideration of the level of direct alignment of each risk to the ability to accomplish strategic objectives as articulated in the National Defense Strategy and National Defense Business Operations Plan (NDBOP). In addition, risks are to be aligned to specific DoD Component objectives and the actions taken to manage those risks. For risks not appropriately mitigated, risk response plans

must be developed to manage key risks, and should take into account existing activities in place to include internal controls.

The DCFO will update this language for FY 2022 to specifically call out the inclusion of fraud risks in the Statement of Assurance Risk Assessment Template.

Text of Appendix III: Comments from the Department of Defense

Mr. Seto Bagdoyan

Director, Forensic Audits and Investigative Services

U.S. Government Accountability Office 441 G Street, NW

Washington DC 20548

Dear Mr. Bagdoyan:

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report, GAO-21-309SU, “DOD FRAUD RISK MANAGEMENT: Actions

Needed to Enhance Department-wide Approach, Focusing on Procurement Fraud Risks,” dated June 10, 2021 (GAO Code 103252).

The DoD response to each recommendation is enclosed. My point of contact is Mr. Jeff Grover, 703-697-9352 or jeffrey.c.grover.civ@mail.mil.

Sincerely

John M. Tenaglia Principal Director,

Defense Pricing and Contracting

Enclosure: As stated

GAO DRAFT REPORT DATED JUNE 10, 2021 GAO-21-309SU (GAO CODE 103252) “DOD FRAUD RISK MANAGEMENT:

Actions Needed to Enhance Department-wide Approach, Focusing on Procurement Fraud Risks”

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The Deputy Chief Financial Officer should ensure that cognizant DOD components designate representatives to the Fraud Reduction Task Force as expeditiously as possible.

DoD RESPONSE: Concur. As discussed during the audit, the Deputy Chief Financial Officer (DCFO) has incorporated identifying Component-level Fraud Reduction Task Force representatives into the Fiscal Year (FY) 2021 Statement of Assurance Execution Handbook. As of June 2021, all but four of the DoD Components have designated representatives to the Fraud Reduction Task Force. The DCFO is working with these remaining DoD Components to designate the appropriate representatives.

RECOMMENDATION 2: The Comptroller should update DOD Instruction 5010.40 to include fraud risk assessment and reporting requirements. Specifically, the instruction should (1) distinguish fraud risk assessment and reporting requirements from financial reporting requirements and (2) clarify that components must report all fraud risks, including fraud risks that are not categorized as a material weakness or significant deficiency.

DoD RESPONSE: Concur, this is part of the ongoing updates we have been working on with regards to DoD Instruction 5010.40.

RECOMMENDATION 3: The Comptroller should update its Statement of Assurance Execution Handbook to clarify that components should report all fraud risks, including fraud risks that are not categorized as a material weakness or significant deficiency.

DoD RESPONSE: Nonconcur. The Department does not concur because the FY 2021 Statement of Assurance Handbook currently requests that Components report all fraud risks, including fraud risks that are not categorized as a material weakness or significant deficiency. Per pages 45-46 in the FY 2021 Statement of Assurance Execution Handbook, the following guidance was provided with regard to the Fraud Risks: For the Fraud Risk Category, DoD Components must annually identify fraud risks related to payroll, beneficiary payments, grants, procurement, information technology and security, asset safeguards, purchase, travel, fleet cards, opaque contractor ownership, contingency/emergency programs (e.g., CARES Act related risks), and commissary. These focus areas are listed in the template under the

"Fraud Risk Category" column. Fraud risks related to focus areas must be reported under the "Other" Fraud Risk Subcategory.

As such, the DoD Components are already required to submit all fraud risks, not just risks related to significant deficiencies or material weaknesses.

RECOMMENDATION 4: The Comptroller should determine and document the fraud risk management roles and responsibilities of all oversight officials, including department-wide Assessable Unit Senior Accountable Officials and their Action Officers and the Defense Business Council, and the chain of accountability for implementing DOD's fraud risk management approach.

DoD RESPONSE: Nonconcur. As directed by the DCFO, the Assessable Unit Senior Accountable Officials' and Action Officers' primary role is to support driving audit progressand mitigating Department-wide material weaknesses. OUSD(C) will internally discuss any potentially required updates regarding the Assessable Unit Senior Accountable Officials' and Action Officers' roles and responsibilities.

Additionally, the Office of the Under Secretary of Defense for Acquisition and Sustainment established the DoD-wide Procurement Fraud Working Group in January 2005 to develop a closer working relationship among the relevant DoD activities and Agencies involved in the identification, investigation, and prosecution of procurement fraud. Specifically, the DoD-wide Procurement Fraud Working Group provides a forum for information exchange, legislative/policy development, and continuing education with regard to current issues, future national trends, investigative strategies, appropriate remedies, and enforcement problems in the procurement fraud arena. As fraud remediation activities are identified, the Working Group will coordinate efforts to resolve and implement solutions.

RECOMMENDATION 5: The Comptroller should direct components, as part of the annual statement of assurance process, to plan and conduct regular fraud risk assessments that align with leading practices in the Fraud Risk Framework. Specifically, the assessment process should include (1) identifying inherent procurement fraud risks, (2) assessing the likelihood and impact of these risks, (3) determining fraud risk tolerance, (4) examining the suitability of existing fraud controls, and (5) compiling and documenting the fraud risk profile.

DoD RESPONSE: Partially concur. The current guidance for the Statement of Assurance Risk Assessment Template (as outlined in the Statement of Assurance Execution Handbook) incorporates fraud, operational, financial, and systems risks. The guidance for the template is on page 44 of the handbook and noted below.

The Risk Assessment Template has been developed to assist the DoD Components in identifying and compiling the most significant financial and non-financial risks relevant to their individual Component as well as those that may have enterprise wide applicability. Identified risks should be prioritized based on an assessment of risks' likelihood and impact, as well as consideration of the level of direct alignment of each risk to the ability to accomplish strategic objectives as articulated in the National Defense Strategy and National Defense Business Operations Plan (NDBOP). In addition, risks are to be aligned to specific DoD Component objectives and the actions taken to manage those risks. For risks not appropriately mitigated, risk response plans must be developed to manage key risks, and should take into account existing activities in place to include internal controls.

The DCFO will update this language for FY 2022 to specifically call out the inclusion of fraud risks in the Statement of Assurance Risk Assessment Tem

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Seto J. Bagdoyan at (202) 512-6722, BagdoyanS@gao.gov

Staff Acknowledgments

In addition to the contact named above, Heather Dunahoo; Tatiana Winger; Pamela Davidson (Assistant Directors); Paulissa Earl; Ranya Elias; Colin Fallon; Jennifer Felder; Lisa Fisher; Maria McMullen; James Murphy; Joy Myers; and Amber Lopez Roberts 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

Orice Williams Brown, Managing Director, WilliamsO@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, (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, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548