



February 2024

DOD FRAUD RISK MANAGEMENT

Enhanced Data Analytics Can Help Manage Fraud Risks

Accessible Version

DOD FRAUD RISK MANAGEMENT

Enhanced Data Analytics Can Help Manage Fraud Risks

Why GAO Did This Study

DOD is the largest contracting agency in the federal government—with contract obligations of \$414.5 billion in fiscal year 2022 for a wide range of goods and services. In 2021, GAO found that DOD had taken initial steps to combat fraud risks but had not implemented a comprehensive approach.

GAO was asked to broadly review DOD’s fraud risk management as related to contracting. This report examines (1) if DOD’s fraud risk management strategy provides the needed direction for fraud-related data-analytics activities and (2) the extent to which analyses of DOD investigative data on alleged and adjudicated procurement fraud cases can help inform fraud risk management.

GAO analyzed DOD’s fraud risk management strategy against leading practices. GAO also analyzed investigative data for fiscal years 2015 through 2021 for closed, unsealed, unclassified cases. GAO compared DOD’s practices related to the usability of investigative data for fraud risk management and the use of investigative information with federal internal control standards and leading practices for fraud risk management. GAO also selected a nongeneralizable sample of eight cases, two from each DCIO, for illustrative information regarding the cases investigated.

What GAO Recommends

GAO is making 11 recommendations to DOD and the DOD OIG. This includes DOD establishing data analytics as a method for fraud risk management and providing the direction needed on data analytics in its strategy.

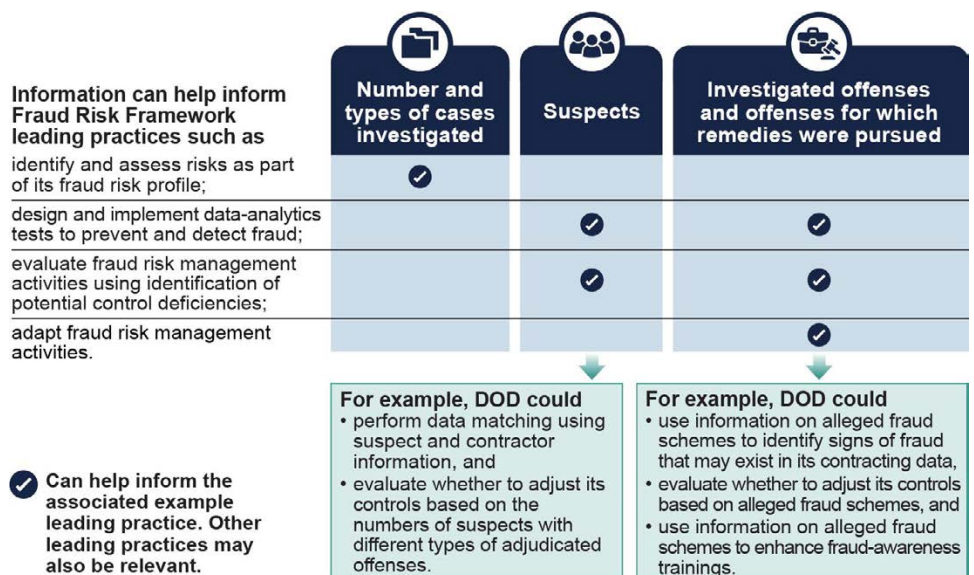
What GAO Found

The Department of Defense (DOD) issued an updated fraud risk management strategy in August 2023. Contrary to leading practices, the strategy does not establish data analytics as a method for fraud risk management or provide the direction needed to conduct such data analytics. Data analytics are control activities that can be used to prevent and detect fraud. Data analytics can include a variety of techniques, such as data matching. Data matching can be used to verify key information to determine eligibility to receive federal contracts. For example, if an entity reports that it is a small business in order to receive federal contracts, DOD can use third-party data sources to verify that the entity actually meets requirements to qualify as a small business.

DOD’s strategy refers generally to data analytics but does not establish it as a specific fraud risk management control activity. Accordingly, the strategy does not identify which DOD entity has the authority to ensure that fraud-related data-analytics activities are planned and implemented. The strategy does not establish clear roles and responsibilities for all entities with data-analytics roles. It also does not provide timelines for designing and implementing data-analytics activities. As a result, DOD is missing an opportunity to provide direction in areas that are critical to achieving its data-analytics goals and managing fraud risks.

GAO analyses demonstrate how information from investigative case data on alleged and adjudicated procurement fraud could help inform DOD’s fraud risk management consistent with leading practices in GAO’s Fraud Risk Framework, despite existing data limitations (see fig.).

Examples of Data Collected by the Department of Defense That Could Help Inform Its Fraud Risk Management



Sources: GAO analysis of Department of Defense (DOD) data; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

Accessible Text for Examples of Data Collected by the Department of Defense That Could Help Inform Its Fraud Risk Management

Information can help inform Fraud Risk Framework leading practices such as	Number and types of cases investigated	Suspects	Investigated offenses and offenses for which remedied were pursued
Identify and assess risks as part of its fraud risk profile;	Can help inform the associated example leading practice. Other leading practices may also be relevant.		
Design and implement data-analytics tests to prevent and detect fraud;		Can help inform the associated example leading practice. Other leading practices may also be relevant.	Can help inform the associated example leading practice. Other leading practices may also be relevant.
Evaluate fraud risk management activities using identification of potential control deficiencies;		Can help inform the associated example leading practice. Other leading practices may also be relevant.	Can help inform the associated example leading practice. Other leading practices may also be relevant.
Adapt fraud risk management activities.			Can help inform the associated example leading practice. Other leading practices may also be relevant.

Information can help inform Fraud Risk Framework leading practices such as	Number and types of cases investigated	Suspects	Investigated offenses and offenses for which remedied were pursued
		<p>For example, DOD could:</p> <ul style="list-style-type: none"> perform data matching using suspect and contractor information, and evaluate whether to adjust its controls based on the numbers of suspects with different types of adjudicated offenses. 	<ul style="list-style-type: none"> For example, DOD could: <ul style="list-style-type: none"> use information on alleged fraud schemes to identify signs of fraud that may exist in DOD's contracting data and enhance fraud-awareness trainings, Evaluate whether to adjust its controls based on alleged fraud schemes, and use information on alleged fraud schemes to enhance fraud-awareness trainings.

Sources: GAO analysis of Department of Defense (DOD) data; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

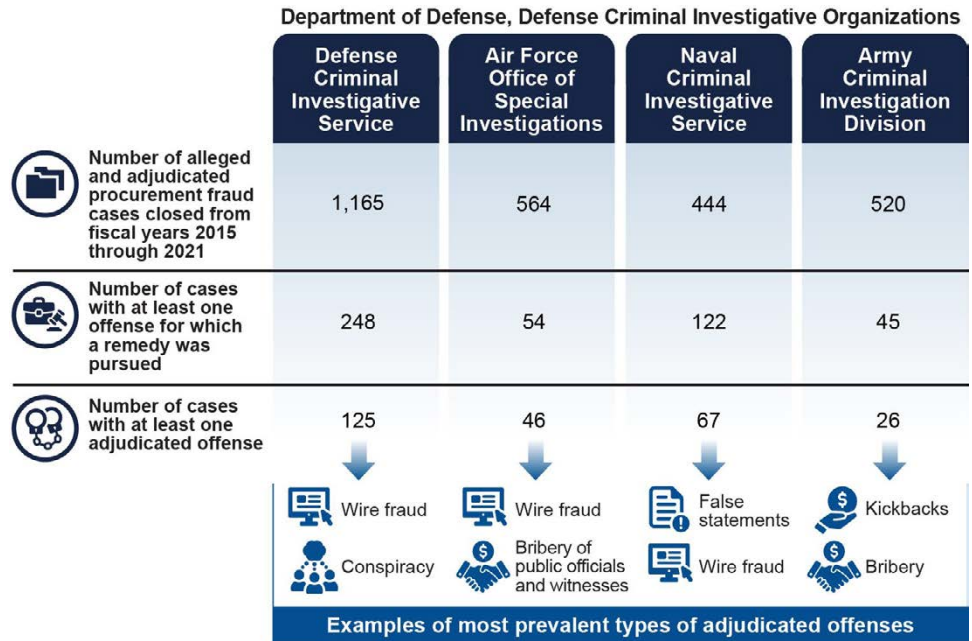
For example, Defense Criminal Investigative Organizations (DCIO) collect data that describe the extent of detected alleged fraud through the number and types

its strategy. It also includes improving the usability of investigative data by DOD for fraud risk management and obtaining and analyzing information from adjudicated procurement fraud cases. Additionally, it includes a recommendation to DOD OIG that it collaborate, as appropriate, on the development of leading practices towards improving the usability of investigative data by DOD for fraud risk management purposes. DOD agreed with some, but not all of the recommendations. DOD OIG agreed with all applicable recommendations. GAO continues to believe that all of the recommendations are warranted and should be implemented in a timely fashion, as discussed in this report.

View [GAO-24-105358](#). For more information, contact Seto J. Bagdoyan at (202) 512-6722 or bagdoyans@gao.gov.

of cases investigated. Using these data, GAO found that the number of alleged and adjudicated procurement fraud cases closed from fiscal years 2015 through 2021 ranged from 444 for the Naval Criminal Investigative Service (NCIS) to 1,165 for the Defense Criminal Investigative Service, a component of the DOD Office of Inspector General (OIG) (see fig.). Such information could help DOD identify and assess risks as part of its fraud risk profile. Specifically, information on the number and types of cases investigated could help DOD (1) identify procurement fraud risks and the likelihood and impact of those risks and (2) prioritize the fraud risks.

Information from Analyses of Investigative Data from Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021



Sources: GAO analysis of Department of Defense data; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

Accessible Data for Information from Analyses of Investigative Data from Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021

Department of Defense, Defense Criminal Investigative Organizations

	Defense Criminal Investigative Service	Air Force Office of Special Investigations	Naval Criminal Investigative Service	Army Criminal Investigation Division
Number of alleged and adjudicated procurement fraud cases closed from fiscal years 2015 through 2021	1,165	564	444	520
Number of cases with at least one offense for which a remedy was pursued	248	54	122	45

Department of Defense, Defense Criminal Investigative Organizations				
	Defense Criminal Investigative Service	Air Force Office of Special Investigations	Naval Criminal Investigative Service	Army Criminal Investigation Division
Number of cases with at least one adjudicated offense	125	46	67	26
Examples of most prevalent types of adjudicated offenses	<ul style="list-style-type: none"> • Wire fraud • Conspiracy 	<ul style="list-style-type: none"> • Wire fraud • Bribery of public officials and witnesses 	<ul style="list-style-type: none"> • False statements • Wire fraud 	<ul style="list-style-type: none"> • Kickbacks • Bribery

Sources: GAO analysis of Department of Defense data; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

DCIOs also collect data describing the number and types of investigated offenses and offenses for which remedies were pursued. For example, GAO found that the most prevalent investigated offense in the 444 NCIS cases identified was false, fictitious, or fraudulent claims. GAO also found that this was the most prevalent offense for which remedies were pursued in the NCIS cases. This information could help DOD take actions, such as enhancing its fraud-awareness trainings to provide details on how these frauds were detected, to aid in preventing similar future fraud.

Information about adjudicated offenses can help DOD better understand the impact of procurement fraud risks, including the financial and reputation impacts. With this information, DOD would be better able to determine its fraud risk tolerance.

GAO's analyses revealed that investigative data on alleged and adjudicated procurement fraud cases were not always complete and could not always be readily analyzed, for various reasons. For example, some investigative data lacked a structured data field identifying cases as involving alleged or adjudicated procurement fraud, requiring analysis of narrative fields. Being able to readily identify such cases would facilitate DOD's fraud risk management.

DOD does not have plans to obtain and analyze relevant information from adjudicated procurement fraud cases. Without obtaining such information, DOD may not fully assess its fraud risks or design and implement data-analytics activities to prevent or detect these risks.

Contents

GAO Highlights		ii
	Why GAO Did This Study	ii
	What GAO Recommends	ii
	What GAO Found	ii
Letter		1
	Background	7
	DOD's Strategy Refers to Data Analytics but Does Not Establish It as a Fraud Risk Management Method	21
	Our Analyses Demonstrate the Usefulness and Feasibility of Using DOD Investigative Data to Inform Fraud Risk Management, Despite Limitations	35
	Conclusions	85
	Recommendations for Executive Action	87
	Agency Comments and Our Evaluation	89
Appendix I: Objectives, Scope, and Methodology		97
Appendix II: Summary of Eight Selected Defense Criminal Investigative Organization Procurement Fraud Cases		109
Appendix III: Department of Defense Reporting to Congress on Procurement Fraud		145
Appendix IV Comments from the Department of Defense		152
Accessible Text for Appendix IV Comments from the Department of Defense		160
Appendix V Comments from the Department of Defense Office of Inspector General		168
Accessible Text for Appendix V Comments from the Department of Defense Office of Inspector General		173
Appendix VI: GAO Contact and Staff Acknowledgments		178
	GAO Contact:	178
	Staff Acknowledgments:	178
Tables		
Table 1: Status of Recommendations to the Department of Defense (DOD) in GAO-21-309		14
Table 2: Department of Defense, Defense Criminal Investigative Organizations and Their Respective Case Management Systems	19	

Table 3: Number of Cases with Recorded Adjudicated Offenses and Example Nonadjudicative Outcomes among Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021	63
Table 4: Case 1 – Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021	112
Table 5: Case 2 - Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021	116
Table 6: Case 3 - Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021	120
Table 7: Case 4 - Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021	123
Table 8: Case 5 - Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021	126
Table 9: Case 6 - Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021	130
Table 10: Case 7 - Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021	138
Table 11: Case 8 - Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021	143
Table 12: Recovered Funds from Department of Defense (DOD) Contracting Fraud Cases from Fiscal Years 2013 to 2017, as Reported in 2018	147

Figures

Examples of Data Collected by the Department of Defense That Could Help Inform Its Fraud Risk Management	ii
Accessible Text for Examples of Data Collected by the Department of Defense That Could Help Inform Its Fraud Risk Management	iii
Information from Analyses of Investigative Data from Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021	v
Accessible Data for Information from Analyses of Investigative Data from Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021	v
Figure 1: Fiscal Year 2022 Department of Defense’s Obligations for Contracting Activity Compared with Civilian Federal Agencies	8
Accessible Data for Figure 1: Fiscal Year 2022 Department of Defense’s Obligations for Contracting Activity Compared with Civilian Federal Agencies	9

Figure 2: Four Components of the Fraud Risk Framework and Relevant Leading Practices	10
Accessible Text for Figure 2: Four Components of the Fraud Risk Framework and Relevant Leading Practices	11
Figure 3: Key Department of Defense (DOD) Entities with Fraud Risk Management Data Analytics Roles and Responsibilities	25
Accessible Text for Figure 3: Key Department of Defense (DOD) Entities with Fraud Risk Management Data Analytics Roles and Responsibilities	26
Figure 4: Examples of Data Collected by the Department of Defense That Could Help Inform Fraud Risk Management	38
Accessible Text for Figure 4: Examples of Data Collected by the Department of Defense That Could Help Inform Fraud Risk Management	39
Figure 5: Number of Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021, by Defense Criminal Investigative Organization	42
Accessible Data for Figure 5: Number of Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021, by Defense Criminal Investigative Organization	42
Figure 6: Range of Number of Known Suspects per Case in Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021	46
Accessible Data for Figure 6: Range of Number of Known Suspects per Case in Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021	46
Figure 7: Number of Suspects by Adjudicated Offense Status for Department of Defense Investigations of Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021	47
Accessible Data for Figure 7: Number of Suspects by Adjudicated Offense Status for Department of Defense Investigations of Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021	47
Figure 8: Suspects Involved in Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021 for the Defense Criminal Investigative Service	49
Accessible Text for Figure 8: Suspects Involved in Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021 for the Defense Criminal Investigative Service	49
Figure 9: Most Prevalent Offenses Investigated for Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021	54
Accessible Data for Figure 9: Most Prevalent Offenses Investigated for Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021	55
Figure 10: Most Prevalent Offenses for Which Remedies Were Pursued for Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021	58

Accessible Data for Figure 10: Most Prevalent Offenses for Which Remedies Were Pursued for Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021	59	
Figure 11: Most Prevalent Types of Adjudicated Offenses among Closed Department of Defense Procurement Fraud Cases from Fiscal Years 2015 through 2021		65
Accessible Data for Figure 11: Most Prevalent Types of Adjudicated Offenses among Closed Department of Defense Procurement Fraud Cases from Fiscal Years 2015 through 2021		66
Figure 12: Example Sentences by Suspect and Case Counts for Closed Defense Criminal Investigative Service and Naval Criminal Investigative Service Procurement Fraud Cases from Fiscal Years 2015 through 2021	72	
Accessible Data for Figure 12: Example Sentences by Suspect and Case Counts for Closed Defense Criminal Investigative Service and Naval Criminal Investigative Service Procurement Fraud Cases from Fiscal Years 2015 through 2021	72	
Figure 13: Average and Range of Case Duration for Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021		74
Accessible Data for Figure 13: Average and Range of Case Duration for Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021		75
Figure 14: Steps Taken to Identify Cases of Alleged or Adjudicated Procurement Fraud		101
Accessible Data for Figure 14: Steps Taken to Identify Cases of Alleged or Adjudicated Procurement Fraud	102	
Figure 15: Case 1 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	110	
Accessible Text for Figure 15: Case 1 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	111	
Figure 16: Case 2 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	114	
Accessible Text for Figure 16: Case 2 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	115	
Figure 17: Case 3 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	118	
Accessible Text for Figure 17: Case 3 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	119	
Figure 18: Case 4 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	121	

Accessible Text for Figure 18: Case 4 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	121
Figure 19: Case 5 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	124
Accessible Text for Figure 19: Case 5 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	125
Figure 20: Case 6 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	128
Accessible Data for Figure 20: Case 6 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	129
Figure 21: Case 7 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	134
Accessible Text for Figure 21: Case 7 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	135
Figure 22: Case 8 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	141
Accessible Text for Figure 22: Case 8 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case	142

Abbreviations

Advana	Advancing Analytics
AFOSI	Air Force Office of Special Investigations
ALERTS	Army Law Enforcement Reporting and Tracking System
BAF	Bagram Airfield
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CRIMS	Case Reporting and Information Management System
DCIO	Defense Criminal Investigative Organization
DCIS	Defense Criminal Investigative Service
DCMA	Defense Contract Management Agency
DFAS	Defense Finance and Accounting Service
DLA	Defense Logistics Agency
DOD	Department of Defense
DOJ	Department of Justice
DUNS	Data Universal Numbering System
EFT	Enterprise Financial Transformation
FBI	Federal Bureau of Investigation
FIAR	Financial Improvement and Audit Remediation
FPDS-NG	Federal Procurement Data System—Next Generation
GPC	Government Purchase Card
GPCR	Government Purchase Card Requisition
MCLB	Marine Corps Logistics Base
MCIO	military criminal investigative organization
NCIS	Naval Criminal Investigative Service
ODA&M	Office of the Director of Administration and Management
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	personally identifiable information
RCC-A	Regional Contracting Center – Afghanistan
RMIC	Risk Management Internal Control
USACID	U.S. Army Criminal Investigation Division

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



February 27, 2024

The Honorable Jamie Raskin
Ranking Member
Committee on Oversight and Accountability
House of Representatives

The Honorable Bernard Sanders
United States Senate

The Department of Defense (DOD) is responsible for about half of the federal government’s discretionary spending and about 15 percent of its total spending.¹ In fiscal year 2022, DOD obligated about \$414.5 billion for contracting activity, making it the largest contracting agency in the federal government. DOD contracts for wide-ranging goods and services, including major weapon systems, support for military bases, information technology, and consulting services.

- We have identified long-standing issues associated with DOD procurement. In 1990, we placed DOD acquisitions on our inaugural High Risk List due in part to DOD continually buying higher-cost systems that substantially exceed original estimates and do not meet the intended capabilities.²

¹Discretionary spending refers to outlays from budget authority that appropriation acts provide and control, unlike mandatory spending, such as for Medicare and other entitlement programs. For fiscal year 2022, DOD reported that it received appropriations of \$1,019.5 billion, approximately \$242.9 billion of which is considered mandatory; the remaining \$776.6 billion is discretionary. Department of Defense, *Agency Financial Report: Fiscal Year 2022* (Nov. 15, 2022).

²The High-Risk Series identifies government operations with vulnerabilities to fraud, waste, abuse, and mismanagement, or in need of transformation. GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, [GAO-23-106203](#) (Washington, D.C.: Apr. 20, 2023).

-
- In 1992, we added DOD’s contract management to the High Risk List due to challenges in its operational contract support and a fragmented approach to acquiring service contracts.³
 - In 2005, we placed DOD’s approach to business transformation on the High Risk List because of weaknesses in operations intended to support the warfighter, including processes related to managing contracts and weapon systems acquisitions.

DOD has made some progress in addressing weaknesses in these High-Risk areas, but it needs to do more to address them fully. For example, with regard to contract management, DOD has taken action to address leadership commitment, such as revising its service acquisition policy. DOD has revised, or reported that it intends to revise, responsibilities for some key acquisition positions. However, it is too early to tell whether these personnel will have the necessary capacity to perform their responsibilities. These three areas remain on our High Risk List, which was most recently updated in April 2023.

Fraud poses a significant risk to program integrity and erodes public trust in the government. Agency managers, including those at DOD, are responsible for managing fraud risks and implementing practices for combating those risks.⁴ We issued *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework) in July 2015 to serve as a guide for agency managers—during normal operations, as well as during emergencies—when developing or enhancing efforts to combat fraud in a strategic, risk-based way.⁵ The Fraud Risk Framework calls for agency managers to document an antifraud strategy that describes the agency’s approach for addressing the prioritized fraud risks identified

³Operational contract support is the process of planning for and obtaining supplies, services, and construction from commercial sources in support of combatant commander-directed operations, as well as combatant commander-directed, single-Service activities, regardless of designation as a formal contingency operation or not. Joint Chiefs of Staff, Joint Pub. 4-10, *Operational Contract Support* (Mar. 4, 2019).

⁴Fraud and “fraud risk” are distinct concepts. Fraud—obtaining something of value through willful misrepresentation—is a determination to be made through the judicial or other adjudicative system. That determination is beyond management’s professional responsibility. 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.

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

during a fraud risk assessment.⁶ Key elements of an antifraud strategy include

1. establishing roles and responsibilities of those involved in fraud risk management activities, such as the antifraud entity;
2. describing the programs' activities for preventing, detecting, and responding to fraud, as well as monitoring and evaluation; and
3. creating time frames for implementing fraud risk management activities, as appropriate, including monitoring and evaluations.⁷

Data analytics can help inform fraud risk management and are a significant tool for helping agencies transition from a costly “pay-and-chase” model to an approach that is more focused on fraud prevention. Data analytics include a variety of techniques to prevent and detect fraud, and can also involve a variety of data sources, such as investigative data. For example, data-mining and data-matching techniques can enable agencies to identify potentially fraudulent payments, thus assisting agencies in recovering these dollars. Predictive analytics can identify potential fraud before making payments. As envisioned by the Fraud Risk Framework, data analytics are control activities to prevent and detect fraud. In general, the use of data analytics is a leading practice for fraud risk management. Additionally, in a fiscal year 2024 report, the DOD Office of Inspector General (OIG) identified accelerating DOD's transformation to a data-centric organization as a top challenge. The report noted DOD's aim to make data readily available and consistently used to inform decision-making but stated that the department does not consistently regard data as a strategic asset and prioritize its management throughout DOD.⁸

You asked us to review issues related to DOD's fraud risk management efforts, specifically those related to contracting. This report assesses (1) if

⁶Key elements of a fraud risk assessment process are (1) identifying inherent fraud risks affecting the program, (2) assessing the likelihood and impact of inherent fraud risks, (3) determining fraud risk tolerance, (4) examining the suitability of existing fraud controls and prioritizing residual fraud risks, and (5) documenting the program's fraud risk profile. [GAO-15-593SP](#).

⁷Other key elements of an antifraud strategy are demonstrating links to the highest internal and external residual fraud risks outlined in the fraud risk profile; and communicating the antifraud strategy to employees and other stakeholders, and link antifraud efforts to other risk activities, if any. [GAO-15-593SP](#).

⁸Department of Defense, Office of Inspector General, *Fiscal Year 2024 Top DOD Management and Performance Challenges*, (Alexandria, Virginia: November 13, 2023).

DOD's fraud risk management strategy provides the needed direction for fraud-related data-analytics activities and (2) the extent to which analyses of DOD investigative data on alleged and adjudicated procurement fraud cases can help inform fraud risk management.

To address the first objective, we analyzed DOD's fiscal year 2023 fraud risk management strategy and related guidance documents—including DOD's fiscal year 2020 fraud risk management strategy, a pertinent DOD directive, and DOD instruction. We assessed DOD's fiscal year 2023 strategy and the extent to which its discussion of data analytics aligns with relevant leading practices in the Fraud Risk Framework and a principle from *Standards for Internal Control in the Federal Government* related to establishing an organizational structure to achieve an entity's objectives.⁹ The relevant leading practices from the Fraud Risk Framework are to

- determine the risk responses and document an antifraud strategy based on the fraud risk profile—including establishing roles and responsibilities of those involved in fraud risk management activities—and
- design and implement specific control activities—including data-analytics activities—to prevent and detect fraud.¹⁰

We also interviewed officials from the Office of the Under Secretary of Defense - Comptroller and the Office of the Director of Administration and Management (ODA&M) to discuss their roles in fraud risk management, specifically with regard to data analytics and the use of Advancing Analytics (Advana), an enterprise-wide data repository.¹¹

To address the second objective, we obtained records for unclassified, unsealed, closed cases for fiscal years 2015 through 2021 from DOD's

⁹GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

¹⁰[GAO-15-593SP](#).

¹¹Advana is a centralized data and analytics platform that is the common enterprise data repository for DOD. Advana is intended to provide DOD users, including military and business decision-makers across DOD, with common business data, decision support analytics, visualization, and data tools. Advana was initially developed by the DOD Office of the Under Secretary of Defense - Comptroller and is now managed by the Chief Digital and Artificial Intelligence Office.

Defense Criminal Investigative Organizations (DCIO), which investigate contract fraud allegations.¹² The DCIOs are

- DOD OIG’s Defense Criminal Investigative Service (DCIS),
- Air Force Office of Special Investigations (AFOSI),
- Naval Criminal Investigative Service (NCIS), and
- Army Criminal Investigation Division (USACID).¹³

Specifically, we obtained records for the following numbers of cases that we identified as full investigations where DCIOs had lead or joint roles: 2,145 for DCIS; 1,208 for AFOSI; 444 for NCIS; and 906 for USACID.¹⁴ The case data provided by DCIOs may overlap, where DCIOs conducted joint investigations.

DCIS investigates fraud allegations for contracts awarded by nonmilitary DOD components and those involving multiple military services, among other contracts. AFOSI, NCIS, and USACID have primary responsibility for investigating fraud allegations within their specific military department, including investigating fraud allegations for contracts awarded by their respective military services.¹⁵ We analyzed these data to determine the extent to which the data could inform procurement fraud risk management at DOD. We reviewed relevant documents from DCIOs and interviewed DCIO officials. To assess the reliability of the data, including the extent to which they are complete and can be readily analyzed, we reviewed relevant documentation, interviewed knowledgeable agency officials, and performed electronic testing of specific data elements in DCIO data. We

¹²Our analysis focused on DCIO investigative data. Other data sources could also be used for fraud risk management.

¹³USACID provided data for cases opened and closed from fiscal years 2015 through 2021.

¹⁴We refer to the population of cases in our analysis as “alleged and adjudicated procurement fraud cases” because, while all involved alleged procurement fraud, they did not all result in adjudicated fraud. However, we found that some of the cases did result in adjudicated fraud. In addition, when describing DOD documents or information from officials, we used the terms “contracting” or “procurement” in this report to reflect the terminology used in DOD documents and by officials. However, we use “procurement” in our analysis of DOD’s implementation of relevant leading practices from GAO’s *A Framework for Managing Fraud Risks in Federal Programs* and the *Standards for Internal Control in the Federal Government* because “procurement” is the broader process through which goods and services are contracted. [GAO-15-593SP](#); and [GAO-14-704G](#).

¹⁵According to a DOD instruction, DCIOs substantially share the responsibility of conducting fraud offense investigations affecting DOD.

determined that the data were sufficiently reliable for our reporting objectives, which included reporting on key areas we identified where the data were incomplete or could not be readily analyzed.

We selected a nongeneralizable sample of eight cases, two from each DCIO, to provide illustrative information regarding the life cycle of cases investigated.¹⁶ We selected the cases using the following as primary criteria:

- cases that were investigated by each of the four DCIOs as either the lead, sole, or joint investigator;
- cases that are closed and resulted in adverse findings or actions against the contractor;
- cases illustrating a variety of the four remedies (contractual, civil, administrative, criminal);¹⁷ and
- cases illustrating a variety of offenses.

As secondary criteria, we also considered cases' geographical dispersion and availability of public information. We reviewed case file documents, including administrative proceeding documentation from DCIOs and, as necessary, the cognizant suspension and debarment officials. We also reviewed publicly available court documents and information from the System for Award Management and interviewed DCIO officials.

We reviewed DCIOs' data collection practices related to the usability of investigative data for fraud risk management purposes and DOD's practices related to its plans to obtain and analyze certain relevant information from DCIOs. We assessed the extent to which these practices align with the principle in the *Standards for Internal Control in the Federal Government* related to using quality information to achieve an entity's objectives.¹⁸ We also assessed these practices against a leading practice in the third component of the Fraud Risk Framework, that agencies establish collaborative relationships with stakeholders, including

¹⁶The intent of our case selection was to provide example illustrative information on the life cycle of cases, rather than to fully describe or to be representative of a broader population of cases.

¹⁷DOD Instruction 7050.05 outlines contractual, civil, administrative, and criminal remedies in response to procurement fraud. Department of Defense, Instruction 7050.05, *Coordination of Remedies for Fraud and Corruption Related to Procurement Activities* (May 12, 2014, incorporating change 1, effective July 7, 2020).

¹⁸[GAO-14-704G](#).

collaborating and communicating with the OIG to improve its understanding of fraud risks.

For more details on all aspects of our analysis and methods, see appendix I.

We conducted this performance audit from August 2021 to February 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

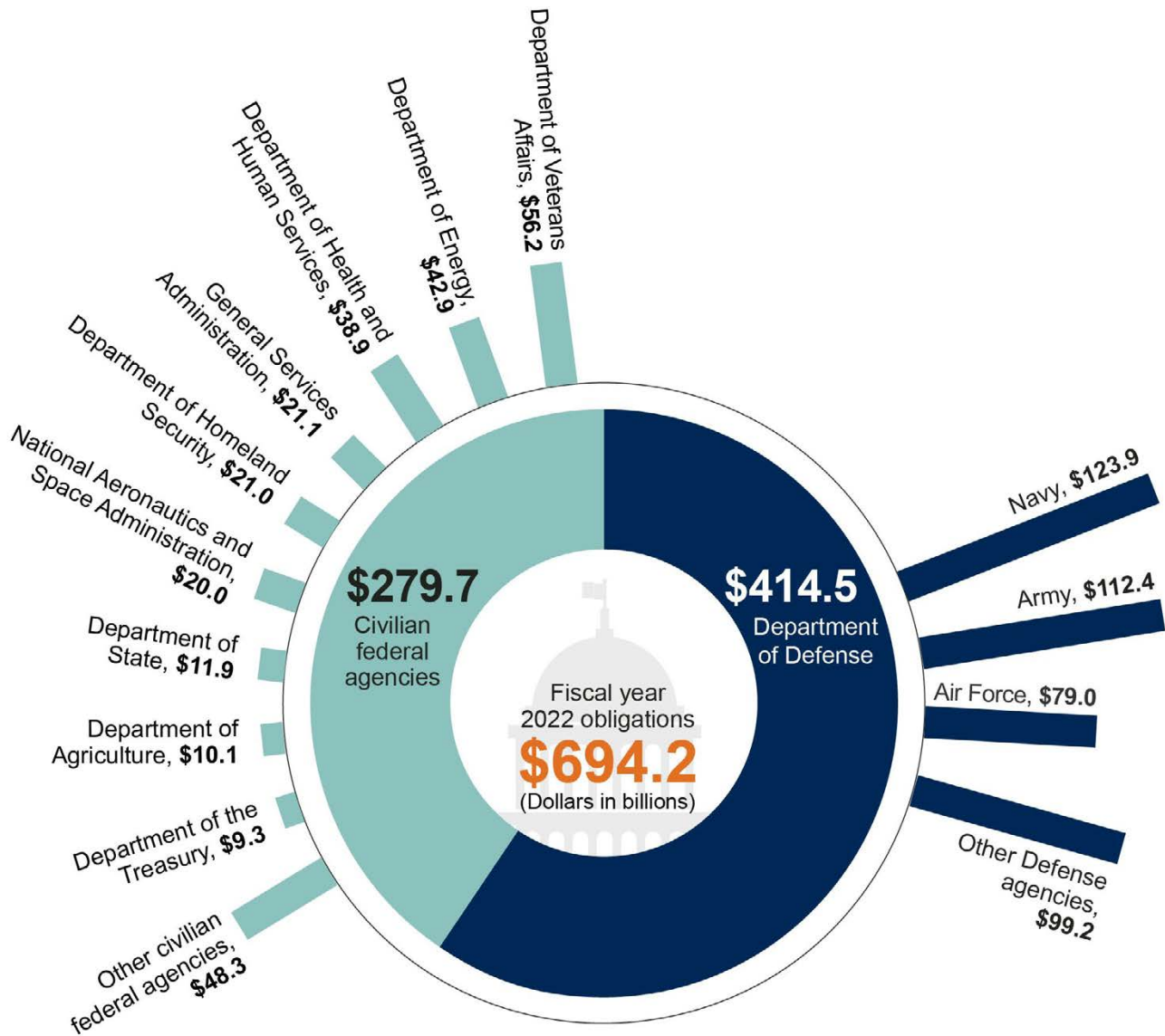
Background

DOD Contracting Obligations

During fiscal year 2022, DOD obligated about \$414.5 billion for contracting activity.¹⁹ As shown in figure 1, DOD accounted for about 60 percent of federal contracting activity, obligating more than all civilian federal agencies combined.

¹⁹At the time of our analysis, fiscal year 2022 data are the most current and complete available for the Federal Procurement Data System.

Figure 1: Fiscal Year 2022 Department of Defense’s Obligations for Contracting Activity Compared with Civilian Federal Agencies



Source: GAO analysis of fiscal year 2022 Federal Procurement Data System – Next Generation data. | GAO-24-105358

Accessible Data for Figure 1: Fiscal Year 2022 Department of Defense's Obligations for Contracting Activity Compared with Civilian Federal Agencies

Fiscal year 2022 obligations

\$694.2 (Dollars in billions)

\$414.5 Department of Defense

- Navy, \$123.9
- Army, \$112.4
- Air Force, \$79.0
- Other Defense agencies, \$99.2

\$279.7 Civilian federal agencies

- Department of Veterans Affairs, \$56.2
- Department of Energy, \$42.9
- Department of Health and Human Services, \$38.9
- General Services Administrations, \$21.1
- Department of Homeland Security, \$21.0
- National Aeronautics and Space Administration, \$20.0
- Department of State, \$11.9
- Department of Agriculture, \$10.1
- Department of the Treasury, \$9.3
- Other civilian federal agencies, \$48.3

Source: GAO analysis of fiscal year 2022 Federal Procurement Data System - Next Generation data. | GAO-24-105358

Framework for Managing Fraud Risks in the Federal Government

In July 2015, we issued the Fraud Risk Framework, which outlines four key components and a comprehensive set of leading practices to guide agency managers in combating fraud in a strategic, risk-based way.²⁰ The Fraud Reduction and Data Analytics Act of 2015 required the Office of Management and Budget (OMB) to establish guidelines for federal agencies to create controls to identify and assess fraud risks and to design and implement antifraud control activities.²¹ 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,

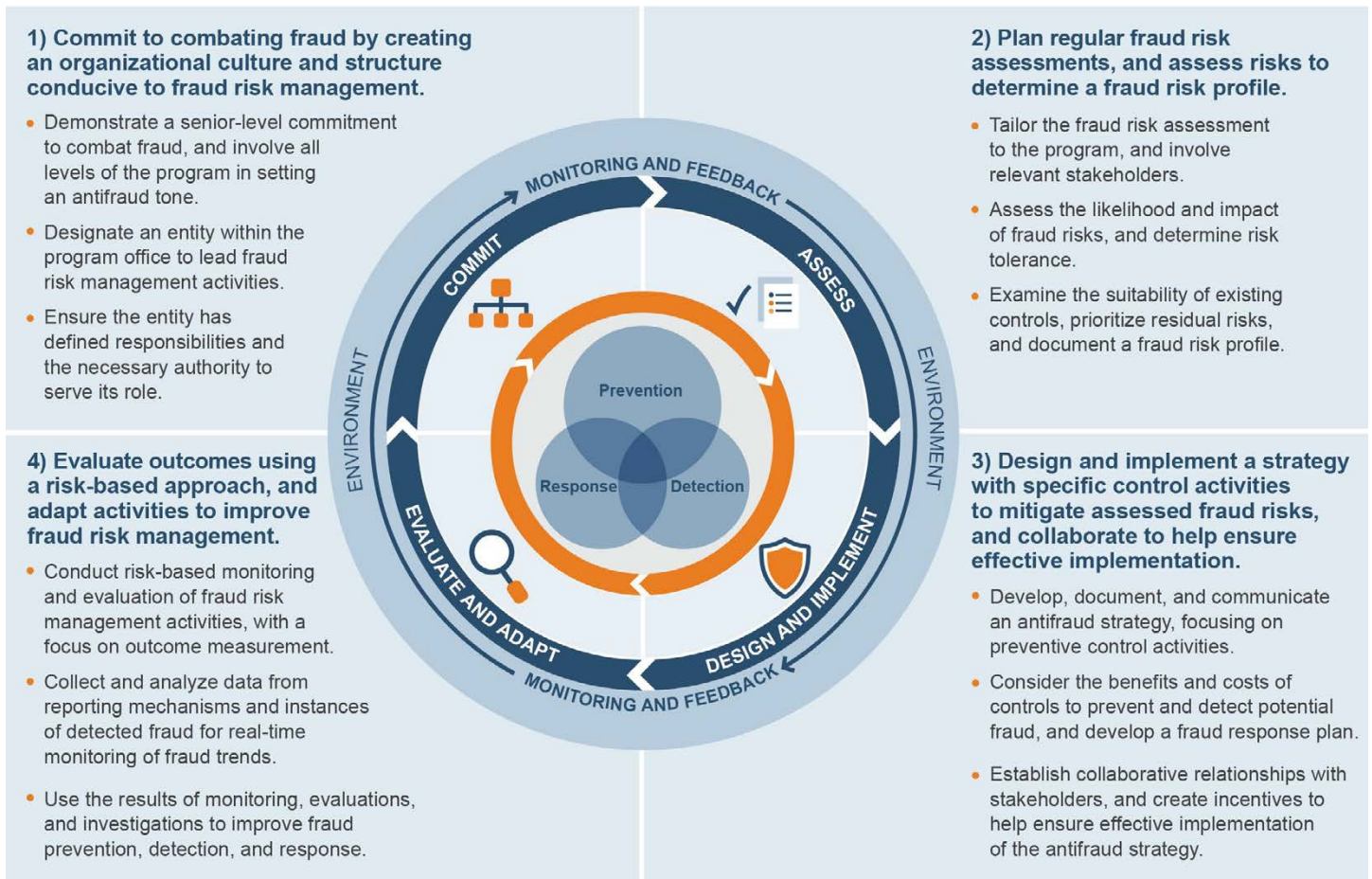
²⁰[GAO-15-593SP](#).

²¹Pub. L. No. 114-186, 130 Stat. 546 (2016).

subject to modification by OMB, as necessary, and in consultation with GAO.²²

As depicted in figure 2, the Fraud Risk Framework describes leading practices within four components: commit, assess, design and implement, and evaluate and adapt.

Figure 2: Four Components of the Fraud Risk Framework and Relevant Leading Practices



Source: GAO (information and icons). | GAO-24-105358

²²Pub. L. No. 116-117, § 2(a), 134 Stat. 113, 131 - 132 (2020), codified at 31 U.S.C. § 3357. In its 2016 Circular No. A-123 guidelines, OMB directed agencies to 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.

Accessible Text for Figure 2: Four Components of the Fraud Risk Framework and Relevant Leading Practices

- 1) Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
 - a. Demonstrate a senior-level commitment to combat fraud, and involve all levels of the program in setting an antifraud tone.
 - b. Designate an entity within the program office to lead fraud risk management activities.
 - c. Ensure the entity has defined responsibilities and the necessary authority to serve its role.
- 2) Plan regular fraud risk assessments, and assess risks to determine a fraud risk profile.
 - a. Tailor the fraud risk assessment to the program, and involve relevant stakeholders.
 - b. Assess the likelihood and impact of fraud risks, and determine risk tolerance.
 - c. Examine the suitability of existing controls, prioritize residual risks, and document a fraud risk profile.
- 3) Design and implement a strategy with specific control activities to mitigate assessed fraud risks, and collaborate to help ensure effective implementation.
 - a. Develop, document, and communicate an antifraud strategy, focusing on preventive control activities.
 - b. Consider the benefits and costs of controls to prevent and detect potential fraud, and develop a fraud response plan.
 - c. Establish collaborative relationships with stakeholders, and create incentives to help ensure effective implementation of the antifraud strategy.
- 4) Evaluate outcomes using a risk-based approach, and adapt activities to improve fraud risk management.
 - a. Conduct risk-based monitoring and evaluation of fraud risk management activities, with a focus on outcome measurement.
 - b. Collect and analyze data from reporting mechanisms and instances of detected fraud for real-time monitoring of fraud trends.
 - c. Use the results of monitoring, evaluations, and investigations to improve fraud prevention, detection, and response.

Source: GAO (information and icons). | GAO-24-105358

The Fraud Risk Framework includes several leading practices that call on agencies to consider fraud schemes and related information to help combat fraud. Under the assess component, leading practices include

- considering the financial and nonfinancial impacts of fraud risks; and
- identifying specific tools, methods, and sources for gathering information about fraud risks, including data on fraud schemes and trends from monitoring and detection activities.

Under the *design and implement* component, leading practices include

- establishing roles and responsibilities of those involved in fraud risk management activities, such as the antifraud entity;
- creating timelines for implementing fraud risk management activities;
- designing and implementing specific control activities to prevent and detect fraud, including data-analytics activities;
- considering known or previously encountered fraud schemes to design data analytics; and
- establishing collaborative relationships with stakeholders to share information on fraud risks and emerging fraud schemes and to share lessons learned related to fraud control activities. Specifically, this component notes that managers who effectively manage fraud risks collaborate and communicate with the OIG, if the agency has one, to improve their understanding of fraud risks.

Data-analytics activities, as described in the Fraud Risk Framework, are control activities that can be used to prevent and detect fraud. They can include a variety of techniques. For example, data matching, data mining, and predictive-analytics are data-analytics techniques that can be used to prevent and detect fraud.

- Data matching is a process in which information from one source is compared with information from another, such as government or third-party databases, to identify any inconsistencies. Data matching can be used to verify key information, including self-reported information and information necessary to determine eligibility, such as eligibility to receive federal contracts. For example, if an entity reports that it is a small business in order to receive federal contracts, DOD can use third-party data sources to verify that the entity actually meets requirements to qualify as a small business.
- Data mining analyzes data for relationships that have not previously been discovered. Data mining can be used to identify suspicious

activity or transactions, including anomalies and other outliers, indicating potentially fraudulent activity that warrants further investigation. Data mining can include, for example, sorting and filtering contractor transaction data to identify suspicious charges to the federal government.

- Predictive-analytics technologies include a variety of automated systems and tools that can be used to identify particular types of behavior, including potential fraud, before transactions are completed. Predictive analytics can help detect patterns of behavior that individually may not be suspicious but, when conducted together, can indicate fraudulent activity.

Under the *evaluate and adapt* component, a leading practice includes collecting and analyzing data, including data from reporting mechanisms and instances of detected fraud.

Prior GAO Reports on DOD Fraud Risk Management and Contracting Fraud

In August 2021, we reported on DOD's fraud risk management efforts and its procurement fraud risks.²³ We found that DOD had taken initial steps consistent with leading practices to combat department-wide fraud risks but had not finalized and implemented a comprehensive approach. For example:

- DOD created a Fraud Reduction Task Force to prioritize fraud risks and lead analytics activities for high-priority fraud risks, but its membership was incomplete.
- DOD uses its Risk Management Internal Control (RMIC) program, which culminates annually with a report on the design and effectiveness of key control activities, to assess and report fraud risks. However, the policy governing the program did not specifically require fraud risk assessments.
- DOD officials told us they share fraud risk information with agencies' risk management officials, but documentation of stakeholders' roles and responsibilities was incomplete.

²³GAO, *DOD Fraud Risk Management: Actions Needed to Enhance Department-Wide Approach, Focusing on Procurement Fraud Risks*, [GAO-21-309](#) (Washington, D.C.: Aug. 19, 2021).

- DOD provided an initial strategy document for combating fraud risks, but officials acknowledged that DOD’s fraud risk management efforts were in the infancy stage.

We also found that DOD had taken steps to conduct a fraud risk assessment, but some components did not report procurement fraud risks, as required by DOD.²⁴

We made recommendations to DOD, including that it take action to ensure that cognizant components designate representatives to the Fraud Reduction Task Force and to ensure that all components plan and conduct regular fraud risk assessments that align with leading practices in the Fraud Risk Framework. For all five recommendations to DOD and their status, see table 1.

Table 1: Status of Recommendations to the Department of Defense (DOD) in GAO-21-309

Recommendation	DOD response	Recommendation status and actions taken by DOD
The Deputy Chief Financial Officer should ensure that cognizant DOD components designate representatives to the Fraud Reduction Task Force.	Concurred	Closed – implemented In June 2023, DOD officials provided us with the latest Fraud Reduction Task Force roster listing 59 components, but three components did not have a representative. In November 2023, DOD provided us with an updated roster indicating that all DOD components that are required to have a task force representative now do so.
The Office of the Under Secretary of Defense – Comptroller should update a DOD instruction on its risk management internal control program to include fraud risk assessment and reporting requirements.	Concurred	Open In July 2023, DOD officials told us that they are in the process of updating DOD Instruction 5010.40. As of October 2023, the instruction had not been finalized.
The Office of the Under Secretary of Defense – Comptroller should update its <i>Statement of Assurance Execution Handbook</i> to clarify that components should report all fraud risks, including those not categorized as a material weakness or a significant deficiency.	Did not concur	Closed – implemented DOD disagreed with this recommendation at the time of our report and subsequently implemented this recommendation. In February 2024, DOD officials provided us with the Fiscal Year 2024 <i>Statement of Assurance Execution Handbook</i> , clarifying that components are to report all fraud risks in their risk assessment template. The revisions made to the Handbook remove the ambiguity about what fraud risks should be reported that was in previous editions.

²⁴Additionally, in 2023, we reported on the status of efforts government-wide to combat fraud. We identified five areas in which federal agencies needed to take additional actions to ensure they were effectively managing fraud risks, including designating an entity to lead fraud risk management, designing and implementing an antifraud strategy, and using data analytics to manage fraud risks. Data-analytics activities could include a variety of techniques, including predictive analytics, which could identify potential fraud before making payments. GAO, *Fraud Risk Management: Key Areas for Federal Agency and Congressional Action*, GAO-23-106567 (Washington, D.C.: Apr. 13, 2023).

Letter

Recommendation	DOD response	Recommendation status and actions taken by DOD
The Office of the Under Secretary of Defense – Comptroller should determine and document the fraud risk management roles and responsibilities of all oversight officials.	Did not concur	Open In July 2023, DOD officials told us that no action is planned to address this recommendation. We continue to believe this recommendation should be implemented.
The Office of the Under Secretary of Defense – 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.	Partially concurred	Open – partially addressed In July 2023, DOD officials told us that they have made progress in implementing this recommendation. DOD’s Fiscal Year 2023 <i>Statement of Assurance Execution Handbook</i> instructs components to evaluate their fraud risk management environment and report fraud risks. In October 2023, DOD provided us with the fiscal year 2023 risk assessment templates for our six selected components. Our review of these assessments found that five of the six selected components included procurement fraud risks in their assessments. We also found that the risk assessment template does not include a fraud risk tolerance.

Sources: GAO, *DOD Fraud Risk Management: Actions Needed to Enhance Department-Wide Approach, Focusing on Procurement Fraud Risks*, GAO-21-309 (Washington, D.C.: Aug. 19, 2021); and analysis of DOD policies and technical documents. | GAO-24-105358

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.²⁵ 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 System for Award Management 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, in January 2022, provided documentation of a review of fraud risks provided by components and developed guidance on identified fraud schemes and indicators related to opaque contractor ownership. Also, based on our November 2019 report, the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 requires the General Services Administration to include, for certain corporations, including those with a federal contract greater

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

than \$500,000, the identification of the corporation's beneficial owner as part of its integrity and performance database.²⁶

DOD's Updated Fraud Risk Management Strategy

In August 2023, DOD issued the updated version of its inaugural July 2020 Fraud Risk Management Strategy.²⁷ The Comptroller is in charge of maintaining this strategy. In May 2023, Comptroller officials informed us of several goals of updating the strategy. These goals include incorporating changes in DOD's fraud risk management organizational structure, incorporating stakeholder feedback, and supporting updates of DOD policy documents. In addition, a Comptroller official noted the importance of assuring that the strategy provides long-term guidance and provides clarity about DOD's fraud risk management efforts.

Organizational structure. Organizational changes have occurred since DOD issued its original 2020 strategy that affect DOD's fraud risk management structure. These changes include the repeal of the Chief Management Officer's position and the delegation of responsibilities regarding defense reform and performance improvement to the Office of the Director of Administration and Management.²⁸ The Director of Administration and Management is the Principal Staff Assistant to the Secretary of Defense on administration, organization, and management.²⁹ ODA&M provides joint oversight, along with the Comptroller, of fraud risk management activities across the department and leads enterprise risk management activities for DOD.

²⁶Pub. L. No. 116-283, Div. A, § 885, 134 Stat. 3388, 3791 (2021).

²⁷Department of Defense, *Fraud Risk Management Strategy and Guidance* (August 2023).

²⁸In 2021, the Chief Management Officer's position was repealed and its responsibilities realigned pursuant to the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021.

²⁹Principal Staff Assistants are responsible for the oversight and formulation of defense strategy, policy, and resource allocation, as well as overseeing the components under their purview. The Principal Staff Assistants are the Under Secretaries of Defense; 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.

Stakeholder feedback. As part of updating the strategy, Comptroller officials told us they obtained feedback from stakeholder groups. According to the strategy, stakeholders include

- the task force, which leads analytics activities for high-priority fraud risks;
- Principal Staff Assistants, who focus on specific fraud risk areas that support fraud risk management activities. There are 18 Principal Staff Assistants, which include, among others, the Under Secretaries of Defense, the General Counsel of DOD, and the DOD Inspector General; and
- components that implement the fraud risk management guidance and execute fraud risk management programs. There are more than 50 components, including military departments, defense agencies, DOD field activities, and combatant commands.³⁰

Updates of related policies. Comptroller officials noted that updates to the strategy required revisions to certain related DOD policy documents. Comptroller officials told us they were revising these documents to be consistent with updates to the strategy. Specifically, officials noted they had updated the strategy concurrently with the RMIC Program policy and guidance documents, including the following two documents:³¹

1. *Managers' Internal Control Program Procedures* (DOD Instruction 5010.40).³² This document establishes DOD's RMIC program. It assigns responsibilities, prescribes procedures, and provides

³⁰In addition to the task force, Principal Staff Assistants, and components, there are eight other stakeholder roles identified in the strategy. These are the Financial Improvement and Audit Remediation (FIAR) Governance Board, Comptroller, Enterprise Financial Transformation, Office of the Director of Administration and Management - Performance Improvement Directorate, Defense Criminal Investigative Service, program managers, program staff, and Assessable Unit subject matter experts.

³¹In response to OMB's requirements for an annual Statement of Assurance, 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' Statement of Assurance submissions. Executive agencies, including DOD, are required to provide an annual Statement of Assurance that represents the agency head's informed judgment as to the overall adequacy and effectiveness of the agency's internal control. As part of this process, components must annually identify fraud risks related to various focus areas, including procurement, and must also identify controls currently in place to prevent and detect fraud. [GAO-21-309](#).

³²Department of Defense, *Managers' Internal Control Program Procedures*, DOD Instruction 5010.40 (May 30, 2013, incorporating change 1, effective June 30, 2020).

guidance for the preparation and submission of the annual Statement of Assurance to the Secretary of Defense.

2. *Fiscal Year 2023 Statement of Assurance Execution Handbook*.³³ The Comptroller issues the *Statement of Assurance Execution Handbook* annually, with the most recent version issued in January 2023. It provides guidance on implementing DOD Instruction 5010.40, outlines assessment and reporting requirements for DOD officials, and provides guidance to assist components in balancing an internal controls program with risk management efforts to effectively and efficiently provide monitoring and oversight.

DOD's updated strategy also calls for the department to undertake a data-analytics pilot. Comptroller officials told us they reviewed risks reported by components and considered those risks from a DOD-wide perspective in determining where to focus data-analytic efforts. In January and February 2022, Comptroller officials told us the department was conducting a time card fraud pilot, which it had been working on since 2020. The pilot included tests focused on excessive overtime, consistent overtime, excessive reported hours, and incorrect use of leave codes.³⁴

Advancing Analytics (Advana)

Advana, the common enterprise data repository for the Department of Defense (DOD), is a centralized data and analytics platform. Advana provides DOD users, including military and business decision-makers across DOD, with common business data, decision support analytics, visualization, and data tools. Advana was initially developed by the DOD Office of the Under Secretary of Defense--Comptroller and is now managed by the Chief Digital and Artificial Intelligence Office.

The use of Advana is intended to ensure that any performance measures or data product that relies on DOD data originates from an authoritative source of transaction-level data. Additionally, Advana is intended to acquire, incorporate, and standardize data to support DOD business domain areas, including procurement analytics. For example, procurement analytics data may include vendor, pricing, and contract history data.

Source: GAO analysis of DOD documentation. | GAO-24-105358

Regarding their experience with the time card fraud pilot, Comptroller officials described to us challenges with performing data analytics. For example, Comptroller officials noted that it was difficult to ingest massive amounts of data, navigate disparate data systems, and identify a common data model. Comptroller officials noted that while Advana has the proper

³³Department of Defense, *Fiscal Year 2023 Department of Defense Statement of Assurance Execution Handbook* (January 2023).

³⁴"Consistent overtime" is defined as over 16 pay periods with over 87 hours, and "excessive reported hours" refers to charging 1,000 hours over the yearly average of 1,920 hours.

credentials to handle personally identifiable information (PII), it is not set up to allow sharing PII through interfaces. DOD officials indicated that PII are not usually used when conducting data analytics in Advana. However, when conducting data analytics for fraud risk management purposes, data analytics were executed with PII. See the sidebar for additional information on Advana.

In April 2023, Comptroller officials told us the time card pilot was on hold due to other competing priorities. For example, officials stated that they were working on developing a fraud risk dashboard.

Defense Criminal Investigative Organizations

DCIO refers to the four criminal investigative organizations at DOD. DCIS, a component of the DOD OIG, investigates fraud allegations for contracts, for example, awarded by nonmilitary DOD components and those involving multiple military services, the top 100 companies with revenues from defense contracts, and violations of antitrust laws. The three military criminal investigative organizations (MCIO)—Air Force Office of Special Investigations, Army Criminal Investigation Division, and Naval Criminal Investigative Service—investigate fraud allegations for contracts awarded by their respective services.³⁵

Each DCIO maintains a case management system, which is used to store data and monitor investigations. The DCIOs and their respective case management systems are shown in table 2.

Table 2: Department of Defense, Defense Criminal Investigative Organizations and Their Respective Case Management Systems

Defense Criminal Investigative Organization	Case management system
Defense Criminal Investigative Service – criminal investigative arm of the Department of Defense Office of Inspector General	Case Reporting and Information Management System (CRIMS)
Air Force Office of Special Investigations – major investigative service of the Air Force that reports to the Inspector General in the Office of the Secretary of Air Force	Investigative Information Management System
Army Criminal Investigation Division – major Army command law enforcement agency that reports to the Under Secretary of the Army	Army Law Enforcement Reporting and Tracking System
Naval Criminal Investigative Service – civilian law enforcement agency for the Department of the Navy that reports to the Secretary of the Navy	Consolidated Law Enforcement Operations Center

Source: GAO analysis of Department of Defense policies and technical documents. | GAO-24-105358

³⁵NCIS covers the U.S. Navy and Marine Corps. AFOSI covers the U.S. Air Force and the U.S. Space Force.

Note: In August 2023, Air Force Office of Special Investigations officials advised that a new case management system was in development.

DCIOs may initiate investigations for various reasons, including, for example, referrals from other DCIOs or agencies, or information received from a contracting office. Investigations may result in one or more types of remedies, which are actions taken to protect DOD interests and deter future incidents of fraudulent conduct. Remedies include

- administrative – could include removing a contractor from lists of qualified bidders or manufacturers or suspending or debaring a contractor;³⁶
- contractual – could include requiring a contractor to correct defects in the procured item, withholding payments to the contractor, or terminating the contract;
- civil – could involve penalties such as fines; and
- criminal – could involve penalties such as fines, as well as imprisonment.

DOD Instruction 7050.05, *Coordination of Remedies for Fraud and Corruption Related to Procurement Activities* outlines these remedies, as well as the roles, responsibilities, and procedures for DOD components, including DCIOs, centralized organizations, and DOD component heads, to follow when pursuing remedies for significant investigations of procurement fraud.³⁷ Centralized organizations are the organizations within a DOD component responsible for monitoring and ensuring the coordination of criminal, civil, administrative, and contractual remedies for each significant investigation of fraud or corruption related to procurement activities affecting that component.

³⁶Suspension takes place for a temporary period, pending the completion of an investigation or legal proceeding. Debarred contractors are ineligible to contract with the government for a specified period, 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. Suspension and debarment are not considered punishments but are meant to protect the government. 48 C.F.R. §§ 9.402, 9.406-4, and 9.407-4.

³⁷Significant investigations are fraud investigations involving an alleged loss of \$500,000 or more; all investigations of corruption involving bribery, gratuities, or conflicts of interest; all defective product, nonconforming product, counterfeit materiel, or product substitution investigations; and investigations otherwise determined to be significant by the cognizant agency official. Department of Defense, Instruction 7050.05, *Coordination of Remedies for Fraud and Corruption Related to Procurement Activities* (May 12, 2014, incorporating change 1, effective July 7, 2020).

DOD's Strategy Refers to Data Analytics but Does Not Establish It as a Fraud Risk Management Method

DOD's Fraud Risk Management Strategy generally refers to data-analytics goals, roles, responsibilities, and activities.³⁸ However, the strategy does not establish data analytics as a fraud risk management method.³⁹ It does not discuss with specificity what data analytics are to be used and how they can be used in preventing, detecting, and responding to fraud. Further, the strategy does not provide the direction needed in key areas. Specifically, the strategy does not identify which entity has the necessary authority to ensure that fraud-related data-analytics activities are implemented, does not establish clear roles and responsibilities for all entities with data-analytics roles, and does not provide timelines for designing or implementing data-analytics activities.

Key Elements of an Antifraud Strategy

Who: Establish roles and responsibilities of those involved in fraud risk management activities, such as the antifraud entity.

What: Describe the program's activities for preventing, detecting, and responding to fraud, as well as for monitoring and evaluation.

When: Create timelines for implementing fraud risk management activities, as appropriate, including monitoring and evaluation.

Where: Demonstrate links to the highest internal and external residual fraud risks outlined in the fraud risk profile.

Why: Communicate the antifraud strategy to employees and other stakeholders, and link antifraud efforts to other risk management activities, if any.

Source: GAO, A Framework for Managing Fraud Risks in Federal Programs, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015). | GAO-24-105358

These areas in which the strategy is lacking direction align with certain key elements of an antifraud strategy as presented in the Fraud Risk Framework. See sidebar for additional information about key elements of an antifraud strategy.

³⁸Department of Defense, *Fraud Risk Management Strategy and Guidance Version 2.0*.

³⁹In this report, we are using the term "method" as an alternative to "control activity." The Fraud Risk Framework and *Standards for Internal Control in the Federal Government* use the term "control activity" to formally describe the policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks. [GAO-14-704G](#).

DOD's Fraud Risk Management Strategy Includes General References to Data Analytics

DOD's strategy says that it provides a roadmap for strengthening DOD's fraud risk management activities, including fraud controls and the mitigation of priority fraud risks. The strategy also says that effective fraud risk management practices must be implemented to detect, prevent, and respond to fraud risks across DOD. Specific to data analytics, the strategy states a broad data-analytics goal for fraud risk management. It states that one of DOD's goals is to use data analytics to identify, prevent, and respond to fraud.

The strategy describes Enterprise Financial Transformation (EFT) and the task force as having lead roles and responsibilities in data analytics. EFT is housed in the Comptroller's office and is to lead DOD data-analytics efforts. According to Comptroller officials, EFT replaced the former Chief Financial Officer Data Transformation Office, whose previous role, according to the 2020 strategy, was to lead the Chief Financial Officer's data-analytics efforts for DOD and support streamlining data-analytics efforts DOD-wide.⁴⁰ EFT's responsibility is to provide the analytics infrastructure to enable the Comptroller, ODA&M, and Principal Staff Assistants to collect inputs and requirements to support the Fraud Risk Management dashboards in Advana. The strategy provides information on two dashboards, the Fraud Risk Profile Dashboard and the Fraud Controls Dashboard, which Comptroller officials told us are operational.⁴¹ The information that populates these dashboards is submitted by the

⁴⁰The Chief Financial Officer Data Transformation Office was an entity within the Comptroller's office. According to Comptroller officials, its role was to assist the Deputy Chief Financial Officer in using Advana to conduct analytics pilots to identify fraud trends and red flags across DOD and collect input and feedback related to current activities across the Office of the Chief Management Officer and Comptroller to support the establishment of a data analytics fraud framework in Advana. According to Comptroller officials, the Chief Financial Officer Data Transformation Office is now part of the newly created EFT.

⁴¹Comptroller officials told us in May 2023 that the dashboards were operational.

components through the annual Statement of Assurance Program.⁴² The Fraud Risk Profile Dashboard provides an overview of the fraud risks that components submit.⁴³ The Fraud Controls Dashboard displays components' submission of Fraud Risk Management Framework Assessment inputs, which assess the number of controls in place and whether those controls are operating effectively.⁴⁴

Department of Defense (DOD) Priority Fraud Risk Areas

In the DOD Fiscal Year 2020 Fraud Risk Management Strategy, six fraud risk categories were selected as high priority for DOD. Procurement was listed as one of these priority areas, in addition to purchase cards, payroll, travel cards, asset safeguards, and information technology.

According to the fraud risk management strategy, these categories were selected based on the likelihood of fraud risk, reported fraud schemes in the areas by DOD Office of Inspector General or GAO, and availability of data.

For 2022, the highest-priority fraud risk categories included procurement, payroll, and asset safeguards.

Sources: Department of Defense Fiscal Year 2020 Fraud Risk Management Strategy (July 2020); and Department of Defense Fraud Risk Management Strategy and Guidance (August 2023). | GAO-24-105358

The task force leads DOD's analytics activities for high-priority fraud risks and is led by the Comptroller's Financial Improvement and Audit Remediation (FIAR) office.⁴⁵ It is comprised of subject matter experts from

⁴²Executive agencies, including DOD, are required to provide an annual Statement of Assurance that represents the agency head's informed judgment as to the overall adequacy and effectiveness of the agency's internal control. As part of this process, components must annually identify fraud risks related to various focus areas, including procurement, and must also identify controls currently in place to prevent and detect fraud. As previously reported, the Comptroller uses input collected from components about these fraud risks and controls to update DOD's fraud risk profile, to create a comprehensive list of controls that are currently in place across the department and to identify best practices to share within DOD. In addition, the Comptroller has used the dashboards during Fraud Risk Management office hours, which is a regular forum for providing fraud risk management updates and training within DOD. [GAO-21-309](#).

⁴³The submitted fraud risks are aggregated, with risks defined as "too broad," or not related to fraud, removed. The dashboard also shows which risks have controls in place and assigns an impact level to each identified fraud risk.

⁴⁴According to the strategy, submissions are due annually in July and aggregated by the Comptroller beginning in August.

⁴⁵Among other responsibilities, the FIAR office is to manage and oversee operations of DOD's Managers' Internal Control Program and provide guidance on the preparation and submission of the annual Statement of Assurance to the Secretary of Defense. Department of Defense, *Managers' Internal Control Program Procedures*, DOD Instruction 5010.40.

the Comptroller's FIAR office, ODA&M, and DOD components.⁴⁶ Among other responsibilities, the strategy lists several data-analytics responsibilities assigned to the task force, including

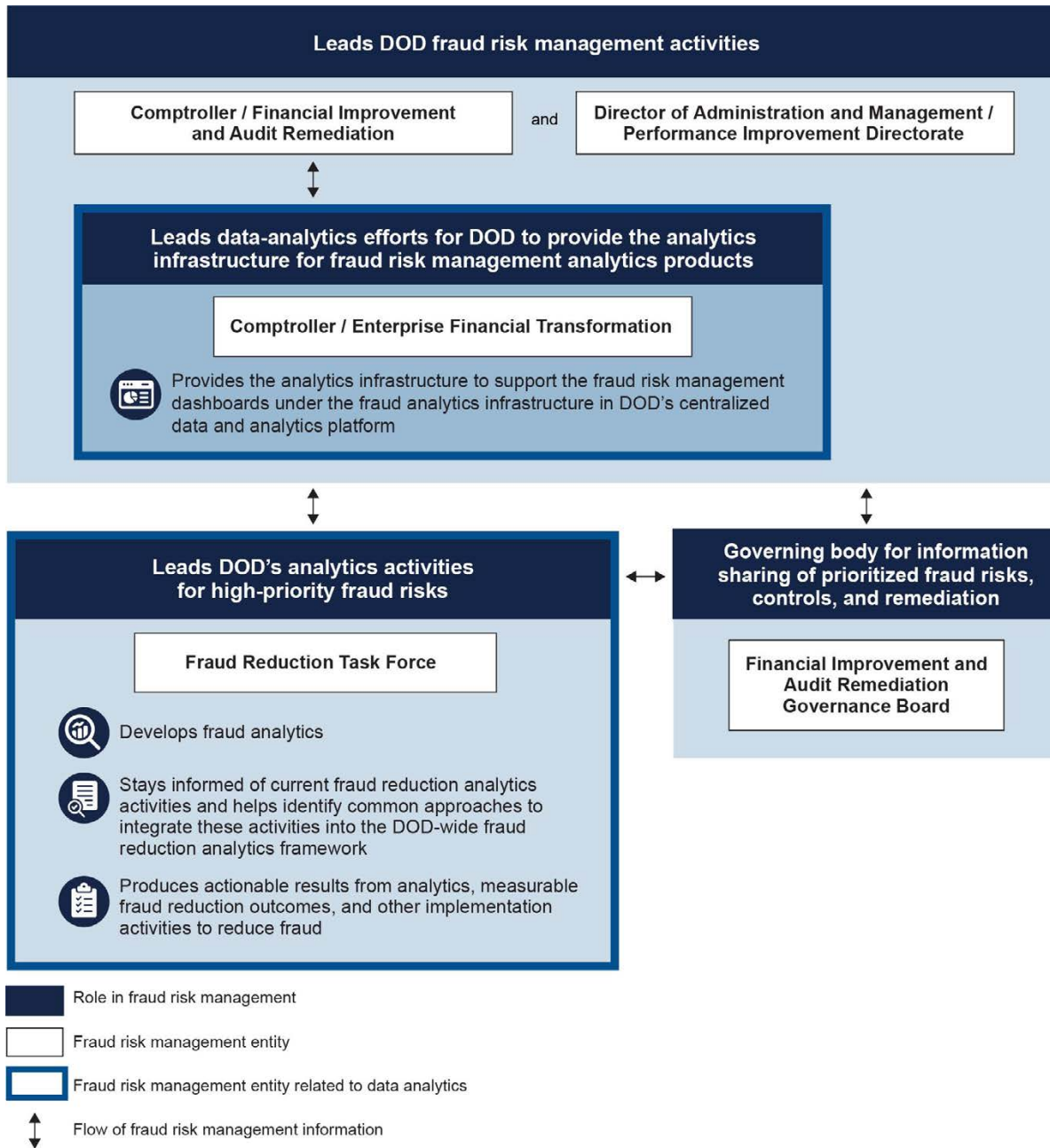
- staying informed of current fraud reduction-analytics activities and helping to identify common approaches to integrate these activities into a DOD-wide fraud reduction analytics framework; and
- producing actionable results from analytics, measurable fraud reduction outcomes, and other implementation activities to reduce fraud. See sidebar for more detail on the priority areas that DOD identified.

The strategy also states that components, who are members of the task force, are to develop fraud analytics based on high-risk areas identified through the Fraud Risk Assessment.⁴⁷ Figure 3 shows the key roles and responsibilities for fraud risk data analytics as described in the strategy.

⁴⁶In August 2021, we reported that the task force's membership was incomplete and recommended that DOD take action to ensure that cognizant components designate representatives to the task force as expeditiously as possible. As of February 2021, 11 of 59 components had not designated a representative to the task force. DOD concurred with this recommendation. DOD provided us with an updated roster in November 2023 indicating that all DOD components that are required to have a task force representative now do so. This recommendation is closed. [GAO-21-309](#).

⁴⁷The Fraud Risk Assessment is an annual survey in which components identify all fraud risks within their respective programs.

Figure 3: Key Department of Defense (DOD) Entities with Fraud Risk Management Data Analytics Roles and Responsibilities



Sources: GAO analysis of Department of Defense Fraud Risk Management Strategy and Guidance (August 2023); Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

Letter

Accessible Text for Figure 3: Key Department of Defense (DOD) Entities with Fraud Risk Management Data Analytics Roles and Responsibilities

Role in fraud risk management: Leads DOD fraud risk management activities

- Fraud risk management entity: Director of Administration and Management / Performance Improvement Directorate
- Fraud risk management entity: Comptroller / Financial Improvement and Audit Remediation
 - Role in fraud risk management: Leads data-analytics efforts for DoD to provide the analytics infrastructure for fraud risk management analytics products
 - Fraud risk management entity: Comptroller / Enterprise Financial Transformation (Fraud risk management entity related to data analytics)
 - Provides the analytics infrastructure to support the fraud risk management dashboards under the fraud analytics infrastructure in DOD's centralized data and analytics platform

Role in fraud risk management: Leads DOD's analytics activities for high-priority fraud risks

- Fraud risk management entity: Fraud Reduction Task Force (Fraud risk management entity related to data analytics)
 - Develops fraud analytics
 - Stays informed of current fraud reduction analytics activities and helps identify common approaches to integrate these activities into the DOD-wide fraud reduction analytics framework
 - Produces actionable results from analytics, measurable fraud reduction outcomes, and other implementation activities to reduce fraud

Role in fraud risk management: Governing body for information sharing of prioritized fraud risks, controls, and remediation

- Fraud risk management entity: Financial Improvement and Audit Remediation Governance Board

Role in fraud risk management

Fraud risk management entity

Fraud risk management entity related to data analytics

Flow of fraud risk management information

In addition to describing the data-analytics responsibilities of the EFT and the task force, the strategy briefly references other data-analytics activities. One of these activities is to pilot analytics models to identify potential fraud in priority fraud risk areas. However, the strategy does not state whose responsibility this is or provide additional direction regarding this activity. The strategy also briefly references other activities, such as the responsibility for entities, including the Comptroller, ODA&M, and the task force, to identify existing analytics to leverage in DOD's efforts to incorporate a risk-based analytics approach. An appendix of the strategy includes a table of examples of fraud control activities and briefly references data-analytics activities.

DOD's Strategy Does Not Establish Data Analytics as a Method for Fraud Risk Management and Does Not Provide Direction on Authorities, Roles, Responsibilities, and Timelines

Strategy Does Not Establish Data Analytics as a Method for Preventing, Detecting, and Responding to Fraud

While DOD's strategy generally references data-analytics activities, it does not discuss with specificity the method for using data-analytics activities in preventing, detecting, and responding to fraud. DOD's strategy does not discuss what or how data analytics are to be used. For example, the strategy does not discuss with specificity the following leading practices that impact what data analytics are used and how they are used to prevent, detect, and respond to fraud:

1. designing and implementing system edit checks, data matching, and data mining, which are data-analytics techniques that are broadly applicable to agencies;
2. combining data across programs to facilitate analytics; and

3. pursuing access to necessary external data.⁴⁸

As a leading practice under the Fraud Risk Framework's third component—*design and implement*—data-analytics activities are an important part of an effective antifraud strategy. As such, they should be integrated into the strategy as one of four different control activities—or methods—for managing fraud risk.⁴⁹ This is aligned with the *what* element of an antifraud strategy. Managers who effectively address fraud risks develop and document a strategy that describes the program's approach for addressing prioritized fraud risks, including designing and implementing specific control activities for preventing, detecting, and responding to fraud, such as data analytics.⁵⁰ Relatedly, federal internal control standards call for management to process data into quality information to support its internal control system and evaluate an entity's performance in meeting key objectives and addressing risks. Data-analytics activities are important in assessing, prioritizing, and managing fraud risks in a strategic manner. For example, data matching, a data-analytics technique, can be used to prevent and detect instances of fraud by helping to identify inconsistencies and verify key information. Establishing data analytics, consistent with leading practice, as a method for preventing, detecting, and responding to fraud, could help DOD inform related decision-making and mitigate assessed fraud risks.

Strategy Does Not Identify Which Entity Has Authority to Ensure That Fraud-Related Data-Analytics Activities Are Planned and Implemented

The Comptroller's FIAR office and ODA&M Performance Improvement Directorate jointly lead fraud risk management activities for DOD. The strategy, however, does not identify which, if either, entity has the necessary authority to ensure that the strategy's fraud-related data-

⁴⁸During a discussion with DOD officials regarding data sources for conducting data analytics, officials noted that entities owning relevant data needed to conduct procurement fraud data analytics were often outside the government. For example, officials noted that in instances of bribery or the provision of invalid information to the government, the relevant data would not appear in the documentation to which DOD has access but may reside in contractors' email or bank records. As we discuss in more detail below, although all such data related to procurement fraud are not always complete or readily available, our analyses demonstrate the usefulness and feasibility of using available data, such as investigative data from DCIOs, to conduct data analytics.

⁴⁹The other three control activities are fraud-awareness initiatives, reporting mechanisms, and employee integrity activities. [GAO-15-593SP](#).

⁵⁰[GAO-15-593SP](#).

analytics activities are planned and implemented. For example, the strategy does not identify either as having the authority to ensure that analytics pilots are conducted, or fraud analytics are developed. The strategy delineates some differences in responsibility, but not authority, between these two entities. For example, the strategy sets out certain independent responsibilities of the Comptroller or ODA&M, including that

- the Comptroller maintains the fraud risk management strategy and department-wide fraud risk profile and leads the task force, and
- ODA&M identifies the highest-priority fraud risks as they relate to DOD's strategic goals and performance objectives.

The strategy also sets forth joint responsibilities between the Comptroller and ODA&M, including collaborating to design and implement strategies with specific control activities to mitigate major fraud risks and ensure effective implementation. Additionally, the strategy states that components are responsible for implementing Comptroller and ODA&M guidance with respect to fraud risk management activities.

While it is beneficial to identify these responsibilities, the strategy does not clarify which entity has the authority across DOD to ensure that fraud-related data-analytics activities, such as conducting analytics pilots and developing fraud analytics, are carried out. Comptroller officials explained to us that to balance fraud risk management responsibilities with ODA&M, Comptroller and ODA&M leadership hold biweekly leadership meetings, in addition to using other communication streams, such as a shared email mailbox and office hours and subcommittees that meet regularly.

In affirming to us that the Comptroller and ODA&M Performance Improvement Officer are co-dedicated entities for the purpose of leading DOD fraud risk management activities, Comptroller officials noted their joint authority to provide internal control guidance related to the annual Statement of Assurance.⁵¹ This joint authority to provide guidance related to the annual Statement of Assurance is stated in the strategy. However, having authority to provide guidance related to an enterprise risk

⁵¹According to the Fraud Risk Framework, the dedicated entity leads fraud risk management activities and can be an individual or a team, depending on the needs of the agency. In addition to other attributes, a leading practice is for the dedicated entity to have defined responsibilities and the necessary authority across the program. [GAO-15-593SP](#). According to Comptroller officials, the forthcoming newly revised *Managers' Internal Control Program Procedures* (DOD Instruction 5010.40) will delegate authority to the Comptroller and the ODA&M Performance Improvement Officer to provide internal control guidance related to the annual Statement of Assurance.

management effort, such as the Statement of Assurance, does not necessarily mean that these entities also have the authority across the program with regard to fraud risk management activities. The annual Statement of Assurance is required, pursuant to OMB guidance on enterprise risk management, and represents the agency head's informed judgment as to the overall adequacy and effectiveness of the agency's internal control.⁵² Moreover, a Comptroller official told us in March 2022 that although the Comptroller is a lead fraud risk management entity, it does not have authority to direct components in their fraud risk management activities.

As we previously reported, DOD uses its risk management program, of which the Statement of Assurance is a part, to assess and report fraud risks.⁵³ The Fraud Risk Framework acknowledges that fraud risk management activities may be incorporated into an agency's existing enterprise risk management efforts, but this does not eliminate the separate and independent fraud risk management requirements. Likewise, a statement in the strategy regarding the authorities associated with the annual Statement of Assurance does not eliminate the need to identify the authorities associated with implementing the fraud risk management strategy. Identifying in the strategy which entity has the authority to ensure that the fraud-related data-analytics activities are planned and implemented is aligned with the *who* element of an antifraud strategy and will make DOD's strategy more effective.

Strategy Does Not Establish Clear Roles and Responsibilities for All Entities with Data-Analytics Roles

According to DOD officials, due in part to organizational changes, fraud risk management roles and responsibilities related to data analytics have changed since DOD issued its 2020 strategy. The August 2023 strategy removes a previous responsibility of the task force to conduct analytics to understand the scope of fraud risks, including the likelihood and potential impact of such risks. The strategy does not specify which, if any, entity will assume the particular responsibility of conducting analytics to understand the scope of fraud risks. We asked Comptroller officials to explain why the August 2023 strategy no longer includes conducting

⁵²OMB required an annual Statement of Assurance starting in fiscal year 2006. See Office of Management and Budget, *Management's Responsibility for Internal Control*, Circular No. A-123 (Washington, D.C.: Dec. 21, 2004).

⁵³[GAO-21-309](#).

analytics to understand the scope of fraud risks as one of the task force's responsibilities and also asked whether a different DOD entity would be conducting such analytics.

In response, Comptroller officials said that components have been advised to develop analytics to assist with fraud detection and take corrective action to remediate. However, the strategy does not specify whether developing analytics entails conducting analytics as well, or whether, for example, these are separate activities where developing analytics is an activity that precedes conducting analytics. The strategy also does not identify, and Comptroller officials did not clarify, who is responsible for conducting data analytics and whether the task force has a role in that.

According to Comptroller officials, EFT replaced the former Chief Financial Officer Data Transformation Office. However, the strategy does not specify that EFT's responsibilities include conducting analytics pilots to identify fraud trends and red flags across DOD programs, which the original strategy listed as one of the Chief Financial Officer Data Transformation Office's responsibilities. The strategy also does not specify which, if any, entity will assume responsibility for conducting analytics pilots. We asked Comptroller officials to explain why the August 2023 strategy does not include conducting analytics pilots to identify fraud trends as one of EFT's responsibilities and whether a different DOD entity will be conducting such analytics pilots. In an August 2023 response, Comptroller officials did not identify which entity, if any, will assume the responsibility for conducting analytics pilots and said that they may include discussions regarding the prioritization of fraud analytics as part of DOD's efforts to finalize its consolidated audit remediation strategy and the Secretary of Defense's audit priorities for fiscal year 2024. In December 2023, officials provided the Secretary of Defense's memorandum on fiscal year 2024 financial statement audit priorities, which does not specifically discuss fraud-related data analytics. However, according to a November 2023 response from Comptroller officials, the Comptroller is focusing the use of Advana on aspects that support the financial statement audit and is leveraging those efforts to enhance fraud-related data analytics.

In multiple interviews with us, DOD officials also described the Procurement Fraud Working Group as having a role in fraud risk management, including a collaborative role in data analytics. However, the working group is not mentioned in the strategy. Cognizant DOD officials noted that the working group has a collaborative role in data-

analytics work, though it does not, according to Comptroller officials, conduct data analytics. Established in January 2005, the working group is an informal DOD-wide group that meets several times a year and provides a forum for information exchange, policy development, and continuing education regarding current issues, future trends, and appropriate remedies in the procurement fraud area.⁵⁴

The working group also seeks to enhance interagency coordination, communication, and cooperation with the Department of Justice, the National Aeronautics and Space Administration, and other government agencies combating procurement fraud. With regard to fraud risk management data analytics, Comptroller and Defense Contract Management Agency officials stated that the working group has a role in sharing information and best practices and helped to develop red-flag indicators of fraud.⁵⁵

This is consistent with what we found in August 2021. Specifically, that DOD officials described entities as having roles and responsibilities for fraud risk management who were not named in DOD's July 2020 fraud risk management strategy. In that report, we recommended that the Comptroller determine and document the fraud risk management roles and responsibilities of all oversight officials and the chain of accountability for implementing its fraud risk management approach.⁵⁶

Standards for Internal Control in the Federal Government require management to establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives and 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

⁵⁴According to Comptroller officials, the working group has no additional objectives other than to serve as an informal forum for coordination, information exchange, policy development, continuing education, and interagency cooperation with government agencies combating procurement fraud.

⁵⁵The Defense Contract Management Agency provides contract administration services for DOD and other federal organizations.

⁵⁶DOD did not concur with this recommendation, saying that it would further discuss internally any potential updates to roles and responsibilities in the strategy. In reviewing the August 2023 strategy, we noted that entities, such as the Assessable Unit Subject Matter Experts, not listed in the July 2020 strategy, have been included in the August 2023 strategy. As of December 2023, this recommendation remains open. [GAO-21-309](#).

parties, such as external auditors.⁵⁷ Additionally, one of the key elements of an effective antifraud strategy is the *who*—establishing roles and responsibilities of those involved in the fraud risk management activities, such as the antifraud entity.

DOD has an expansive organizational structure—with 45 major components, including 19 defense agencies, 11 combatant commands, eight DOD field activities, and three military departments. Given this structure, revising the Fraud Risk Management Strategy to identify which entity has the necessary authority, and to clarify and document roles and responsibilities related to data-analytics activities, is critical to helping DOD manage its fraud risks.

Strategy Does Not Provide Timelines for Designing or Implementing Data-Analytics Activities

DOD's fraud risk management strategy states that data-analytics activities are to be conducted but does not provide timelines for designing or implementing such activities. For example, the strategy states that analytic models are to be piloted to identify potential fraud risks in priority areas and that fraud analytics are to be developed. However, the strategy does not provide timelines for designing and implementing the pilots or developing fraud analytics.

FIAR within the Comptroller's office is responsible for maintaining the fraud risk management strategy. We asked these officials about their plans outlining future data-analytics efforts, timelines, and priorities. In response, they said the strategy serves as the roadmap for DOD priorities. Aside from the strategy, Comptroller officials told us they were in the process of reaffirming components' abilities to explore data analytics at that level and were continuing to reexamine the best use of DOD time and resources. The officials did not identify any additional documents outlining the timelines for designing or implementing fraud-related data-analytics activities.

The Fraud Risk Framework notes the importance of designing and implementing data-analytics control activities and creating timelines for implementing them.⁵⁸ A leading practice of designing and implementing an antifraud strategy—the *when* element of an effective antifraud

⁵⁷[GAO-14-704G](#).

⁵⁸[GAO-15-593SP](#).

strategy—is to create timelines for implementing fraud risk management activities. Creating timelines for designing and implementing data-analytics activities that are documented in the antifraud strategy will help DOD ensure that such control activities can be used in a timely manner to help prevent, detect, and respond to fraud risks.

Comptroller officials told us that rather than delay the publication of the fiscal year 2023 strategy, they determined it would be best to address fraud analytics as part of a later, larger assessment of analytics. According to Comptroller officials, the Comptroller will be assessing the prioritization, capabilities, and resourcing of additional analytics, which may utilize tools such as Advana. They noted that fraud analytics may be included in discussions as part of DOD’s efforts to finalize its consolidated audit remediation strategy and the Secretary of Defense’s audit priorities for fiscal year 2024.

Having an antifraud strategy in place is important. Data analytics are a core aspect of designing and implementing an effective strategy. Additionally, one of DOD’s goals, as noted in the strategy, is to use data analytics to identify, prevent, and respond to fraud. While DOD has plans to examine fraud-related analytics as part of a larger effort, doing so is not a substitute for ensuring that its current antifraud strategy incorporates key elements identified in the Fraud Risk Framework. Having a strategy that establishes data analytics as a method for fraud risk management and provides direction on authorities, roles, responsibilities, and timelines for designing and implementing data-analytics activities is critical to helping DOD achieve its data-analytics goals and manage its fraud risks.

Our Analyses Demonstrate the Usefulness and Feasibility of Using DOD Investigative Data to Inform Fraud Risk Management, Despite Limitations

Our analyses demonstrate how DCIO investigative data can help inform DOD’s management of procurement fraud risk, although we identified some limitations with the data.⁵⁹ DCIOs collect data in their case

⁵⁹Throughout this objective, “data” refers to specific data elements, while “information” refers more broadly to what could be gleaned from the data and used for fraud risk management purposes.

management systems that describe, to varying levels, the extent of detected alleged fraud through the number and types of cases investigated.⁶⁰ We found that the data also provide insight, to varying levels, on characteristics of alleged and adjudicated fraud schemes and trends from DOD's associated monitoring and detection activities, such as through the number and types of suspects involved, offenses investigated and adjudicated, and other case outcomes.⁶¹ Further, the data on case outcomes provide some insight into financial impacts of adjudicated fraud.

However, we found that the data were not always complete and could not always be readily analyzed, which creates limitations for fraud-related data-analytics activities.⁶² For example, some fields in the DCIO case management systems are required for all cases. Other fields are completed based on the facts and circumstances of a case, which can result in incomplete data. We also found that MCIOs captured some data in narrative fields, which made analysis difficult.

DOD does not have plans to obtain and analyze information from the DCIOs regarding investigations of alleged and adjudicated procurement fraud to inform its fraud risk management activities. Comptroller officials told us they are in the process of identifying appropriate data sources to develop data analytics for procurement fraud. While DOD's strategy identifies DCIS as an information source, it does not outline the use of information from case management data. As discussed in more detail below, according to DOD OIG, although the draft strategy was informally reviewed within the DOD OIG, the Comptroller/Chief Financial Officer did not formally coordinate the strategy with the DOD OIG in accordance with established DOD coordination processes.

⁶⁰In this objective, we refer to cases as involving "alleged" fraud because they did not all result in adjudicated fraud. However, we found that some of the cases did result in adjudicated fraud.

⁶¹In technical comments on this report, one of the DCIOs noted that it does not routinely engage in monitoring or detection activities as related to procurement fraud. As discussed here, monitoring and detection activities are applicable to DOD as it performs fraud risk management activities.

⁶²In this objective, we refer to data with blank or unknown values as "incomplete." However, this does not mean that these or other fields were not completed as required by case management system policies. In some instances, fields with blank or unknown data were not required. In others, fields were required, but unknown values were an acceptable entry based on available information and the circumstances of the case.

In addition to analyzing the DCIO data, we reviewed eight procurement fraud cases that were closed by DCIOs between fiscal years 2015 and 2021. See appendix II for summaries of each of these cases, including summaries of the general fraud scheme(s) employed, offenses investigated or adjudicated, and case outcomes.

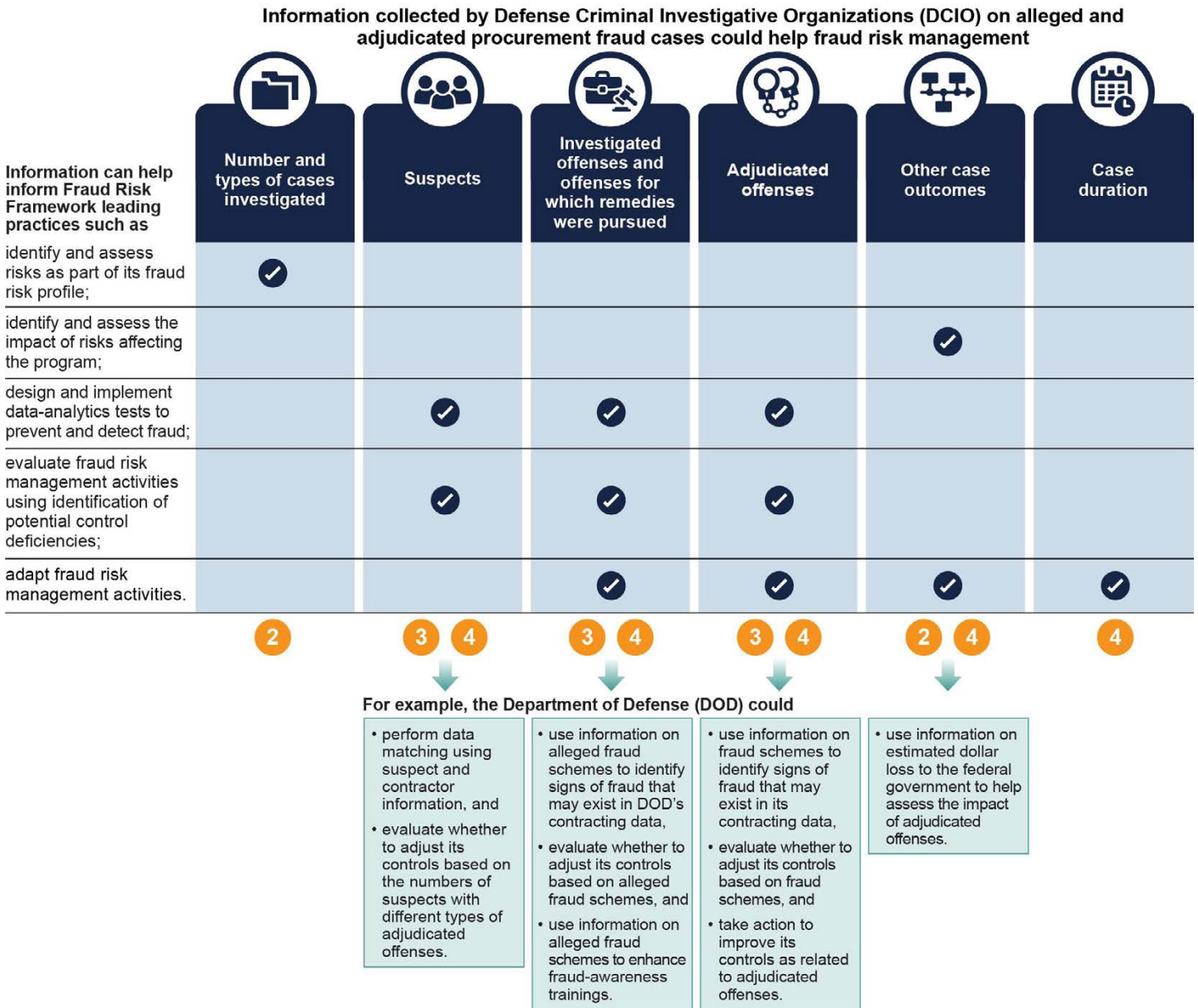
DOD Investigative Data Provide Insight into Characteristics of Fraud Schemes and Results of DOD Monitoring Activities

DCIOs' investigative data on procurement fraud can help inform DOD's management of procurement fraud risk based on leading practices outlined in the Fraud Risk Framework.⁶³ Specifically, we found through our analyses that the information from the data collected by DCIOs on alleged and adjudicated procurement fraud cases could help DOD identify and assess existing fraud risks and their impact and take corresponding actions to design, implement, evaluate, and adapt fraud risk management activities.

Figure 4 provides examples of data collected by DCIOs and how we found it can inform leading practices from the Fraud Risk Framework.

⁶³The Fraud Risk Framework includes several leading practices that call on agencies to consider fraud schemes and related information to help combat fraud. For example, it calls on agencies to identify and assess risks affecting the program, as well as the impact of those risks; consider known or previously encountered fraud schemes to design data-analytic tests to prevent and detect fraud; use data from instances of detected fraud to identify potential control deficiencies; and use analysis of identified instances of fraud and fraud trends to improve fraud risk management activities. See [GAO-15-593SP](#).

Figure 4: Examples of Data Collected by the Department of Defense That Could Help Inform Fraud Risk Management



 Can help inform the associated example leading practice. Other leading practices may also be relevant.	Related component of GAO's Fraud Risk Framework 1 Commit 2 Assess 3 Design and implement 4 Evaluate and adapt
--	---

Sources: GAO analysis of DOD data; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

Accessible Text for Figure 4: Examples of Data Collected by the Department of Defense That Could Help Inform Fraud Risk Management

Information collected by Defense Criminal Investigative Organizations (DCIO) on alleged and adjudicated procurement fraud cases could help fraud risk management						
Information can help inform Fraud Risk Framework leading practices such as	Number and types of cases investigated	Suspects	Investigated offenses and offenses for which remedies were pursued	Adjudicated offenses	Other case outcomes	Case duration
identify and assess risks as part of its fraud risk profile;	Can help inform the associated example leading practice. Other leading practices may also be relevant.					
identify and assess the impact of risks affecting the program;					Can help inform the associated example leading practice. Other leading practices may also be relevant.	
design and implement data-analytics tests to prevent and detect fraud;		Can help inform the associated example leading practice. Other leading practices may also be relevant.	Can help inform the associated example leading practice. Other leading practices may also be relevant.	Can help inform the associated example leading practice. Other leading practices may also be relevant.		
evaluate fraud risk management activities using identification of potential control deficiencies;		Can help inform the associated example leading practice. Other leading practices may also be relevant.	Can help inform the associated example leading practice. Other leading practices may also be relevant.	Can help inform the associated example leading practice. Other leading practices may also be relevant.		
adapt fraud risk management activities.			Can help inform the associated example leading practice. Other leading practices may also be relevant.	Can help inform the associated example leading practice. Other leading practices may also be relevant.	Can help inform the associated example leading practice. Other leading practices may also be relevant.	Can help inform the associated example leading practice. Other leading practices may also be relevant.

Letter

Information collected by Defense Criminal Investigative Organizations (DCIO) on alleged and adjudicated procurement fraud cases could help fraud risk management

Information can help inform Fraud Risk Framework leading practices such as	Number and types of cases investigated	Suspects	Investigated offenses and offenses for which remedies were pursued	Adjudicated offenses	Other case outcomes	Case duration
Related component of GAO's Fraud Risk Framework	Assess	<ul style="list-style-type: none"> Design and implement Evaluate and adapt 	<ul style="list-style-type: none"> Design and implement Evaluate and adapt 	<ul style="list-style-type: none"> Design and implement Evaluate and adapt 	<ul style="list-style-type: none"> Assess Evaluate and adapt 	Evaluate and adapt
For example, the Department of Defense (DOD) could		<ul style="list-style-type: none"> perform data matching using suspect and contractor information, and evaluate whether to adjust its controls based on the numbers of suspects with different types of adjudicated offenses. 	<ul style="list-style-type: none"> use information on alleged fraud schemes to identify signs of fraud that may exist in DOD's contracting data, evaluate whether to adjust its controls based on alleged fraud schemes, and use information on alleged fraud schemes to enhance fraud-awareness trainings. 	<ul style="list-style-type: none"> use information on fraud schemes to identify signs of fraud that may exist in its contracting data, evaluate whether to adjust its controls based on fraud schemes, and take action to improve its controls as related to adjudicated offenses. 	use information on estimated dollar loss to the federal government to help assess the impact of adjudicated offenses.	

Sources: GAO analysis of DOD data; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

Note: More information about GAO's Fraud Risk Framework is available at GAO, A Framework for Managing Fraud Risks in Federal Programs, GAO-15-593SP (Washington, D.C.: July 28, 2015).

We analyzed investigative case management data for unclassified, unsealed cases closed from fiscal years 2015 through 2021, focusing on alleged and adjudicated procurement fraud cases.⁶⁴ (See text box for further insights into the case management data.) Specifically, we used the

⁶⁴Closed cases could involve "alleged," rather than "adjudicated," fraud if they did not lead to an adjudicative outcome—for example, if all charges were dismissed.

data to analyze the number and types of cases investigated; suspects; investigated offenses and offenses for which remedies were pursued; adjudicated offenses; other case outcomes, including financial and nonfinancial impacts; and case duration.

Data insights – structured and narrative fields

Investigators at the Military Criminal Investigative Organizations enter data into their respective case management systems using a combination of structured and narrative data fields. Investigators at the Defense Criminal Investigative Service (DCIS) enter data into their case management system using structured fields. The structured fields are intended for certain discrete pieces of data, such as suspect name or sentence type, and may restrict the types of characters that can be entered, or rely on drop-down menus to prescribe the types of data that can be recorded. The narrative fields are open-ended fields that allow investigators to describe the investigation more broadly, based on available information. The completeness of the structured and narrative fields vary based on a range of factors, including the specific Defense Criminal Investigative Organization's (DCIO) case management system and policies for data entry, such as policies specifying fields that are required. We focused our analysis on the DCIOs' structured fields.

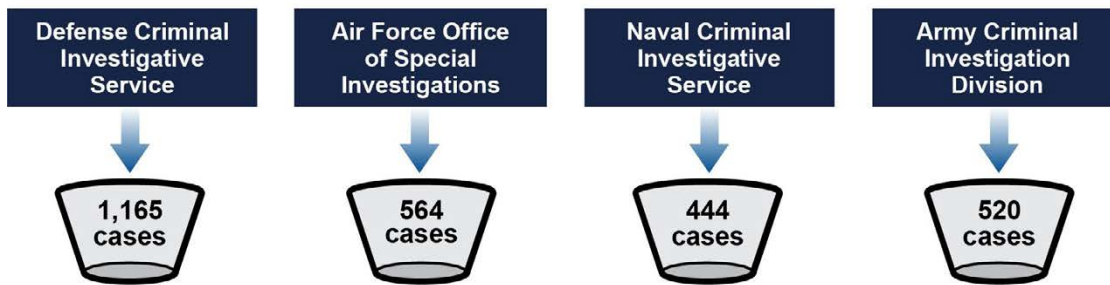
Source: GAO review of Department of Defense data and documentation. | GAO-24-105358

Number and type of cases investigated. DCIOs collect structured data that can be used to identify the total number and type of cases investigated by the DCIO, which can provide visibility into the extent of alleged procurement fraud detected. This information could help DOD identify and assess risks as part of its fraud risk profile. Specifically, information on the number and types of cases investigated could help DOD (1) identify procurement fraud risks and the likelihood and impact of those risks and (2) prioritize the fraud risks.

Using these data, for each DCIO, we identified the number of alleged and adjudicated procurement fraud cases closed from fiscal years 2015 through 2021. The number of closed cases ranged from about 444 cases

for NCIS to about 1,165 cases for DCIS.⁶⁵ See figure 5 and text box for further insights into identifying the number and type of cases.

Figure 5: Number of Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021, by Defense Criminal Investigative Organization



Source: GAO analysis of Department of Defense data. | GAO-24-105358

Accessible Data for Figure 5: Number of Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021, by Defense Criminal Investigative Organization

Defense Criminal Investigative Organization	Number of cases
Defense Criminal Investigative Service	1165
Air Force Office of Special Investigations	564
Naval Criminal Investigative Service	444
Army Criminal Investigation Division	520

Source: GAO analysis of Department of Defense data. | GAO-24-105358

⁶⁵The number of cases identified for each DCIO may overlap, as DCIOs sometimes conduct joint investigations. While the DCIOs' unique identifiers allow them to individually assess the number of cases in which they played a role, there is no shared identifier that would allow DOD to determine the total number of cases investigated across DCIOs without leveraging additional data sources. In addition, some DCIOs varied in the population of case data they provided, which may limit comparability in some instances. For example, USACID officials provided data for cases opened and closed from fiscal year 2015 through fiscal year 2021, rather than all cases closed during this time frame. In addition, NCIS provided us with data on all criminal cases that NCIS determined were relevant to alleged or adjudicated procurement fraud and that closed during this period. This included cases in which NCIS provided limited assistance or that never progressed from initial inquiries to full investigations. DCIS officials stated that they generally provided data on only full investigations DCIS led or jointly led but, due to data limitations, a few limited investigations or inquiries may exist in the data. We took steps to focus on full investigations led or jointly led by the DCIO, where possible. For example, we excluded NCIS investigations that were characterized as limited assistance or inquiries, based on our review of the data and discussions with NCIS officials. We also limited all our DCIO analyses to cases with at least one suspect.

Letter

Note: Defense Criminal Investigative Organizations (DCIO) provided data for unsealed, unclassified cases closed during this period. The Army Criminal Investigation Division provided data for cases opened and closed during this period. The Naval Criminal Investigative Service provided us with data on all criminal cases that NCIS determined were relevant to alleged or adjudicated procurement fraud and that closed during this period. We took steps, where possible, to exclude limited assistance investigations and inquiries, as our focus was on full investigations. The number of cases identified for each DCIO may overlap where DCIOs conducted joint investigations.

Data insights – identifying the number and type of cases

Each Defense Criminal Investigative Organization's (DCIO) case management system automatically generates a unique identification number for each case created. In addition, each case management system contains fields, automatically populated in some instances, specifying the dates that cases are opened and closed.

In contrast, the steps required to identify case type vary by DCIO. The Defense Criminal Investigative Service (DCIS) and Naval Criminal Investigative Service (NCIS) case management systems contain case category fields, completed by investigators at the onset of an investigation. The systems allow those DCIOs to readily identify alleged and adjudicated procurement fraud cases, as opposed to cases involving other types of fraud. According to DCIO officials, these categories are generally selected based on an investigator's judgment of the most pressing aspect of a case. It is possible for the focus of the case to change over time, but the investigator may not always change the category. It is also possible that cases involving alleged or adjudicated procurement fraud were not labeled as such in the case category field because investigators' focus was another type of fraud. We used the case category field to identify alleged and adjudicated procurement fraud cases for DCIS. NCIS officials used the case category field to provide us with data on alleged and adjudicated procurement fraud cases.

The Air Force Office of Special Investigations (AFOSI) and Army Criminal Investigative Division (USACID) case management systems do not contain structured fields that would allow for classification of cases as related to alleged or adjudicated procurement fraud. To identify relevant AFOSI and USACID cases, we analyzed the DCIOs' narrative fields using keyword searches and a natural language processing model that was used to classify text.

Source: GAO review of Department of Defense data and documentation. | GAO-24-105358

Number and type of suspects. Each DCIO collects identifiers in structured fields that can be used to help determine the number and type of suspects involved with alleged and adjudicated procurement fraud cases, information that is a key characteristic of fraud schemes. This information could help DOD design and implement data-analytic tests to prevent and detect fraud, such as by performing data matching using suspect and contractor data. It could also help DOD evaluate fraud risk management activities by identifying potential control deficiencies. For example, each of the DCIOs collects a suspect's name. While this field alone can be limited as a unique identifier, such as instances in which suspects share the same name, analyzing the number of suspect names involved with a case can provide insight into characteristics of alleged and adjudicated procurement fraud schemes and help DOD evaluate its existing controls. As another example, DOD could use information on the numbers of suspects with different types of adjudicated offenses to evaluate whether to adjust its controls.

Using the DCIOs' suspect identifiers, we found that the total number of known suspects in alleged and adjudicated procurement fraud cases closed from fiscal years 2015 through 2021 ranged from 831 in NCIS

cases to 3,509 in DCIS cases.⁶⁶ See text box for further insights into identifying suspects.

Data insights – identifying suspects

Some Defense Criminal Investigative Organizations collect additional suspect identifiers. For example, the Naval Criminal Investigative Service (NCIS) provided data on suspects' dates of birth. NCIS officials reported that NCIS also collects Social Security numbers but did not provide these data for our report. The Defense Criminal Investigative Service collects identifiers such as date of birth, Social Security number, and driver's license number, in some instances. Where available, these identifiers can be used alone or in addition to others to obtain a more precise count of suspects.

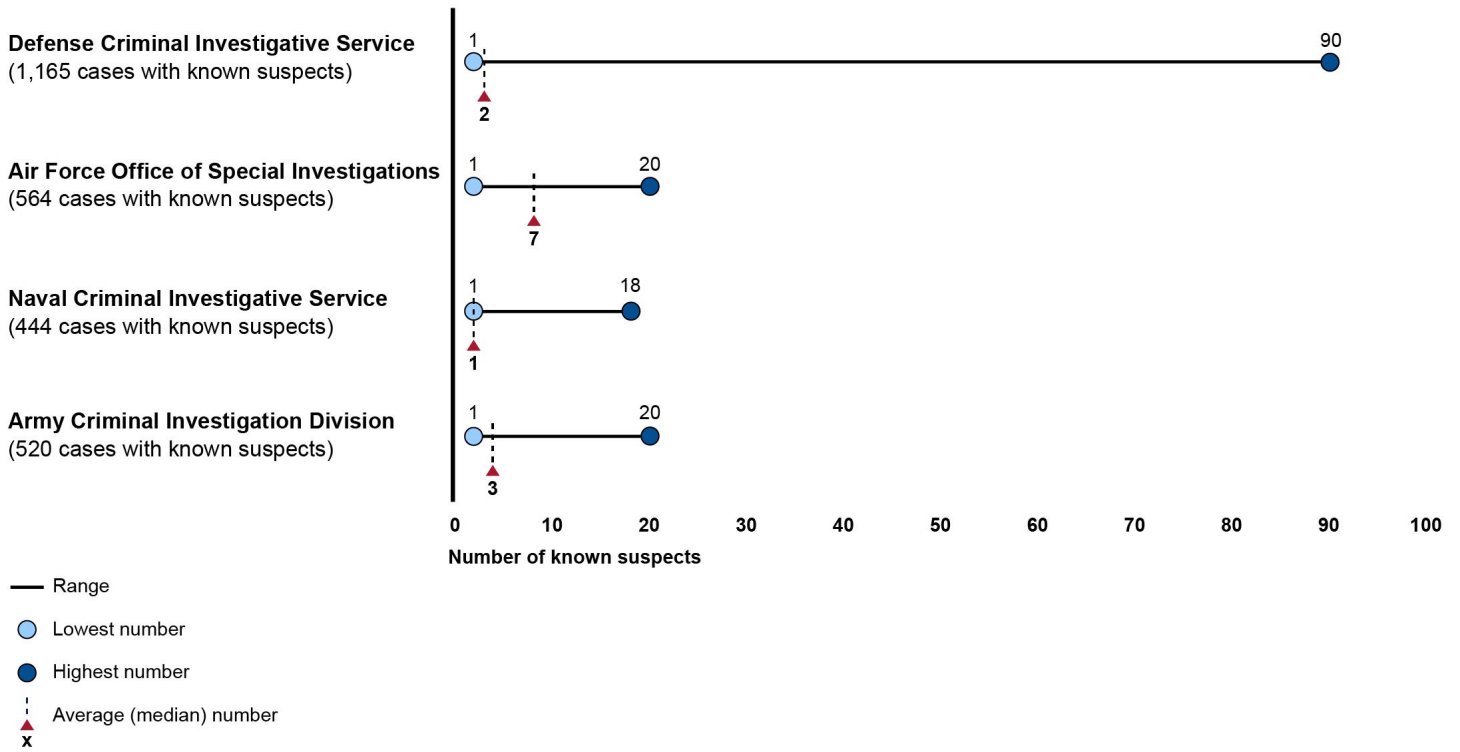
Source: GAO review of Department of Defense data and documentation. | GAO-24-105358

We also found that the maximum number of known suspects per case ranged from 10 suspects for USACID cases to 90 suspects for DCIS cases.⁶⁷ See figure 6.

⁶⁶Suspects may not always be identified throughout the course of an investigation. We excluded unknown suspects for the purposes of this analysis. Our analysis does not account for possible misspellings or other errors in data entry, which might inflate the count of unique suspect identifiers.

⁶⁷The number of known suspects per case may include separate divisions or locations within the same business, where they are labeled as separate suspects within the DCIO's case management data.

Figure 6: Range of Number of Known Suspects per Case in Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021



Source: GAO analysis of Department of Defense data. | GAO-24-105358

Accessible Data for Figure 6: Range of Number of Known Suspects per Case in Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021

Defense Criminal Investigative Organization	Number of known suspects (range)	Average (median)
Defense Criminal Investigative Service (1,165 cases with known suspects)	1-90	2
Air Force Office of Special Investigations (564 cases with known suspects)	1-20	7
Naval Criminal Investigative Service (444 cases with known suspects)	1-18	1
Army Criminal Investigation Division (520 cases with known suspects)	1-20	3

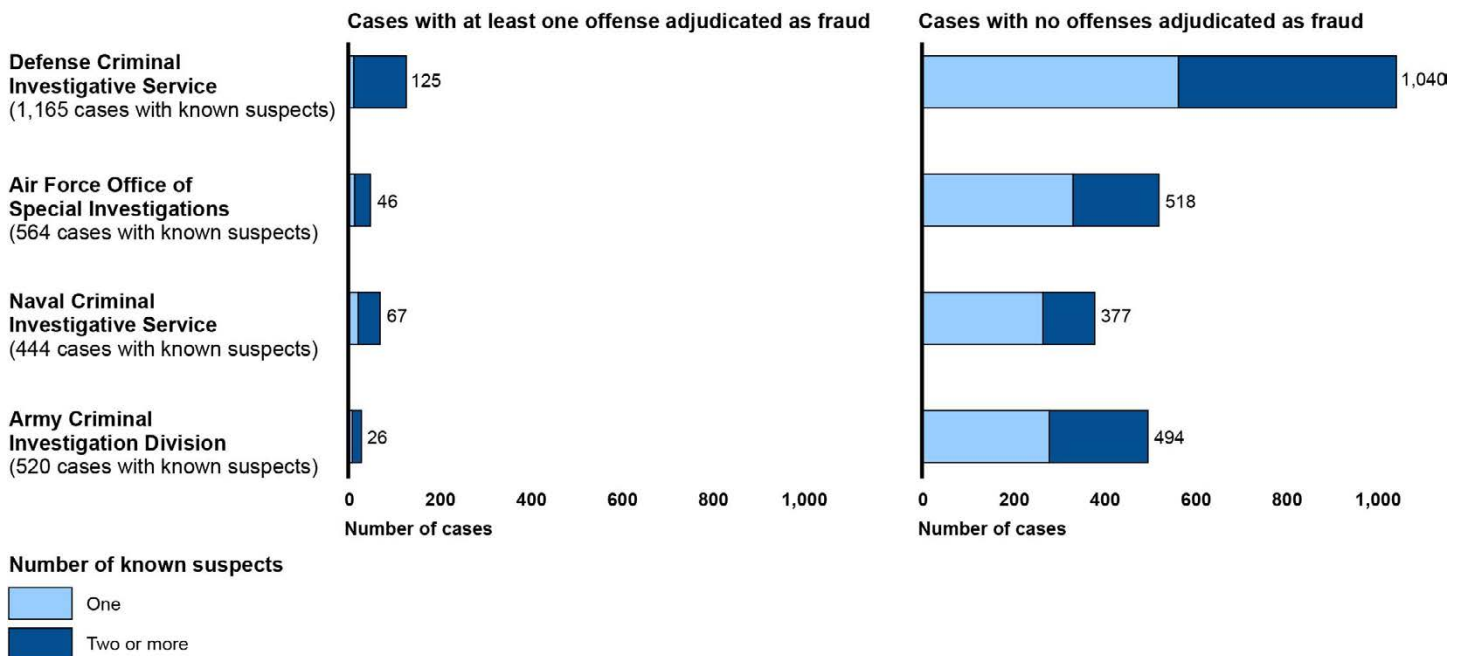
Source: GAO analysis of Department of Defense data. | GAO-24-105358

In general, a greater proportion of cases with multiple known suspects involved at least one offense adjudicated as fraud, as compared with the proportion of cases with one known suspect.⁶⁸ For example, about 30

⁶⁸Our data likely do not include all adjudicative information. Based on available data, cases with multiple known suspects might be more likely to involve adjudicated offenses.

percent of the 162 NCIS cases with multiple known suspects involved at least one adjudicated offense, as compared with about 7 percent of the 282 NCIS cases with one known suspect. See figure 7.

Figure 7: Number of Suspects by Adjudicated Offense Status for Department of Defense Investigations of Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021



Source: GAO analysis of Department of Defense data. | GAO-24-105358

Accessible Data for Figure 7: Number of Suspects by Adjudicated Offense Status for Department of Defense Investigations of Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021

Defense Criminal Investigative Organization	Number of cases with known suspects
Defense Criminal Investigative Service	1165
Air Force Office of Special Investigations	564
Naval Criminal Investigative Service	444
Army Criminal Investigation Division	520

Letter

Cases with at least one offense adjudicated as fraud

Defense Criminal Investigative Organization	Number of cases with one known suspect	Number of cases with two or more known suspects	Total number of cases with one or more known suspects
Defense Criminal Investigative Service	9	116	125
Air Force Office of Special Investigations	11	35	46
Naval Criminal Investigative Service	19	48	67
Army Criminal Investigation Division	6	20	26

Cases with no offenses adjudicated as fraud

Defense Criminal Investigative Organization	Number of cases with one known suspect	Number of cases with two or more known suspects	Total number of cases with one or more known suspects
Defense Criminal Investigative Service	561	479	1,040
Air Force Office of Special Investigations	329	189	518
Naval Criminal Investigative Service	263	114	377
Army Criminal Investigation Division	277	217	494

Source: GAO analysis of Department of Defense data. | GAO-24-105358

Note: We define adjudicated offenses as offenses that were ultimately adjudicated through a judicial or other adjudicative system as fraud. While these offenses were involved in cases that we determined were related to alleged procurement fraud, not all the offenses may have been related to procurement fraud. We reviewed the data and consulted with Defense Criminal Investigative Organization officials to determine the most appropriate structured fields to use to identify cases with adjudicated offenses. However, our analysis may not have captured all cases involving adjudicated offenses, or all adjudicated offenses involved with a case. In addition, cases can involve multiple suspects, and suspects can have multiple offenses. Therefore, the cases we identified as involving adjudicated offenses may also involve nonadjudicative outcomes, such as dismissals.

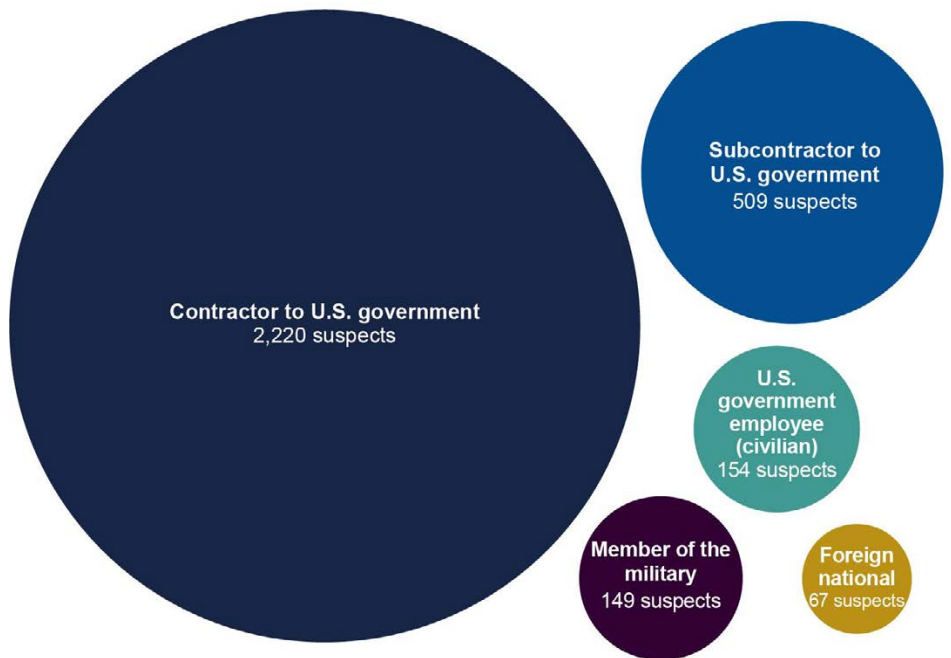
DCIOs may collect structured data on suspect type and relationship to the government.⁶⁹ Both of these data types can offer DOD greater insight into the types of fraud schemes and potential vulnerabilities it faces, thus helping direct its fraud risk management efforts. For example, DCIS data on suspect type shows that 1,889, or about 54 percent, of the 3,509 known suspects involved with the 1,165 DCIS cases we reviewed were businesses, while 1,598, or about 46 percent, were individuals.⁷⁰ DCIS data on relationship to the government shows that, for example, 2,220 known suspects, or about 63 percent, were contractors. Figure 8

⁶⁹For example, DCIS collects structured data on suspect type and relationship to the government, and NCIS collects structured data on relationship to the government.

⁷⁰The remaining suspects were labeled as government entities or the public.

illustrates the number of suspects by type of relationship to the government, of the 3,509 known suspects in the 1,165 DCIS cases we reviewed.

Figure 8: Suspects Involved in Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021 for the Defense Criminal Investigative Service



Source: GAO analysis of Department of Defense data. | GAO-24-105358

Accessible Text for Figure 8: Suspects Involved in Alleged and Adjudicated Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021 for the Defense Criminal Investigative Service

Category	Number of suspects
Contractor to U.S. government	2220
Subcontractor to U.S. government	509
U.S. government employee (civilian)	154
Member of the military	149
Foreign national	67

Source: GAO analysis of Department of Defense data. | GAO-24-105358

Note: This figure illustrates the number of known suspects by type of relationship to the government, of the 3,509 known suspects in the 1,165 Defense Criminal Investigative Service cases we reviewed. Suspects can have multiple relationships to the government. As a result, the numbers in the figure may overlap and are not additive. Other government relationships not included in this figure include local government employees and government agencies, among others.

Letter

Procurement Fraud Scheme Participants – Illustrative Case Studies



Participants in fraud schemes can include the fraudster; complicit, coerced, or unknowing facilitator; victim; external fraudster; internal fraudster; and combination (external and internal) fraudster.

The following describes selected participant information from two of the closed investigative case files we reviewed.

Victim and unknowing facilitator: In an Army Criminal Investigation Division case, the victims were tricked into believing they had a valid contract with the Department of Defense to deliver air conditioning units.

Fraudsters misrepresented themselves as contracting officers to accomplish this deception.

After delivering the air conditioning units, the victims submitted invoices requesting payment, referencing a nonexistent contract.

The victims were initially identified as subjects of the investigation before investigators determined they were actually victims.

The victims unknowingly facilitated the scheme by delivering the air conditioning units, after which the fraudsters requested and collected payment from the government under a legitimate contract.

External and internal fraudsters: In a Naval Criminal Investigative Service case, one fraudster was a Master Scheduler at a naval base and was responsible for approving material purchases, service contracts, vendors, and payments on invoices.

The fraudster used this position to direct U.S. Navy purchases to preferred vendors.

Another conspirator fraudster who was the President of a corporation that did procurement work for the U.S. Navy issued vendor invoices that inflated the quantity of items delivered and hours worked on service contracts, thereby inflating the associated costs purportedly owed by the U.S. Navy. The conspirator fraudster then paid kickbacks to the fraudster Master Scheduler.

Sources: GAO review of Department of Defense closed investigative case files and other case documentation; Icons-Studio/stock.adobe.com (icon). | GAO-24-105358

In addition to suspects, fraud schemes can involve other types of participants, such as victims. See sidebar for examples of participants in the investigative case studies we completed.

Number and types of investigated offenses and offenses for which remedies were pursued. Each DCIO collects some data in structured fields describing investigated offenses, as well as offenses for which remedies were pursued.⁷¹ Such data, even where incomplete, can provide officials with information on the types and possible emerging trends of procurement fraud risks faced by DOD. This information could help DOD design and implement data-analytic tests to prevent and detect fraud, evaluate fraud risk management activities by identifying potential control deficiencies, and adapt fraud risk management activities. For

⁷¹Data on investigated offenses can reflect all offenses—to the extent the data were entered—investigated throughout a case. Data on offenses for which remedies were pursued generally reflect a smaller set of offenses for which criminal charges, or other actions, such as suspension or debarment, were pursued based on findings of the investigation. Decisions regarding whether to pursue remedies in court are made by the Department of Justice. Decisions regarding whether to pursue contractual or administrative remedies are made by the centralized organizations.

example, DOD could use information on alleged fraud schemes to help design data-analytic tests to identify signs of fraud that may exist in DOD's contracting data. DOD could also use information on alleged fraud schemes to evaluate whether to adjust its controls, or to adapt fraud risk management activities, such as by enhancing fraud-awareness trainings.

We used available data to identify, for each DCIO, the number of cases and known suspects with known investigated offenses and offenses for which remedies were pursued.⁷² For example, according to available data, each of the 1,103 known suspects in the 564 AFOSI cases we identified had at least one listed investigated offense. Of these known suspects, 110, or about 10 percent of known suspects—corresponding to 54, or about 10 percent of cases—had data showing they had offenses for which remedies were pursued.

⁷²The DCIS data did not contain specific investigated offenses for most cases. We, therefore, used case category data to supplement our analysis where a case did not have a listed investigated offense. According to DCIS officials, case category provides a broader depiction of the type of fraud investigated and could include multiple types of offenses.

Offenses Investigated – Illustrative Case Study



Procurement fraud schemes may involve multiple offenses. In some cases, remedies may not be pursued for all investigated offenses. In the example from a closed case below, remedies were pursued for all of the listed investigated offenses.

The basic scheme in this Naval Criminal Investigative Service case involved a Master Scheduler at a naval base who supervised purchasing agents who placed orders for supplies and services and paid vendor invoices. The Master Scheduler used this position to direct purchases to preferred vendors.

In addition to being charged with conspiracy, the fraudster was charged with

conflicts of interest – for participating, as a government officer and employee, in an application, contract, and claim in which the fraudster, and organizations in which the fraudster was serving as an officer, director, or employee, had a financial interest;

false, fictitious, and fraudulent claims against the United States – for making and presenting to the U.S. Navy an invoice for labor and materials in connection with the replacement of a shower valve cartridge, knowing such claim to be false, fictitious, and fraudulent;

acceptance of bribes – for accepting money as the master scheduler, in exchange for directing and approving government purchase orders and payments to certain companies; and

false statement – for making a false, fictitious, and fraudulent statement on a U.S. Office of Government Ethics Form, in which the fraudster represented that the fraudster had no position outside the U.S. government in any business entity, knowing that the fraudster was the Chief Executive Officer of a company and owned 85 percent of another company.

Sources: GAO review of Department of Defense closed investigative case files and other case documentation; Icons-Studio/stock.adobe.com (icon). | GAO-24-105358

Where available, data from the DCIOs suggest that alleged and adjudicated procurement fraud cases involved a range of the types of investigated offenses and offenses for which remedies were pursued. For example, the most prevalent offenses investigated in the 444 NCIS cases we identified were

- false, fictitious, or fraudulent claims (138 cases);
- false statements (103 cases); and
- civil false claims (72 cases).⁷³

These were also the most prevalent offenses for which remedies were pursued in the NCIS cases we identified.

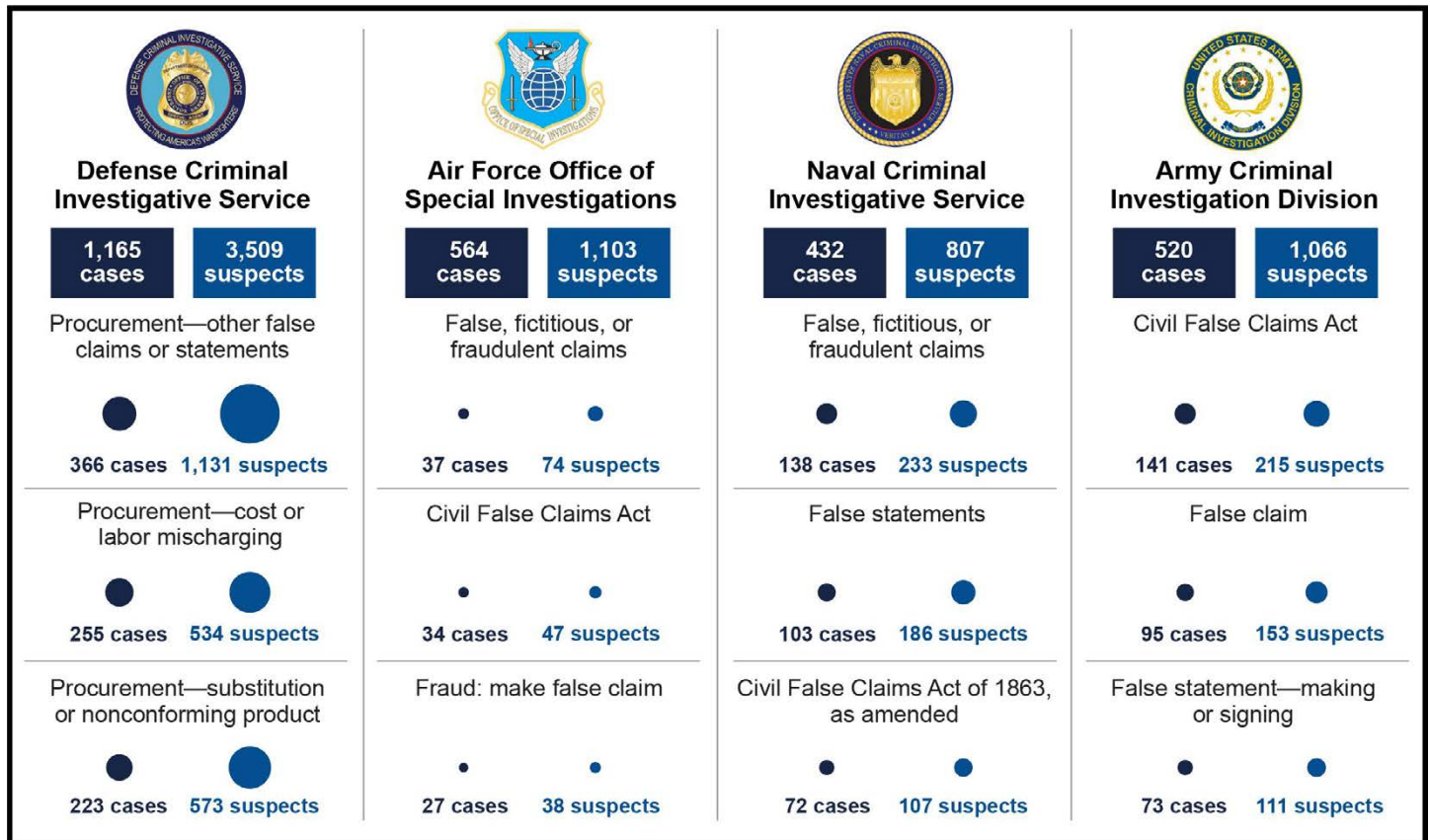
See figures 9 and 10 for the numbers of cases with investigated offenses and offenses for which remedies were pursued. These figures also show

⁷³The most prevalent investigated offense citations were, respectively, 18 U.S.C. § 287, 18 U.S.C. § 1001, and 31 U.S.C. § 3729. We used case count to determine prevalence for the purposes of our analysis.

the most prevalent types of offenses in each DCIO's case management data.

See sidebar for examples of investigated offenses in the investigative case studies we completed.

Figure 9: Most Prevalent Offenses Investigated for Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021



Number of cases with at least one investigated offense
 Number of known suspects with at least one investigated offense

Number of cases by most prevalent investigated offense
 Number of known suspects by most prevalent investigated offense

Sources: GAO analysis of Department of Defense (DOD) data; DOD (agency seals). | GAO-24-105358

Letter

Accessible Data for Figure 9: Most Prevalent Offenses Investigated for Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021

Defense Criminal Investigative Service

- 1,165 cases (Number of cases with at least one investigative offense)
- 3,509 suspects (Number of known suspects with at least one investigated offense)
- Procurement—other false claims or statements
 - 366 cases (Number of cases by most prevalent investigated offense)
 - 1131 suspects (Number of known suspects by most prevalent investigate offense)
- Procurement—cost or labor mischarging
 - 255 cases (Number of cases by most prevalent investigated offense)
 - 534 suspects (Number of known suspects by most prevalent investigate offense)
- Procurement—substitution or nonconforming product
 - 223 cases (Number of cases by most prevalent investigated offense)
 - 573 suspects (Number of known suspects by most prevalent investigate offense)

Air Force Office of Special Investigations

- 564 cases (Number of cases with at least one investigative offense)
- 1,103 suspects (Number of known suspects with at least one investigated offense)
- False, fictitious, or fraudulent claims
 - 37 cases (Number of cases by most prevalent investigated offense)
 - 74 suspects (Number of known suspects by most prevalent investigate offense)
- Civil False Claims Act
 - 34 cases (Number of cases by most prevalent investigated offense)
 - 47 suspects (Number of known suspects by most prevalent investigate offense)
- Fraud: make false claim
 - 27 cases (Number of cases by most prevalent investigated offense)
 - 38 suspects (Number of known suspects by most prevalent investigate offense)

Naval Criminal Investigative Service

- **432 cases (Number of cases with at least one investigative offense)**
- **807 suspects (Number of known suspects with at least one investigated offense)**
- **False fictitious, or fraudulent claims**
 - **138 cases (Number of cases by most prevalent investigated offense)**
 - **233 suspects (Number of known suspects by most prevalent investigate offense)**
- **False statements**
 - **103 cases (Number of cases by most prevalent investigated offense)**
 - **186 suspects (Number of known suspects by most prevalent investigate offense)**
- **Civil False Claims Act of 1863, as amended**
 - **72 cases (Number of cases by most prevalent investigated offense)**
 - 107 suspects (Number of known suspects by most prevalent investigate offense)

Army Criminal Investigation Division

- 520 cases (Number of cases with at least one investigative offense)
 - 1,066 suspects (Number of known suspects with at least one investigated offense)
 - Civil False Claims Act
-

Letter

-
-
- 141 cases (Number of cases by most prevalent investigated offense)
 - 215 suspects (Number of known suspects by most prevalent investigate offense)
 - False claim
 - 95 cases (Number of cases by most prevalent investigated offense)
 - 153 suspects (Number of known suspects by most prevalent investigate offense)
 - False statement—making or signing
 - 73 cases (Number of cases by most prevalent investigated offense)
 - 111 suspects (Number of known suspects by most prevalent investigate offense)
-

Sources: GAO analysis of Department of Defense (DOD) data; DOD (agency seals). | GAO-24-105358

Note: Each Defense Criminal Investigative Organization collects information in separate case management systems and has separate policies for data entry. Offense information can, therefore, be listed under different terminology across the different systems. In general, we provided the offense terminology as listed in the case management system. However, for the purposes of this figure, we removed any listed legal citations. We used case count to determine prevalence for the purposes of our analysis.

Figure 10: Most Prevalent Offenses for Which Remedies Were Pursued for Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021



Number of cases with at least one offense for which a remedy was pursued
 Number of known suspects with at least one offense for which a remedy was pursued
 Number of cases by most prevalent offense for which a remedy was pursued
 Number of known suspects by most prevalent offense for which a remedy was pursued

Sources: GAO analysis of Department of Defense (DOD) data; DOD (agency seals). | GAO-24-105358

Letter

Accessible Data for Figure 10: Most Prevalent Offenses for Which Remedies Were Pursued for Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021

Letter

Defense Criminal Investigative Service

- 248 cases (Number of cases with at least one offense for which a remedy was pursued)
- 855 suspects (Number of known suspects with at least one offense for which a remedy was pursued)
- False Claims Act
 - 90 cases (Number of cases by most prevalent offense for which a remedy was pursued)
 - 855 suspects (Number of known suspects by most prevalent offense for which a remedy was pursued)
- Wire fraud
 - 49 cases (Number of cases by most prevalent offense for which a remedy was pursued)
 - 107 suspects (Number of known suspects by most prevalent offense for which a remedy was pursued)
- Conspiracy
 - 41 cases (Number of cases by most prevalent offense for which a remedy was pursued)
 - 120 suspects (Number of known suspects by most prevalent offense for which a remedy was pursued)

Air Force Office of Special Investigations

- 54 cases (Number of cases with at least one offense for which a remedy was pursued)
- 110 suspects (Number of known suspects with at least one offense for which a remedy was pursued)
- Civil False Claims Act
 - 10 cases (Number of cases by most prevalent offense for which a remedy was pursued)
 - 16 suspects (Number of known suspects by most prevalent offense for which a remedy was pursued)
- Wire fraud
 - 9 cases (Number of cases by most prevalent offense for which a remedy was pursued)
 - 17 suspects (Number of known suspects by most prevalent offense for which a remedy was pursued)
- False statements
 - 8 cases (Number of cases by most prevalent offense for which a remedy was pursued)
 - 17 suspects (Number of known suspects by most prevalent offense for which a remedy was pursued)

Naval Criminal Investigative Service

- 122 cases (Number of cases with at least one offense for which a remedy was pursued)
- 287 suspects (Number of known suspects with at least one offense for which a remedy was pursued)
- False fictitious, or fraudulent claims
 - 28 cases (Number of cases by most prevalent offense for which a remedy was pursued)
 - 47 suspects (Number of known suspects by most prevalent offense for which a remedy was pursued)
- False Statements
 - 25 cases (Number of cases by most prevalent offense for which a remedy was pursued)
 - 53 suspects (Number of known suspects by most prevalent offense for which a remedy was pursued)
- Civil False Claims Act of 1863, as amended
 - 17 cases (Number of cases by most prevalent offense for which a remedy was pursued)
 - 21 suspects (Number of known suspects by most prevalent offense for which a remedy was pursued)

Army Criminal Investigation Division^a

- 45 cases (Number of cases with at least one offense for which a remedy was pursued)
 - 129 suspects (Number of known suspects with at least one offense for which a remedy was pursued)
 - Civil False Claims Act
-

Letter

-
- 5 cases (Number of cases by most prevalent offense for which a remedy was pursued)
 - 11 suspects (Number of known suspects by most prevalent offense for which a remedy was pursued)
 - Laundering of monetary instruments
 - 2 cases (Number of cases by most prevalent offense for which a remedy was pursued)
 - 2 suspects (Number of known suspects by most prevalent offense for which a remedy was pursued)
 - Theft
 - 2 cases (Number of cases by most prevalent offense for which a remedy was pursued)
 - 4 suspects (Number of known suspects by most prevalent offense for which a remedy was pursued)
-

Sources: GAO analysis of Department of Defense (DOD) data; DOD (agency seals). | GAO-24-105358

Note: Each Defense Criminal Investigative Organization collects information in separate case management systems and has separate policies for data entry. Offense information can, therefore, be listed under different terminology across the different systems. In general, we provided the offense terminology as listed in the case management system. However, for the purposes of this figure, we removed any listed legal citations. We used case count to determine prevalence for the purposes of our analysis.

^aThe Army Criminal Investigation Division data contained some offenses that were labeled similarly—such as relating to the Civil False Claims Act—but with slightly different terminology. Additional cases may have also involved the Civil False Claims Act or other offenses we present in this figure. Further, additional offenses in the Army data were equally prevalent to those we present in this figure; those we present are examples for illustrative purposes.

The data that investigators enter in the fields describing investigated offenses and offenses for which remedies were pursued can vary due to factors such as the structure of the DCIO's case management system, including whether data are entered manually or using drop-down menus; investigator discretion; and the information available at the time of data entry. DCIO officials acknowledged that offense data may be incomplete or outdated because investigators are not required to enter data about all offenses involved with a case into the case management system, or to update the data if they change throughout the course of an investigation. In addition, DCIO officials told us that investigators might not always have insight into the charges filed against a suspect. For example, USACID officials said that investigators' involvement ends once they submit their cases to commanders; post-investigative or judicial activities can take a long time to resolve; and investigators are not required to follow up with the cases after they have concluded the investigation.

Number and types of adjudicated offenses. Each DCIO collects at least some data in structured fields describing adjudicated offenses—offenses that were ultimately adjudicated as fraud through a judicial or

other adjudicative system.⁷⁴ Such data on the extent and types of adjudicated fraud, while potentially incomplete, can provide valuable insight into types and possible emerging trends of fraud risks faced by DOD. This information could help DOD design and implement data-analytic tests to prevent and detect fraud; evaluate fraud risk management activities by identifying potential control deficiencies; and adapt fraud risk management activities. For example, DOD could use available information on fraud schemes to help design data-analytic tests to identify signs of fraud that may exist in DOD's contracting data, or to evaluate and improve its existing controls. DOD could also use such information to better understand the impact of procurement fraud risks, including the financial and reputation impacts. With this information, DOD would be better able to determine its fraud risk tolerance.

We used available data to calculate the number of alleged procurement fraud cases involving offenses adjudicated as fraud for each DCIO, as recorded in structured fields we selected based on review of the data and consultation with DCIO officials.⁷⁵ For example, of the 444 cases we identified in the NCIS data, we identified 67, or about 15 percent, that involved at least one known suspect with an adjudicated offense. The remaining 377 cases, or about 85 percent, did not have recorded adjudicated offenses in the structured data fields we used for this analysis. Some of the 377 NCIS cases with no recorded adjudicated offenses had nonadjudicative outcomes, such as dismissals. See table 3 for the number of cases with recorded adjudicated offenses and example nonadjudicative outcomes for each DCIO.

⁷⁴We identified adjudicated offenses involved with the cases in our analysis. However, not all the adjudicated offenses may have been related to procurement fraud. While the cases in our analysis had an alleged procurement fraud focus, they also may have led to other types of adjudicated fraud. For example, an alleged procurement fraud case could have involved adjudicated theft or forgery charges that were unrelated to procurement.

⁷⁵We reviewed the data and consulted with DCIO officials to determine the most appropriate fields to use for analysis. Our analysis may not have captured all cases involving adjudicated offenses or all adjudicated offenses involved within a case, if these outcomes were not recorded in the fields we used for analysis. In addition, cases can involve multiple suspects, and suspects can have multiple offenses. Therefore, the cases we identified as involving adjudicated offenses may also involve offenses with other nonadjudicative outcomes, such as dismissals. The adjudicated offense information we report for DCIS may also be understated because 14 of the DCIS cases in our analysis had some sealed adjudicative information, according to the data provided.

Table 3: Number of Cases with Recorded Adjudicated Offenses and Example Nonadjudicative Outcomes among Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021

na	Number of cases	Number of cases	Number of cases	Number of cases
Category	Total	At least one adjudicated offense	No adjudicated offenses	Example nonadjudicative outcomes for cases with no adjudicated offenses ^a
Defense Criminal Investigative Service	1,165	125 (11 percent of total cases) ^b	1040 (89 percent of total cases)	Civil settlements: 142 cases Criminal dismissals: 18 cases
Air Force Office of Special Investigations	564	46 (8 percent of total cases)	518 (92 percent of total cases)	Charges withdrawn: 30 cases Dismissals: 23 cases
Army Criminal Investigation Division	520	26 (5 percent of total cases)	494 (95 percent of total cases)	Prosecution declined/other: 50 cases "No probable cause" determination by attorney: 22 cases
Naval Criminal Investigative Service	444	67 (15 percent of total cases)	377 (85 percent of total cases)	Dismissals: 42 cases Suspect found not guilty: 7 cases

Source: GAO analysis of Department of Defense data. | GAO-24-105358

Note: We define adjudicated offenses as offenses that were ultimately adjudicated through a judicial or other adjudicative system as fraud. While these offenses were involved in cases that we determined were related to alleged procurement fraud, not all the offenses may have been related to procurement fraud. We reviewed the data and consulted with Defense Criminal Investigative Organization officials to determine the most appropriate structured fields to use to identify cases with adjudicated offenses. However, our analysis may not have captured all cases involving adjudicated offenses, or all adjudicated offenses involved with a case. In addition, cases can involve multiple suspects, and suspects can have multiple offenses. Therefore, the cases we identified as involving adjudicated offenses may also involve nonadjudicative outcomes, such as dismissals.

^aThis table presents example outcomes and does not contain an exhaustive list of outcomes for the cases we identified with no adjudicated offenses.

^bAn additional 67 Defense Criminal Investigative Service cases had data showing that a suspect was convicted but with no listed adjudicated offense.

Offenses Adjudicated – Illustrative Case Studies



Offenses may be adjudicated via various mechanisms, including criminal and civil legal proceedings and administrative proceedings.

In one of the closed Air Force Office of Special Investigations cases we reviewed, a criminal court adjudicated the offenses charged against six defendants. The defendants were convicted for participating in the fraud scheme.

Certain defendants pled guilty and were convicted of fewer offenses than those for which they were initially charged. For example, one defendant was charged with 21 counts of various offenses and ultimately pled guilty to, and was convicted of, one count of conspiracy to commit wire fraud and one count of tax evasion. The remaining charges were dismissed.

In one of the closed Army Criminal Investigation Division cases that we reviewed, fraudsters' offenses were adjudicated in administrative proceedings, resulting in the fraudsters' debarment from government contracting.

Sources: GAO review of Department of Defense closed investigative case files and other case documentation; Icons-Studio/stock.adobe.com (icon). | GAO-24-105358

Available data from the DCIOs show that the cases involved a range of adjudicated offenses, such as false statements, wire fraud, bribery, and conspiracy. See figure 11 for the number of cases with adjudicated offenses, as well as the most prevalent types of adjudicated offenses, in each DCIO's case management data. See sidebar for examples of adjudicated offenses in the investigative case studies we completed.

Figure 11: Most Prevalent Types of Adjudicated Offenses among Closed Department of Defense Procurement Fraud Cases from Fiscal Years 2015 through 2021



Number of cases with at least one adjudicated offense
 Number of known suspects with at least one adjudicated offense
 Number of cases by most prevalent adjudicated offense
 Number of known suspects by most prevalent adjudicated offense

Sources: GAO analysis of Department of Defense (DOD) data; DOD (agency seals). | GAO-24-105358

Letter

Accessible Data for Figure 11: Most Prevalent Types of Adjudicated Offenses among Closed Department of Defense Procurement Fraud Cases from Fiscal Years 2015 through 2021

Defense Criminal Investigative Service

- 125 cases^a (Number of cases with at least one adjudicated offense)
- 274 suspects (Number of known suspects with at least one adjudicated offense)
- Wire fraud
 - 32 cases (Number of cases by most prevalent adjudicated offense)
 - 37 suspects (Number of known suspects by most prevalent adjudicated offense)
- Conspiracy
 - 28 cases (Number of cases by most prevalent adjudicated offense)
 - 51 suspects (Number of known suspects by most prevalent adjudicated offense)
- Bribery
 - 18 cases (Number of cases by most prevalent adjudicated offense)
 - 43 suspects (Number of known suspects by most prevalent adjudicated offense)

Air Force Office of Special Investigations

- 46 cases (Number of cases with at least one adjudicated offense)
- 93 suspects (Number of known suspects with at least one adjudicated offense)
- Wire fraud
 - 12 cases (Number of cases by most prevalent adjudicated offense)
 - 22 suspects (Number of known suspects by most prevalent adjudicated offense)
- Bribery of public officials and witnesses
 - 7 cases (Number of cases by most prevalent adjudicated offense)
 - 17 suspects (Number of known suspects by most prevalent adjudicated offense)
- Conspiracy to commit offense or to defraud the government
 - 6 cases (Number of cases by most prevalent adjudicated offense)
 - 23 suspects (Number of known suspects by most prevalent adjudicated offense)

Naval Criminal Investigative Service

- 67 cases (Number of cases with at least one adjudicated offense)
- 133 suspects (Number of known suspects with at least one adjudicated offense)
- False statements
 - 11 cases (Number of cases by most prevalent adjudicated offense)
 - 14 suspects (Number of known suspects by most prevalent adjudicated offense)
- Wire fraud
 - 11 cases (Number of cases by most prevalent adjudicated offense)
 - 24 suspects (Number of known suspects by most prevalent adjudicated offense)
- Conspiracy to commit offense or to defraud the United States
 - 11 cases (Number of cases by most prevalent adjudicated offense)
 - 23 suspects (Number of known suspects by most prevalent adjudicated offense)

Army Criminal Investigation Division^b

- 26 cases (Number of cases with at least one adjudicated offense)
 - 88 suspects (Number of known suspects with at least one adjudicated offense)
 - Kickbacks
-

Letter

-
- 2 cases (Number of cases by most prevalent adjudicated offense)
 - 7 suspects (Number of known suspects by most prevalent adjudicated offense)
 - Bribery
 - 1 case (Number of cases by most prevalent adjudicated offense)
 - 1 suspect (Number of known suspects by most prevalent adjudicated offense)
 - Aircraft or space vehicle parts fraud
 - 1 case (Number of cases by most prevalent adjudicated offense)
 - 3 suspects (Number of known suspects by most prevalent adjudicated offense)
-

Sources: GAO analysis of Department of Defense (DOD) data; DOD (agency seals). | GAO-24-105358

Note: Each Defense Criminal Investigative Organization (DCIO) collects information in separate case management systems and has separate policies for data entry. Offense information can, therefore, be listed under different terminology across the different systems. In general, we provided the offense terminology as listed in the case management system. However, for the purposes of this figure, we removed any listed legal citations. We define adjudicated offenses as offenses that were ultimately adjudicated through a judicial or other adjudicative system as fraud. While these offenses were involved in cases that we determined were related to alleged procurement fraud, not all the offenses may have been related to procurement fraud. We reviewed the data and consulted with DCIO officials to determine the most appropriate structured fields to use to identify cases with adjudicated offenses. However, our analysis may not have captured all cases involving adjudicated offenses, or all adjudicated offenses involved with a case. We used case count to determine prevalence for the purposes of our analysis.

^aAn additional 67 Defense Criminal Investigative Service cases had data showing that a suspect was convicted but with no listed adjudicated offense.

^bAdditional offenses in the Army data were equally prevalent to those we present in this figure; those we present are examples for illustrative purposes.

As with investigated offenses and offenses for which remedies were pursued, the data that investigators enter as related to adjudicated offenses can vary by a range of factors. According to DCIO officials, the data may be incomplete because investigators may not always have insight into the results of trial or other judicial proceedings, or they may not record the results.⁷⁶

Other case outcomes. The DCIOs vary in the extent to which they collect structured data illustrating other outcomes of the alleged and adjudicated procurement fraud cases, such as financial impacts of fraud, sentences imposed, and reasons for case clearance. However, available data can provide additional visibility on the results of DOD's procurement fraud monitoring and detection activities, as well as financial impacts of procurement fraud risks faced by DOD. This information could help DOD

⁷⁶We reviewed the data and discussed with DCIO officials to identify the best structured fields to use to determine which cases involved adjudicated fraud. Our analysis may not have captured all cases involving adjudicated offenses, or all adjudicated offenses involved within a case, if these outcomes were not recorded in the fields we used for analysis. Some of the fields we used for analysis were blank or unknown for most cases. Blank or unknown values could be expected where a case did not lead to an adjudicative outcome.

identify and assess the impact of risks affecting the program and adapt fraud risk management activities. For example, DOD could use available information on estimated dollar loss to the federal government to help assess the impact of adjudicated offenses.

DCIS has a structured field representing the estimated dollar loss to the federal government, reflecting the total estimated financial amount lost due to fraud involved with a particular case, as estimated by investigators at the onset of an investigation.⁷⁷ The total recorded estimated dollar loss to the federal government for 74 of the 125 cases with adjudicated offenses in the DCIS data was about \$679 million.⁷⁸ The estimated dollar loss ranged from \$15,000 to \$350 million and averaged about \$950,000 per case.⁷⁹ These amounts may not reflect the total extent of actual fraud that was committed. Because of fraud's deceptive nature, financial losses may not be identified, and such losses are difficult to reliably estimate.

The other DCIOs do not have structured fields illustrating financial impacts of fraud for the federal government.⁸⁰ However, each DCIO collects sentencing data, which can provide insight into impacts for fraud participants.⁸¹

For example, the DCIS and NCIS case management systems have structured fields illustrating the type and quantity of sentences imposed

⁷⁷DCIS documentation specifies that the estimate is based on an investigator's subjective assessment of the facts surrounding a case, and the investigator does not need to obtain objective evidence to support the estimate. However, according to the documentation, the estimate should be reasonable and based on information documented in the case initiation or other investigative report, which, in some instances, must be reviewed by supervisors. The documentation also states that the estimate should be updated throughout the course of an investigation, if necessary. However, officials told us there is no process in place to update the estimates.

⁷⁸The remaining DCIS cases with adjudicated offenses did not have data on estimated dollar loss to the federal government.

⁷⁹For the purposes of this report, we used median to illustrate the average.

⁸⁰NCIS officials stated that information on estimated dollar loss to the federal government is documented in reports in NCIS investigative files and not in a structured data field.

⁸¹Data on the type and quantity of sentences can also provide some insight into estimated additional costs, such as the costs of incarceration or supervision, borne by the federal government.

for a suspect, which allow for analysis of outcomes such as the frequency and extent of restitution, penalties, fines, confinement, and probation.⁸²

In our analysis of available data, we identified the following:⁸³

- DCIS: a total of \$115 million ordered in restitution, penalties, and fines for 146 of the 274 known suspects with at least one adjudicated offense in the DCIS data.⁸⁴ The dollar amount for these sentences ranged from \$1 to \$45 million and averaged \$3,000 per sentence.
- NCIS: a total sanction amount of at least \$257.8 million for 112 of the 133 known suspects with at least one adjudicated offense.⁸⁵ The sanction amount ranged from \$100 to \$29 million and averaged about \$215,400 per sentence.⁸⁶
- For both DCIOs, other sentences included confinement, probation, and debarment, among others. For instance, available DCIS data showed that 84 known suspects were sentenced to confinement for an average of about 21 months.

⁸²Because multiple offenses can be pursued against an individual suspect, it is possible for an individual suspect to have multiple sentences.

⁸³As our data could include joint NCIS and DCIS cases, the amounts we report may overlap.

⁸⁴In our analysis of DCIS data, we took steps to exclude any duplicate sentences for a suspect within a case to prevent possible inflation of sentence amounts. It is, therefore, possible that we undercounted total sentence amounts to the extent any suspects had multiple, identical sentences.

⁸⁵The data we received from NCIS do not provide the amount per sanction where individuals received multiple sanctions. We, therefore, cannot calculate total amounts for specific types of sanctions. However, the internal data available to NCIS officials do offer this distinction. In addition, the total sanction amounts we report for NCIS are likely undercounted. According to NCIS officials, it is possible that where multiple suspects within a case collectively owed an amount, the amount was duplicated for each suspect's records in the data we received. We took steps to exclude any duplicate sanction amounts within a case to prevent possible inflation of sanction amounts. However, it is, therefore, possible that we undercounted total sanction amounts. Further, according to NCIS officials, some sanction data exist in narrative fields and court documents, rather than in the structured fields we used for analysis.

⁸⁶Sanction amounts could vary significantly across recipients.

Financial and Nonfinancial Impacts of Fraud – Illustrative Case Study



The fraud scheme in one of the closed Defense Criminal Investigative Service cases we reviewed involved a fraudster who provided purposefully falsified documents, including a fraudulent certificate of conformance for a machine gun bipod compression spring, to conceal the fraudster's company's failure to maintain contractually required manufacturing standards.

Financial impacts

- **To the Department of Defense (DOD):** DOD paid the fraudster about \$124,200.
- **To fraudster:** The fraudster was ordered to pay about \$124,200 in restitution and a \$100 assessment.

Nonfinancial impacts

- **To DOD:** A military engineer tested one of the bipods that the company manufactured and found a number of deficiencies, including a broken compression spring. These deficiencies could pose potential safety hazards and have potential national security impacts.
- **To fraudster:** The fraudster was sentenced to prison for time served (10 months) and to 3 years' supervised release. The fraudster was also debarred from federal government contracting for 5 years.

Sources: GAO review of DOD closed investigative case files and other case documentation; Icons-Studio/stock.adobe.com (icon). | GAO-24-105358

The AFOSI and USACID case management systems collect data on some sentence types and quantities and, therefore, allow for analysis of some outcomes. For example:

- For AFOSI, of the known suspects with at least one adjudicated offense, we identified 15 sentenced to debarment. Of these, nine had sentence length listed, which averaged 36 months.
- For USACID, of the known suspects with at least one adjudicated offense, we identified 18 sentenced to debarment, ranging from 3 to 100 years, and three sentenced to confinement ranging from 8 to 21 months.

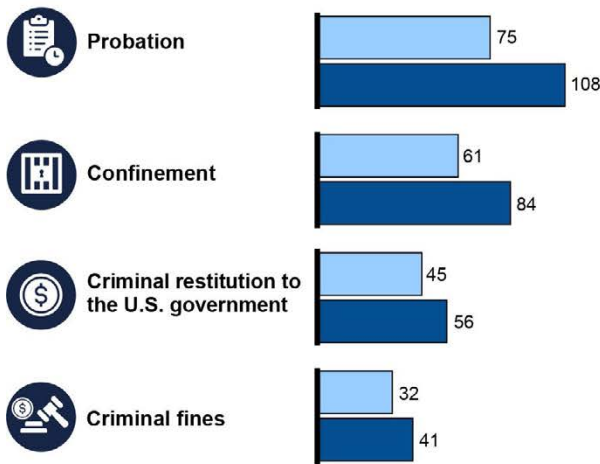
However, while the NCIS and DCIS cases we identified with at least one adjudicated offense generally contained data on sentencing information, a smaller proportion of AFOSI and USACID cases contained these data.⁸⁷ See sidebar for information on financial and nonfinancial impacts from a

⁸⁷Specifically, of the 67 NCIS cases we identified with at least one offense adjudicated as fraud, 66, or 99 percent, contained sentencing data. Each of the 125 DCIS cases we identified with at least one offense adjudicated as fraud contained sentencing data. Of the 46 AFOSI cases we identified with at least one offense adjudicated as fraud, 23, or 50 percent, contained sentencing data. Of the 26 USACID cases we identified with at least one offense adjudicated as fraud, 12, or 46 percent, contained sentencing data.

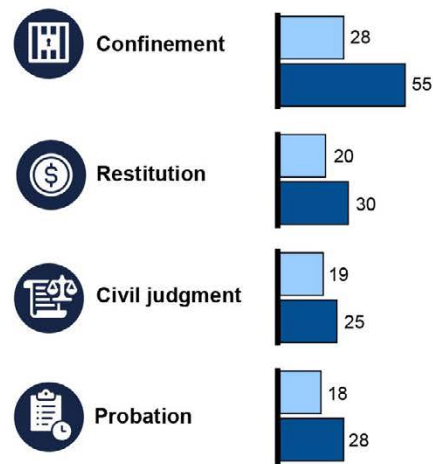
DCIS case we studied. Figure 12 provides additional information on sentences.

Figure 12: Example Sentences by Suspect and Case Counts for Closed Defense Criminal Investigative Service and Naval Criminal Investigative Service Procurement Fraud Cases from Fiscal Years 2015 through 2021

Example Defense Criminal Investigative Service sentences



Example Naval Criminal Investigative Service sentences



Number of cases
Number of known suspects

Sources: GAO analysis of Department of Defense data; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

Accessible Data for Figure 12: Example Sentences by Suspect and Case Counts for Closed Defense Criminal Investigative Service and Naval Criminal Investigative Service Procurement Fraud Cases from Fiscal Years 2015 through 2021

Example Defense Criminal Investigative Service sentences	Number of cases	Number of known suspects
Probation	75	108
Confinement	61	84
Criminal restitution to the U.S. government	45	56
Criminal fines	32	41

Example Naval Criminal Investigative Service sentences	Number of cases	Number of known suspects
Confinement	28	55
Restitution	20	30
Civil judgment	19	25

Example Naval Criminal Investigative Service sentences	Number of cases	Number of known suspects
Probation	18	28

Sources: GAO analysis of Department of Defense data; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

Note: Cases and suspects can appear in multiple categories. The counts we present are, therefore, not additive. The information we present in this figure is for cases and known suspects we identified with at least one adjudicated offense. We define adjudicated offenses as offenses that were ultimately adjudicated through a judicial or other adjudicative system as fraud. While these offenses were involved in cases we determined were related to alleged procurement fraud, not all the offenses may have been related to procurement fraud. We reviewed the data and consulted with Defense Criminal Investigative Organization officials to determine the most appropriate structured fields to use to identify cases with adjudicated offenses. However, our analysis may not have captured all cases involving adjudicated offenses, or all adjudicated offenses involved with a case.

Each DCIO’s case management system also has one or more structured fields illustrating various reasons for case clearance, such as where prosecution was declined, or charges were withdrawn.⁸⁸ The DCIS and NCIS case management systems also have fields describing the reason for prosecution declination. According to available data, of the 1,165 DCIS cases we identified, at least 683 involved suspects for whom there was a prosecution declination. The data also showed that of the 1,165 cases, there were 388 cases where there was a prosecution declination for all suspects. The most prevalent reasons for prosecution declination for the DCIS cases included weak or insufficient evidence and civil, administrative, or other disciplinary alternatives. Of the 444 NCIS cases we identified, 82 involved suspects for whom there was a prosecution declination. Listed reasons included a lack of evidence of criminal intent and, separately, the allegations were determined to be unfounded.

According to AFOSI and USACID officials, their structured fields on case outcomes may be left blank, and much of the data may be in narrative reports. We identified one AFOSI case, of the 564 we identified, involving suspects who were referred for court-martial proceedings. Of the 520 USACID cases we identified, we identified 50 that involved suspects for whom there was a prosecution declination and six that were declined without explanation.⁸⁹

⁸⁸We define case clearance as a decision not to pursue remedies against a particular suspect. The Department of Justice, rather than DOD, makes prosecution declination decisions—that is, whether to pursue remedies in court. The fields we identified describing reasons for case clearance may also describe other, unrelated outcomes.

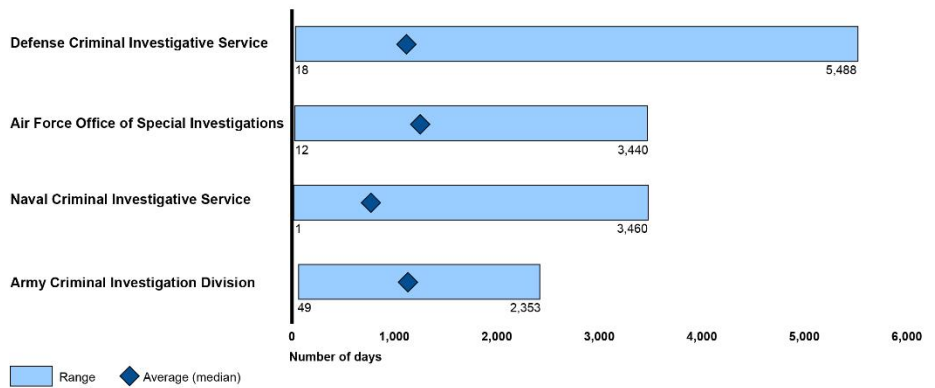
⁸⁹USACID officials stated *Declined Without Explanation* is when the commander or prosecutor decides to take no action on an offense but does not provide a specific reason for the decision. This is distinguishable from the Prosecution Decline/Other option, which relates to a subject being investigated for multiple offenses for which the adjudication action proceeded on some, but not all.

As with offense data, case outcome data may be incomplete. According to DCIO officials, investigators may not always have insight into this stage of the case, or record these data, even when known.

Case duration. Each DCIO collects structured data on case open and closed dates, which can provide an estimate of the duration of alleged and adjudicated procurement fraud cases. Case closed dates could occur long after the DCIO’s role in an investigation is complete, depending on factors such as the length of time involved with adjudication efforts and the timeliness by which case outcome information is communicated to investigators. However, available case duration data can still provide visibility into DOD’s procurement fraud monitoring and detection activities by providing an estimate of the length of time and resources generally required for investigating cases of procurement fraud.

We used the case open and closed dates to calculate case duration for each DCIO. We found that average case duration ranged from about 2.1 years, for NCIS, to about 3.4 years, for AFOSI.⁹⁰ See figure 13.

Figure 13: Average and Range of Case Duration for Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021



⁹⁰For DCIS, we excluded cases with duration of less than 2 days from this analysis because DCIS officials told us that those durations may reflect inaccurate case open dates.

Accessible Data for Figure 13: Average and Range of Case Duration for Alleged and Adjudicated Department of Defense Procurement Fraud Cases Closed from Fiscal Years 2015 through 2021

Defense Criminal Investigative Organization	Range	Average (median)
Defense Criminal Investigative Service	1 day – 5,488 days	1,102 days
Air Force Office of Special Investigations	12 days – 3,440 days	1,237 days
Naval Criminal Investigative Service	1 day – 3,460 days	755 days
Army Criminal Investigation Division	49 days – 2,353 days	1,117 days

Source: GAO analysis of Department of Defense data. | GAO-24-105358

Note: For the Defense Criminal Investigative Service (DCIS), we excluded cases with duration of less than 2 days from this analysis because DCIS officials told us that those durations may reflect inaccurate case open dates.

DCIOs may collect data on the date that investigative steps were completed prior to submission of a case for administrative or judicial decision. This date, together with the case open date, can provide a more precise illustration of the duration of the DCIO’s portion of an investigation. For example, using these data for NCIS, we found that the duration of NCIS’s portion of an investigation averaged about 1.7 years.

DOD Investigative Data on Alleged and Adjudicated Procurement Fraud Cases Are Not Always Complete and Cannot Always Be Readily Analyzed

Investigative Data Were Not Always Complete

We found that the investigative data on alleged and adjudicated procurement fraud cases were not always complete for the purpose of fraud-related data analytics. All four DCIOs require that a subset of fields be completed for all cases. Required fields vary by DCIO and include, for example:

- unique case identification numbers;
- fields specifying if a person for whom a record is created is a suspect or victim; and
- incident details, such as the date an alleged incident occurred.

Beyond required fields, according to DCIO officials and documentation, the facts and circumstances of a specific case will inform which fields the investigators populate. For example, if a case did not involve theft, then

fields associated with documenting a property loss would not be completed. DCIO officials said that investigators use judgment when completing fields, and that prior to closing a case, supervisors review cases to ensure that pertinent data have been entered. Further, officials from all four DCIOs told us that data in structured fields may not be populated because a field is not required; investigators may not have the data at the time of data entry; and investigators may not always update structured fields where the circumstances of a case change, or additional data are received.

We identified some structured fields that could be informative for DOD fraud risk management, but those fields were not always required and not always complete.

- **Data on offenses investigated.** These data could provide DOD with insights on the types and possible emerging trends of fraud risks faced. This information could help DOD evaluate and adapt fraud risk management activities, such as by using information on alleged fraud schemes to evaluate whether to adjust its controls. However, DCIO officials stated that investigators are not required to enter all investigated offenses involved with a case. For DCIS, the structured field on investigated offenses was blank for 1,118, or about 96 percent, of the 1,165 cases we identified.⁹¹ According to officials, the field is largely incomplete because it is not required.
- **Data on offenses for which remedies were pursued.** These data could also provide DOD insights on the types and possible emerging trends of fraud risks faced. For USACID, the structured field used to collect data on offenses for which remedies were pursued was blank for 475 of 520 cases, or about 91 percent of cases. Officials stated that this field was not required.⁹² An Army official noted that the field might be left blank because this type of data becomes available at a later time through the legal process, and investigators have moved on to other cases.
- **Data on case outcomes.** These data could provide DOD with insights into the results of fraud monitoring and detection efforts. For

⁹¹We limited all our DCIO analyses to cases with at least one suspect. In addition, in our reporting of DCIS investigated offense data, we used case category data to supplement our analysis, where a case did not have a listed investigated offense.

⁹²According to the USACID's Army Law Enforcement Reporting and Tracking System (ALERTS) manual, the charged offense field must be populated in the Commander's Report of Disciplinary or Administrative Action (Form 4833).

AFOSI, the structured field used to collect data on case outcomes, such as if a case was dismissed or an adjudication was obtained, was blank for 496 of the 564 cases, or 88 percent. Officials said this was because the data are frequently documented in narrative fields and that completing the case outcome field is not mandatory. Sanction type, such as prison sentences or fines, could not always be determined by the structured field.

According to AFOSI officials, the data have at least two fields to document the lengths or amounts that correspond to the sentences or fines. One field documents numeric values, which ranged from 1 to 1,375,000, and the other field documents the unit, such as dollars or years. For 667 of the 3,153 records (167 out of 458 cases) that had values in the sanctions duration field, the corresponding field documenting units was blank. Officials did not expressly confirm if these fields were required, and we could not determine this based on a review of technical documents. Officials stated that investigators are required to indicate some sort of disposition to close a case, which can include no action. Officials also noted that such data could be found in the narrative field.

Investigative Data Could Not Always Be Readily Analyzed, Including by Aggregating Data Across DCIOs

We found that the investigative data on alleged and adjudicated procurement fraud could not always be readily analyzed for various reasons. For example:

- **Lack of shared identifier allowing for the connection of data on joint cases investigated by multiple DCIOs.** We found that data could not be readily aggregated across DCIOs due to a lack of a shared identifier. This type of identifier would help DOD measure fraud risks across DOD, rather than risks specific to an individual DOD component. While we were able to identify the number of cases by DCIO, we could not fully account for joint investigations because there is no shared identifier across case management systems that can be used to track joint investigations. Therefore, we could not seek to develop a total number of cases investigated and could not calculate other totals, such as the total number of DOD's alleged procurement fraud cases involving adjudicated offenses.
- **Lack of structured fields identifying cases as involving alleged and adjudicated procurement fraud.** We had to perform varying levels of analysis to identify alleged and adjudicated procurement

fraud cases. DCIS and NCIS have structured fields that collect data on case categories. We used the case category field to identify alleged and adjudicated procurement fraud cases for DCIS, and NCIS officials used the field to provide us with data on alleged and adjudicated procurement fraud cases.⁹³ However, neither USACID nor AFOSI have structured fields that could be used to identify alleged and adjudicated procurement fraud cases for our purposes.⁹⁴ As a result, we analyzed the USACID and AFOSI narrative fields using a natural language processing model to classify text and identify a pool of potentially relevant cases, which was further refined through keyword searches that targeted specific terms. Being able to readily identify alleged and adjudicated procurement fraud cases would facilitate DOD's efforts to assess fraud risks and take corresponding actions to improve fraud risk management.

- **Lack of structured fields identifying cases that involved adjudicated offenses.** We found that identifying cases involving adjudicated offenses required varying degrees of analysis. For example, for USACID, we used three separate structured fields to determine if a case involved adjudicated offenses.

For AFOSI, we analyzed a field that contains information on case outcomes, such as whether a suspect was convicted or acquitted, and compared it with a field with high-level offense categorizations, such as "wire fraud" and "Civil False Claims Act," to identify cases involving adjudicated offenses.⁹⁵

We likely did not capture all cases involving adjudicated offenses. As previously noted, the data may be incomplete where investigators do

⁹³We reviewed case categorization schemes for DCIS and NCIS to inform our data request. Our request included case categories that were not exclusive to procurement fraud cases but could potentially include them. This was because the focus of an investigation may evolve over time, but investigators may not always update case category fields accordingly. NCIS officials did not provide records for all case categories we requested and, instead, provided records for case categories they determined were intended for investigation of procurement fraud-related criminal offenses. NCIS advised that procurement fraud-related offenses would rarely be involved in investigations under other case categories such as narcotics, sexual assault, or death.

⁹⁴USACID has fields to collect information on if a case is contract fraud related, the contract ID, and the contract number. However, among the cases we identified as being procurement fraud related, the contract fraud field was blank for 286 of 520 cases, or 55 percent; the contract ID field was blank for 242 of 520 cases, or 47 percent; and the contract number field was blank for 246 of 520 cases, or 47 percent.

⁹⁵ AFOSI officials noted that a field that tracks the AFOSI region leading the investigation could be used to identify fraud cases.

not have insight into case outcomes or do not record the results, and some fields we used for our analysis were blank or unknown for most cases. Further, our analysis may not have captured all cases involving adjudicated offenses, or all adjudicated offenses involved with a case, if these outcomes were not recorded in the fields we used for analysis. The results of our analysis of structured data may, therefore, be understated, which we acknowledge in this report.

Being able to readily identify information on adjudicated offenses could help DOD evaluate existing fraud risks and take corresponding actions to improve fraud risk management.

- **Differences in type and organization of data collected.** DCIOs collect similar, though varying, types of data. For example, USACID has a field that is used to provide high-level categorizations of cases and can be used to identify investigated offenses involved with a case. The values in the field are a unique system of codes that help facilitate regularly occurring Defense Incident-Based Reporting System reporting requirements to record offense information.⁹⁶ We referenced a USACID crosswalk to determine which cases pertained to fraud or contract fraud, since it was not always apparent from other fields containing offense name or description. Additionally, the crosswalk also links the offense codes to the federal statute or Uniform Code of Military Justice article that a suspect is investigated for or charged with. DCIS has several fields used to collect offense-related information. Values in the field used to collect information on offenses investigated generally use high-level categorizations such as “False Statements” and “Wire Fraud.” The vast majority of the values in the field used by DCIS to track offenses for which remedies were pursued are citations for federal statutes.⁹⁷ Differences in the type and organization of data collected resulted in our needing to take several, varying analytical steps for each DCIO to develop information that would be comparable.

⁹⁶The Defense Incident-Based Reporting System is DOD’s centralized reporting system to the Federal Bureau of Investigation’s National Incident-based Reporting System (NIBRS). NIBRS is a system for collecting data on crime from federal, state, local, and tribal agencies. Specifically, NIBRS captures information about criminal incidents, including offenses; types and amount of property lost; demographic information about victims, offenders, and persons arrested; as well as the type of weapon, if any, used in the incident.

⁹⁷A small number of cases had high-level categorizations in the fields that tracked offenses for which remedies were pursued.

There were also fields that some DCIOs collected, while others did not. For example, DCIS has a structured field for estimated dollar loss to the federal government, reflecting the total financial amount lost due to fraud involved in a particular case. The MCIOs do not have this field.⁹⁸ In addition, DCIS and USACID collect structured data on suspect type, specifying if a suspect is an individual or business, while NCIS does not.⁹⁹ Where DCIOs do not have these fields, we are not able to report on this information.

Consistency in the type and organization of data collected would facilitate DOD's efforts to evaluate existing fraud risks across DOD and take corresponding actions to improve fraud risk management.

- **The use of narrative fields by MCIOs to capture data.** Officials from some MCIOs told us that narrative, as well as structured, data were necessary to understand the facts and circumstances of a case.¹⁰⁰ Additionally, MCIO officials described instances where narrative fields were used to capture data for which structured fields existed. In some instances, MCIO officials noted that the narrative fields might contain more accurate or timely data than structured fields. For example, we identified some NCIS cases for which there was additional information on sanctions in the narrative fields, rather than the applicable structured fields. The results of our analysis of structured data may, therefore, be understated, as previously noted. Increased and consistent usage of structured fields to capture data would allow DOD to more readily perform data analytics as part of its fraud risk management activities.

DOD encountered similar data challenges to those we identified when responding to a requirement in the National Defense Authorization Act for Fiscal Year 2018 on procurement fraud, which contributed to a delay in

⁹⁸NCIS officials stated that information on estimated dollar loss to the federal government is documented in reports in NCIS investigative files and not in a structured data field.

⁹⁹According to AFOSI officials and documentation, the AFOSI case management system has a field collecting the type of suspect, such as individual or organization, among others. However, the data that we reviewed did not have this information.

¹⁰⁰Specifically, according to MCIO officials, MCIOs have narrative fields intended to capture information from investigation reports, which are documents completed by investigators that contain key details about a case. According to DCIS officials, DCIS does not have a narrative field that collects information from these reports. NCIS officials stated that these reports capture some information that cannot be captured by structured fields.

DOD providing the report to Congress.¹⁰¹ Specifically, DOD advised Congress in an April 2018 letter that the final report would be delayed because the department had no central repository for the data it was required to report and that information would be obtained from a manual data call from the military departments, DOD Office of General Counsel, the defense agencies, and the Department of Justice. Data were then to be analyzed by the department and the DOD OIG. The final report was provided by DOD to Congress in December 2018, about 6 months after it was to be provided. Additional information on this and other similar reports by DOD to Congress are in appendix III.

Through our analyses we demonstrated that the DCIOs collect data that could help inform DOD's procurement-fraud risk management activities. However, investigative case data that are incomplete and difficult to analyze represent missed opportunities to provide DOD with information that would help DOD better understand and mitigate the fraud risks it faces. While overseeing fraud risk management is the responsibility of DOD's dedicated entities and implemented by program managers, as discussed in the Fraud Risk Framework, stakeholders, including law enforcement, have a role. This includes sharing information on fraud risks and schemes.

For that investigative information to be useful to DOD, it must be quality information. According to *Standards for Internal Control in the Federal Government*, managers use quality information to achieve the entity's objectives. Quality information is, among other things, complete and accessible. Management uses quality information to make informed decisions and evaluate the entity's performance in achieving key objectives and addressing risks. Therefore, the DCIOs have opportunities to improve the quality of their investigative information to support DOD fraud risk management efforts.

¹⁰¹National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Div. A, § 889, 131 Stat. 1283, 1508 (2017).

Council of the Inspectors General on Integrity and Efficiency's (CIGIE) Quality Standards for Investigations – Managing Investigative Information

CIGIE's fourth qualitative standard for investigations is that investigative data must be stored in a manner that allows effective retrieval, reference, and analysis, while ensuring the protection of sensitive data. It goes on to state that one of the hallmarks of an efficient organization is its ability to retrieve information that it has collected. It also notes that an effective information management system creates and enhances institutional memory. This, in turn, enhances the entire organization's ability to conduct pattern and trend analyses and to fulfill the mandate of detection and prevention.

Source: GAO review of CIGIE Quality Standards for Investigations dated November 15, 2011. | GAO-24-105358

Further, investigative quality standards and the DCIO's own policies point to the need for accurate and complete investigative case data not only to support investigative efforts but also to advise DOD and Congress. For example, a DCIS policy manual notes that the Case Reporting and Information Management System (CRIMS) is the principal reporting system for timely reporting of DOD investigative activities and helps the DOD OIG achieve its mission to support the warfighter; promote accountability, integrity, and efficiency; and advise the Secretary of Defense and Congress. The manual goes on to note that CRIMS facilitates compliance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) Quality Standards for Investigations. For more information about these standards, see the sidebar.

Further, an NCIS policy manual states that investigative data support the NCIS analysis program; provide input into semiannual reporting required under the Inspector General Act of 1978, as amended; and help meet other reporting requirements levied by the Department of Defense and Department of the Navy. Regarding USACID, an Army regulation notes that the Army Law Enforcement Reporting and Tracking System (ALERTS) provides the chain of command with timely information to respond to queries from the Department of Defense, the news media, and others. Therefore, timely and accurate reporting of information in ALERTS is critical.

DOD Does Not Have Plans to Obtain and Analyze Relevant Investigative Information and Has Coordinated to Some Extent with DCIOs to Share Information

While our analyses demonstrated how, even with current limitations, DCIO investigative data could help inform DOD's management of procurement fraud risks, DOD does not have plans to obtain and analyze the relevant information regarding DCIOs' investigations to inform its fraud risk management activities. Specifically, DOD's 2023 antifraud

strategy does not mention plans for obtaining and analyzing information from DCIOs regarding investigations of alleged and adjudicated procurement fraud.¹⁰²

The antifraud strategy identifies DCIS, but not the other DCIOs, as a source of information to inform fraud risk management efforts. Specifically, the strategy states that DCIS maintains regular communication with the Comptroller, ODA&M, and Principal Staff Assistants regarding existing and potential fraud cases and emerging trends to help improve fraud risk assessments, prevention, detection, and mitigation across the department. As stated above, according to DOD OIG, although the draft strategy was informally reviewed within the DOD OIG, the Comptroller/Chief Financial Officer did not formally coordinate the strategy with the DOD OIG in accordance with established DOD coordination processes. Further, according to DOD OIG, an issuance that requires specific actions from the DOD OIG requires formal coordination and approval from the Inspector General or Principal Deputy Inspector General, which did not occur. DCIS officials told us that DOD OIG does not participate in the management of DOD programs or operations but has shared information with DOD on a variety of topics, including fraud trends and how to report fraud.¹⁰³ DCIS officials also said they provide case outcomes for specific cases to program officials, when appropriate, and clarified that DCIS does not share information on ongoing, existing, or closed investigative cases that have not been made public by the U.S. courts. However, information from investigative data that DCIS and the other DCIOs possess is not mentioned in the strategy.

When we asked Comptroller officials if they had considered obtaining information from the DCIOs, they told us that they were collaborating with DCIOs and provided some examples of this coordination. For example, they described a DCIS presentation at a Fraud Reduction Task Force office hours session and coordination with DCIOs and the Procurement Fraud Working Group to identify fraud and ensure reporting completeness to close a DOD OIG recommendation related to Payment Integrity

¹⁰²For the purposes of this objective, “data” refers to specific data elements, while “information” refers more broadly to what could be gleaned from the data and used for fraud risk management purposes.

¹⁰³ DCIS officials also noted that the DOD OIG is an independent entity; thus, DCIS is not required to share information with DOD.

Information Act reporting requirements for confirmed fraud.¹⁰⁴ While examples of coordination, these are not examples of information sharing on data sources to develop data analytics for procurement fraud.

Comptroller officials also told us that they are in the process of identifying appropriate data sources to develop data analytics for procurement fraud. Officials indicated that they are considering several data sources, including the

- Federal Procurement Data System, the federal government’s procurement database;
- Electronic Document Access – Defense Finance and Accounting Service, which contains information on contracts, contract modifications, and contract deficiency reports, among other information; and
- Wide Area Workflow, a system for electronic invoicing, receipt, and acceptance.

However, these officials did not include information from DCIO case management data among the potential sources mentioned.

Coordination between the DOD OIG, OIG components, MCIOs, and DOD is called for by law and fraud risk leading practices. The Inspector General Act of 1978, as amended, requires the Inspector General of DOD, to whom DCIS reports, to be the principal adviser to the Secretary of Defense for matters relating to the prevention and detection of fraud, waste, and abuse in the programs and operations of DOD.¹⁰⁵ Further, a leading practice of the Fraud Risk Framework calls for agencies to establish collaborative relationships with stakeholders. Specifically, it notes that managers who effectively manage fraud risks collaborate and communicate with the OIG, if the agency has one, to improve their understanding of fraud risks. The OIG may also share information for analyzing data for potential fraud.

¹⁰⁴In 2022, the Department of Defense’s OIG recommended that the Under Secretary of Defense - Comptroller/Chief Financial Officer develop and implement a process for accurately reporting confirmed fraud in the accompanying materials to the DOD Agency Financial Report. Department of Defense, Office of Inspector General, *Audit of the Department of Defense’s FY 2021 Compliance With Payment Integrity Information Act Requirements* (June 28, 2022).

¹⁰⁵Pub. L. No. 95-452, 92 Stat. 1101 (1978), codified as amended at 5 U.S.C. § 408(c)(1).

The Fraud Risk Framework also states that managers should establish collaborative relationships with other stakeholders, including law enforcement entities, which would include all four of the DCIOs, to share fraud-related information. Given the OIGs' and other law enforcement entities' role in investigating instances of potential fraud, frequent communication with the OIG can help managers to identify emerging fraud risks and proactively enhance preventive activities. In addition, effective collaboration and communication can help align efforts of key stakeholders to address potential fraud. Increased collaboration with the DCIOs, including obtaining and using information from their case management data, could, therefore, help improve DOD's fraud risk management efforts.

We recognize that there are sensitivities around sharing investigative case management data. For example, protecting law enforcement sensitive data that is housed in investigative case management systems is a key consideration. Further, maintaining the independence of investigative and oversight organizations is important. However, these concerns do not preclude investigative information-sharing opportunities between DOD and the DCIOs.

Our analysis illustrates the range of relevant information from alleged and adjudicated procurement fraud cases—such as information on fraud participants and adjudicated offenses—that, if used in data analytics, could help inform DOD's fraud risk management activities. Without obtaining this information from the DCIOs, DOD may not fully assess its fraud risks or design and implement data-analytics activities to prevent or detect these fraud risks.

Conclusions

DOD is the largest contracting agency in the federal government. The scope and scale of DOD's contracting activity—which includes contracts on major weapon systems, support for military bases, information technology, and consulting services—makes DOD procurement inherently susceptible to fraud. It also makes preventing, detecting, and mitigating procurement fraud paramount.

As we found in 2021, DOD has taken some steps consistent with leading practices to implement a fraud risk management program by, for example, providing an initial strategy document for combating fraud risks and creating a Fraud Reduction Task Force to prioritize fraud risks.

However, DOD has opportunities, particularly related to data analytics, to better identify and mitigate fraud risks. One such opportunity is revising its fraud risk management strategy, which was reissued in 2023, so that the strategy leverages data analytics to prevent and detect potential fraud. Data analytics are a significant tool for helping agencies transition from a costly “pay-and-chase”-focused fraud risk program to an approach that is more focused on fraud prevention.

DOD’s fraud risk management strategy refers to broad goals related to data analytics and includes high-level information on roles, responsibilities, and activities. However, it does not establish data analytics as one of the four different methods that are used together for preventing, detecting, and responding to fraud, consistent with leading practices in the Fraud Risk Framework. Additionally, the strategy does not document with specificity the direction needed in key areas to fully implement data analytics. It does not identify which, if any, entities have the necessary authority to ensure that the fraud-related data-analytics activities are carried out and does not clearly define or document roles and responsibilities or timelines related to data-analytics activities. Having a strategy that establishes data analytics as a method for fraud risk management and provides direction on authorities, roles, responsibilities, and timelines for data-analytics activities will better position DOD to employ data analytics to help manage fraud risks.

As demonstrated by our analyses, DOD investigative data can be used to generate information that is useful for fraud risk management purposes. For example, data on adjudicated offenses can provide DOD visibility on the extent of fraud detected, characteristics of fraud schemes, and types and possible emerging trends of fraud risks faced by DOD. However, we also identified limitations in the DCIOs’ data for the purposes of fraud-related data analytics. Specifically, DOD investigative data were not always complete and could not always be readily analyzed, potentially making the data less useful for fraud risk management purposes. Furthermore, the extent to which information about cases is collected in narrative fields means that advanced analytics or manual review is needed to access the information—the latter of which, manual review, can be a time- and resource-intensive process. Ensuring that DCIOs achieve greater consistency in the type and organization of data collected could yield improvements that would facilitate DOD’s efforts to assess existing fraud risks across DOD. Additionally, ensuring that DCIOs make DOD investigative data complete, accessible, and readily subject to analysis and aggregation would improve the usability of those data for fraud risk management purposes.

Despite the potential for using DOD investigative data to inform fraud risk management and having used the data in the past to provide Congress with information on procurement fraud, DOD's antifraud strategy does not include plans for obtaining and analyzing the information that can be gleaned from such data. While there are sensitivities that would need to be considered and mitigated in sharing investigative case management data, these concerns do not preclude all information-sharing opportunities. Given DCIOs' role in investigating instances of potential fraud, information from DCIOs can help DOD identify emerging fraud risks and proactively enhance preventive activities and can help align efforts of key stakeholders to address potential fraud. Additionally, the DCIOs' collaboration with each other and with relevant stakeholders will be helpful in developing leading practices towards improving the usability of their respective procurement fraud investigative data for fraud risk management purposes. Until DOD obtains information from the DCIOs on relevant adjudicated procurement fraud cases, DOD's ability to conduct fraud-related data analytics to inform its risk management efforts will be limited.

Recommendations for Executive Action

We are making 11 recommendations to DOD:

The Secretary of Defense should ensure that the Under Secretary of Defense (Comptroller) revises DOD's Fraud Risk Management Strategy to establish data analytics as a method for preventing, detecting, and responding to fraud. (Recommendation 1)

The Secretary of Defense should ensure that the Under Secretary of Defense (Comptroller) identifies and documents in DOD's Fraud Risk Management Strategy which entity has the necessary authority to ensure that fraud-related data-analytics activities are planned and implemented. (Recommendation 2)

The Secretary of Defense should ensure that the Under Secretary of Defense (Comptroller) revises DOD's Fraud Risk Management Strategy to clarify and document roles and responsibilities related to data-analytics activities. (Recommendation 3)

The Secretary of Defense should ensure that the Under Secretary of Defense (Comptroller) incorporates and documents timelines for

designing and implementing data-analytics activities into DOD's Fraud Risk Management Strategy. (Recommendation 4)

The Inspector General of DOD should improve the usability of its procurement fraud investigative data for fraud risk management purposes. Specific actions should include ensuring that data in structured fields are complete, accessible, and readily subject to analysis and aggregation. (Recommendation 5)

The Secretary of the Air Force, in collaboration with the Inspector General of DOD and the other military departments, should improve the usability of its respective procurement fraud investigative data by DOD for fraud risk management purposes. Specific actions should include ensuring that data in structured fields are complete, accessible, and readily subject to analysis and aggregation. (Recommendation 6)

The Secretary of the Army, in collaboration with the Inspector General of DOD and the other military departments, should improve the usability of its respective procurement fraud investigative data by DOD for fraud risk management purposes. Specific actions should include ensuring that data in structured fields are complete, accessible, and readily subject to analysis and aggregation. (Recommendation 7)

The Secretary of the Navy, in collaboration with the Inspector General of DOD and the other military departments, should improve the usability of its respective procurement fraud investigative data by DOD for fraud risk management purposes. Specific actions should include ensuring that data in structured fields are complete, accessible, and readily subject to analysis and aggregation. (Recommendation 8)

The Comptroller should collaborate with the Inspector General of DOD and the Secretaries of the Navy, Air Force, and Army, respectively, to obtain and analyze relevant information from adjudicated procurement fraud cases. (Recommendation 9)

The Secretary of Defense should ensure that the Under Secretary of Defense (Comptroller) revises DOD's Fraud Risk Management Strategy to obtain and analyze relevant information from adjudicated procurement fraud cases from the Defense Criminal Investigative Organizations. (Recommendation 10)

The Inspector General of DOD should collaborate, as appropriate, with the military departments and relevant stakeholders, on the development

of leading practices towards improving the usability of their respective procurement fraud investigative data by DOD for fraud risk management purposes. (Recommendation 11)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD and DOD OIG for review and comment. We received written comments from DOD and DOD OIG, reproduced in appendix IV and appendix V, respectively, and summarized below. DOD and DOD OIG also provided technical comments that we incorporated as appropriate.

In its written comments, DOD concurred with our seventh, ninth, and tenth recommendations. However, DOD did not concur with our first, second, third, fourth, and eighth recommendations and partially concurred with our sixth recommendation. In considering DOD's comments, we continue to believe that all the recommendations directed to DOD are warranted and that they should be implemented in their entirety and in an expeditious manner. DOD OIG concurred with our fifth, sixth, seventh, eighth, ninth, and eleventh recommendations.

DOD did not concur with our first recommendation that the Under Secretary of Defense (Comptroller) revise DOD's Fraud Risk Management Strategy to establish data analytics as a distinct method for preventing, detecting, and responding to fraud. In its comments, DOD stated that it has already accomplished the work reflected in the recommendation. In doing so, DOD pointed to examples in the strategy where data analytics are referenced. Specifically, DOD identified the following in the strategy:

- a statement that the Payment Integrity Information Act of 2019 (PIIA) requires and encourages agencies to use data analytics, and that DOD is subject to these requirements;¹⁰⁶

¹⁰⁶PIIA contains requirements for managing improper payments and fraud. PIIA's requirements related to fraud generally involve implementing control activities to prevent, detect, and respond to fraud. PIIA requires the Office of Management and Budget to maintain guidelines for agencies to establish financial and administrative controls to identify and assess fraud risks and that incorporate leading practices detailed in our Fraud Risk Framework. Pub. L. No. 116-117, 134 Stat. 113 (2020) (codified at 31 U.S.C. §§ 3351-58).

- a statement that components should develop fraud analytics and should produce actionable results from analytics; and
- a statement in an appendix listing examples of fraud control activities that includes data mining and matching techniques.

We agree that the strategy makes references to data analytics, as acknowledged in the draft report. Such references may express DOD's commitment to using data analytics. However, these general references to data analytics are made without an accompanying discussion regarding DOD's specific plans for such activities. Without discussing with specificity what data analytics are to be used and how they are to be used, the strategy does not effectively establish data analytics as a distinct method for preventing, detecting, and responding to fraud. For example, the strategy does not discuss, with specificity, the design and implementation of various data analytics techniques, the combining of data across programs to facilitate analytics, or the pursuit of access to necessary external data. A discussion of how these leading practices for data analytics activities from the Fraud Risk Framework are to be developed and implemented across DOD would help inform decisions regarding what data analytics are used and how they are to be used. Similarly, although data-analytics techniques, such as data matching, are mentioned in the strategy's appendix, there is no accompanying discussion of DOD's plans to use these techniques.

DOD also stated in its comments that it is employing tools such as an improper payment detection tool and fraud-related dashboards. However, the strategy, as currently written, does not specifically document the use of these tools in a way that establishes data analytics as a method for preventing, detecting, and responding to fraud. Our report describes DOD's fraud-related dashboards and their inclusion in the strategy. Conversely, we did not discuss the improper payment detection tool as the strategy does not reference this tool. Furthermore, in its comments, DOD stated that the fraud-related dashboards display aggregated fraud risks and fraud risk control assessments submitted through the Statement of Assurance program. Although these dashboards may inform DOD's fraud risk management, they are not data-analytics techniques—for example, data mining to analyze transaction-level data—as contemplated by the Fraud Risk Framework's leading practices regarding data analytics.

DOD's comments on the first recommendation also note two recent Secretary of Defense memoranda that stress the importance of implementing enterprise risk management and strengthening the internal

control environment. While these statements may help set the tone at the top, they do not establish data analytics as a method for preventing, detecting, and responding to fraud. Further, as discussed in this report, the Fraud Risk Framework acknowledges that fraud risk management activities may be incorporated into an agency's existing enterprise risk management efforts in a complementary fashion. This does not eliminate the separate and independent fraud risk management requirements.

We continue to believe that our first recommendation is warranted, especially given DOD's long-standing challenges with financial management and approach to business transformation. Moreover, DOD OIG's fiscal year 2024 report noting accelerating DOD's transformation to a data-centric organization as a top DOD management challenge, underscores the importance of this recommendation. In this regard, in its report, the OIG, among other things, noted that the department does not consistently regard data as a strategic asset and prioritize its management throughout DOD.¹⁰⁷

DOD did not concur with our second recommendation that the Under Secretary of Defense (Comptroller) identify and document in DOD's Fraud Risk Management Strategy which entity has the necessary authority to ensure that fraud-related data-analytics activities are planned and implemented. In its comments, DOD stated that the strategy already identifies the entity responsible for planning and implementing fraud-related data-analytics activities. Specifically, DOD commented that the strategy identifies the Comptroller/EFT as the entity for leading data analytics efforts, and the task force as the entity leading the analytics activities for high-priority risks. However, as discussed in the draft report, having responsibility for leading activities is not the same as having the necessary authority to ensure those activities are carried out.

Furthermore, although the strategy indicates that the Comptroller and the ODA&M Performance Improvement Officer have joint authority to provide guidance related to the annual Statement of Assurance, an enterprise risk management effort, the strategy does not include a statement regarding the authority specifically over fraud risk management activities. As discussed in this report, a statement in the strategy regarding the authorities associated with the annual Statement of Assurance does not eliminate the need to identify the authorities associated with implementing

¹⁰⁷Department of Defense, Office of Inspector General, Fiscal Year 2024 Top DOD Management and Performance Challenges, (Alexandria, Virginia: November 13, 2023).

the fraud risk management strategy. We believe our second recommendation remains valid. Identifying in the strategy which entity has the authority to ensure that the fraud-related data-analytics activities are planned and implemented is aligned with the *who* element of an antifraud strategy, as described in the Fraud Risk Framework, and will make DOD's strategy more comprehensive and effective.

DOD did not concur with our third recommendation that the Under Secretary of Defense (Comptroller) revise DOD's Fraud Risk Management Strategy to clarify and document roles and responsibilities related to data-analytics activities. In its comments, DOD reiterated the strategy's statements regarding various entities and their roles and responsibilities. As discussed in this report, although the strategy does discuss some of the roles and responsibilities for certain entities, the strategy does not establish clear roles and responsibilities for all entities with data-analytics roles.

In its comments, DOD points to the strategy's statement that the task force is responsible for leading DOD's data-analytic activities for high-priority risks, and to a sentence in the strategy stating that components should develop fraud analytics. However, as discussed in the report, the strategy does not make clear what responsibilities are involved in developing such analytics and whether developing analytics also includes conducting analytics. Further, the strategy does not identify, and Comptroller officials did not clarify, who is responsible for conducting data analytics and whether the task force has a role in doing so. Likewise, although the strategy references piloting analytics models, it does not clarify who will conduct analytics pilots, and it does not provide additional direction regarding this activity. Furthermore, the Procurement Fraud Working Group is not mentioned in the strategy as having a role, although DOD officials, in multiple interviews with us, described this group as having a collaborative role in data analytics.

As described in the Fraud Risk Framework, establishing roles and responsibilities of those involved in the fraud risk management activities is one of the key elements of an antifraud strategy. In its comments, DOD also noted the strategy's statement that DOD is subject to PIIA and that there are associated requirements for agencies to use data analytics to identify, prevent, and respond to fraud. However, this statement does not provide additional clarity regarding roles and responsibilities related to data analytics. Moreover, being subject to PIIA requirements does not mean that DOD will take the necessary action to implement those requirements. For example, despite DOD's efforts over the past several

decades to comply with legal requirements to improve its financial management and auditability, DOD remains the only major federal agency that has never been able to receive a clean audit opinion on its consolidated financial statements.¹⁰⁸ As a result, we believe DOD still needs to revise its strategy to clarify and document roles and responsibilities related to data-analytics activities.

DOD did not concur with our fourth recommendation that the Under Secretary of Defense (Comptroller) incorporate and document timelines for designing and implementing data-analytics activities into DOD's Fraud Risk Management Strategy. In its comments, DOD stated that the timelines are already included in the strategy. We disagree. The comments refer to a figure in the strategy as an example. However, this figure provides an annual timeline for fraud risk management activities in general. This figure does not provide a timeline for data analytics activities, such as timelines for designing and implementing analytics pilots or developing fraud analytics. The comments also refer to an appendix of the strategy listing fraud control activities. However, these appear to be examples of activities and do not appear to reflect DOD's actual plans or timelines with respect to fraud-related data analytics activities.

Additionally, in its comments, DOD stated that the strategy includes a requirement of timelines in the list of fraud control activities. The comments also refer to language in the strategy indicating that management has created timelines for implementing fraud risk management activities. However, as discussed in this report, no actual timelines for designing and implementing data analytics activities appear in the strategy. The Fraud Risk Framework notes the importance of designing and implementing data-analytics control activities and creating timelines for implementing them. We continue to believe that this recommendation is warranted.

DOD partially concurred, and DOD OIG concurred, with our sixth recommendation that the Secretary of the Air Force, in collaboration with the Inspector General of DOD and the other military departments, should improve the usability of its respective procurement fraud investigative data by DOD for fraud risk management purposes. The recommendation states that specific actions should include ensuring that data in structured

¹⁰⁸GAO, DOD Financial Management: Additional Actions Needed to Achieve a Clean Audit Opinion on DOD's Financial Statements, [GAO-23-105784](#) (Washington, D.C.: May 15, 2023).

fields are complete, accessible, and readily subject to analysis and aggregation. The Secretary of the Air Force, Inspector General, commented that not all data in structured fields should be required to be completed and that not all fields are relevant to every case or case type.

We agree that not all fields may be relevant for every case. However, based on our analyses, we believe completing a structured field to indicate its irrelevancy with respect to a certain data point would provide additional insight and improve usability for fraud risk management purposes. The Secretary of the Air Force, Inspector General, concurred that key fields for procurement fraud investigations should be required to be completed. Additionally, the Secretary of the Air Force, Inspector General, commented that AFOSI is moving to a new case management system, currently in its roll-out phase, which will address many of the issues raised in our report.

The Secretary of the Air Force, Inspector General, also provided technical comments and raised concerns regarding how we characterized information and interpreted the data and commented that AFOSI was not able to validate the report findings. We have reviewed the technical comments and incorporated them, as appropriate, into our final report. As detailed in our objectives, scope, and methodology (see app. I), we believe that we have planned and performed the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. During this engagement, we coordinated extensively with AFOSI officials to discuss the case management data, and took steps, consistent with generally accepted government auditing standards, to ensure that our reporting is accurate.

Our audit objective was not to perform an analysis that would be replicable by the DCIOs, including AFOSI. Rather, our objective was to provide insight into the types of analyses that could be performed to inform fraud risk management. As discussed in this report, our analyses demonstrate the usefulness of using investigative data to inform fraud risk management, despite limitations. These limitations made our analysis difficult, and, as we note in the report, limitations include incomplete data and lack of a shared identifier across DCIOs. We acknowledge in the report that our assessment may be incomplete, for example, where we did not capture all adjudicated offenses. Variations in the interpretation of the data do not negate the validity of our recommendation that the usability of procurement fraud investigative data by DOD for fraud risk management purposes should be improved. In fact, these challenges

support the importance of improving the usability of procurement fraud investigative data to support fraud risk management.

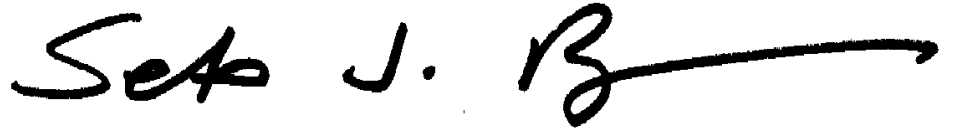
DOD did not concur, and DOD OIG concurred, with our eighth recommendation that the Secretary of the Navy, in collaboration with the Inspector General of DOD and the other military departments, should improve the usability of its respective procurement fraud investigative data by DOD for fraud risk management purposes. As discussed in this report, our analyses demonstrate the usefulness of using investigative data to inform fraud risk management, despite limitations. These limitations make analysis difficult, and, as we note in the report, limitations include incomplete data and lack of a shared identifier across DCIOs. In its comments, NCIS raised concerns with GAO's interpretation of the data but agreed that there are limitations with its case management system regarding data collection and aggregation.

We have addressed NCIS's technical comments, as appropriate, in this report. As detailed in our objectives, scope, and methodology (see app. I), we believe that we have planned and performed the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. During this engagement, we coordinated extensively with NCIS officials to discuss the case management data, and took steps, consistent with generally accepted government auditing standards, to ensure that our reporting is accurate. As mentioned in response to AFOSI comments, our audit objective was not to perform an analysis that would be replicable by the DCIOs. Rather, our objective was to provide insight into the types of analyses that could be performed to inform fraud risk management.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, DOD Inspector General, 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 key contributions to this report are listed in appendix VI.

Letter

A handwritten signature in black ink that reads "Seto J. Bagdoyan". The signature is written in a cursive style, with the first name "Seto" being the most prominent. The last name "Bagdoyan" is written in a more compact, cursive script. A long horizontal stroke extends from the end of the signature to the right.

Seto J. Bagdoyan
Director, Forensic Audits and Investigative Service

Appendix I: Objectives, Scope, and Methodology

This report assesses (1) if the Department of Defense’s (DOD) fraud risk management strategy provides the needed direction for fraud-related data-analytics activities and (2) the extent to which analyses of DOD investigative data on alleged and adjudicated procurement fraud cases can help inform fraud risk management.¹

To assess if DOD’s fraud risk management strategy provides direction for fraud-related data-analytics activities, we analyzed DOD’s fiscal year 2023 strategy and related guidance documents—including DOD’s fiscal year 2020 fraud risk management strategy, a pertinent DOD directive, and DOD instruction. We also reviewed relevant documentation regarding the data-analytics pilots and interviewed officials from the Offices of the Under Secretary of Defense— Comptroller and the Office of the Director of Administration and Management to discuss their roles in fraud risk management, specifically with regard to data analytics and the use of Advancing Analytics (Advana), an enterprise-wide data repository.

We assessed the extent to which DOD fraud risk management strategy aligns with relevant leading practices in the third component of the Fraud Risk Framework.² Specifically, leading practices to

- determine the risk responses and document an antifraud strategy based on the fraud risk profile—including establishing roles and responsibilities of those involved in fraud risk management activities; and
- design and implement specific contract activities—including data-analytics activities—to prevent and detect fraud.

We also assessed the extent to which DOD’s fraud risk management strategy aligns with principles in the *Standards for Internal Control in the*

¹We refer to the population of cases in our analysis as “alleged and adjudicated procurement fraud cases” because, while all involved alleged procurement fraud, they did not all result in adjudicated fraud. However, we found that some of the cases did result in adjudicated fraud.

²GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015).

Federal Government, specifically the principle related to establishing an organizational structure to achieve an entity's objectives.³

We assessed DOD's fraud risk management strategy by analyzing these DOD documents and DOD officials' responses to our questions against the above criteria from the Fraud Risk Framework and *Standards for Internal Control in the Federal Government*.

To determine the extent to which analyses of DOD investigative data on alleged and adjudicated procurement fraud cases can help inform fraud risk management, we analyzed investigative case management data, interviewed officials, and reviewed relevant documents from DOD's Defense Criminal Investigative Organizations (DCIO). The DCIOs are

- the Department of Defense Office of Inspector General's Defense Criminal Investigative Service (DCIS);
- the Air Force Office of Special Investigations (AFOSI);
- the Naval Criminal Investigative Service (NCIS); and
- the Army Criminal Investigation Division (USACID).

Specifically, we requested records for unsealed, unclassified, cases closed from fiscal years 2015 through 2021 from the DCIOs. DCIS and AFOSI provided data for all cases we requested, while the remaining two DCIOs provided data for a narrower population of cases. Specifically, NCIS provided data for criminal cases that NCIS determined were related to alleged or adjudicated procurement fraud, and USACID provided data for cases opened and closed from fiscal years 2015 through 2021.⁴ The variation in the populations of case data provided may limit comparability between DCIOs in some instances. In addition, the case data provided by DCIOs may overlap, where DCIOs conducted joint investigations.

We took steps where possible to restrict our analysis to full investigations where DCIOs had lead or joint roles. For example, for the purposes of our

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

⁴NCIS officials used a case category field in the NCIS case management system, populated by investigators at the onset of a case, to identify cases related to alleged or adjudicated procurement fraud. According to NCIS officials, these categories are generally selected based on the most pressing aspect of a case. It is possible for the focus of the case to change over time; officials stated that when this occurs, investigators should, but might not always, change the category. It is also possible that cases involving alleged or adjudicated procurement fraud were not labeled as such in the case category field.

analysis, we excluded any cases with no identified suspects.⁵ Where possible, we also excluded any cases labeled as limited assistance investigations or inquiries, rather than full investigations.⁶

We reviewed relevant documentation, interviewed knowledgeable agency officials, and performed electronic testing of specific data elements in DCIO data to assess the reliability of the data, including the extent to which they were complete and could be readily analyzed. We reviewed DCIOs' data collection practices related to the usability of investigative data for fraud risk management purposes and DOD's practices related to its plans to obtain and analyze certain relevant information from DCIOs.

We found that the data were reliable for the purposes of our reporting objectives, which included reporting on key areas we identified where the data were incomplete or could not be readily analyzed. For example, we found that some types of data, such as data on offenses and case outcomes, may be incomplete. However, we also found that even where incomplete, the data can provide important insights to DOD for fraud risk management purposes.

We performed analyses in the categories discussed below, which we selected because they can provide insight into fraud risks faced by DOD and the results of DOD's fraud risk management activities. Our analysis steps varied, depending on each DCIO's available data, their completeness, and the extent to which the data could be readily analyzed.

We generally report the results of our analyses at the case or suspect level, rather than at the record level. For example, a single case may involve multiple records reflecting multiple suspects, investigated offenses, or case outcomes. Except where otherwise noted, we report on the number of cases or suspects with applicable records, rather than the number of records.

- **Number and type of cases investigated.** For all DCIOs aside from NCIS—which provided data for cases officials had identified as being

⁵Suspects may not always be identified throughout the course of an investigation. According to some DCIO officials, cases must have known suspects to be considered full investigations.

⁶ DCIS officials stated that they generally provided data on only full investigations that DCIS led or jointly led but, due to data limitations, a few limited assistance investigations or inquiries may exist in the data.

related to alleged or adjudicated procurement fraud—we took steps to identify cases related to alleged or adjudicated procurement fraud.⁷

- For DCIS, we used a case category field in the DCIS case management system, populated by investigators at the onset of a case, to identify relevant cases.⁸
- The AFOSI and USACID case management data do not contain structured fields that would allow for classification of cases as related to alleged or adjudicated procurement fraud.⁹ We, therefore, used information in case narrative fields to identify relevant cases. We analyzed the DCIOs' narrative fields using keyword searches and a natural language processing model that was used to classify text. Specifically, we applied a natural language processing model, which we trained to identify cases that are relevant to alleged or adjudicated procurement fraud. We found that the results of the natural language processing model were more accurate in identifying alleged or adjudicated procurement fraud cases than using keyword searches alone.¹⁰ We took additional steps to manually review and exclude cases we identified as related to other types of fraud, such as health care fraud, rather than alleged or adjudicated procurement fraud. See figure 14.

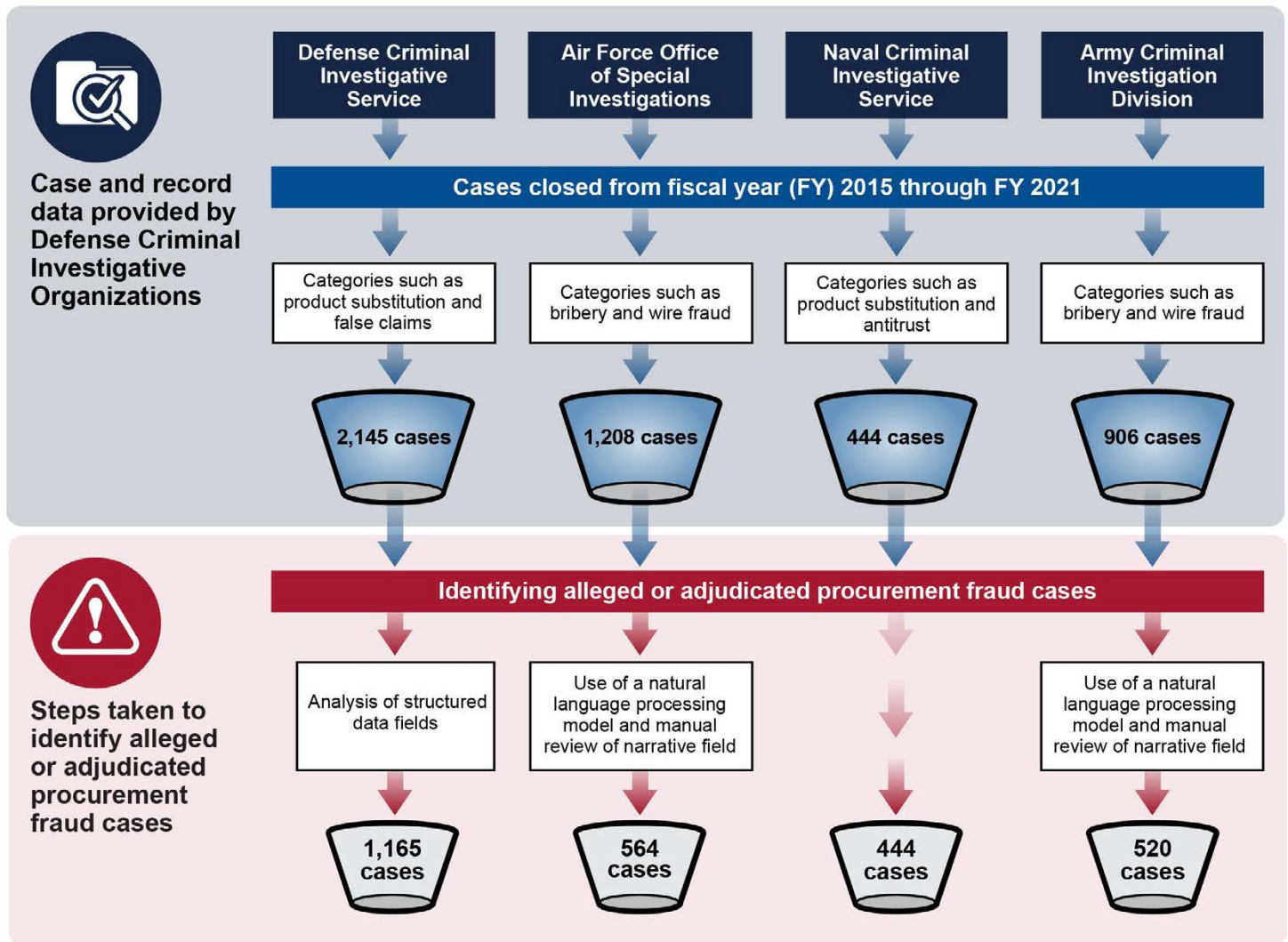
⁷As stated previously, the case data provided by DCIOs may overlap, where DCIOs conducted joint investigations. However, there is no shared identifier that allows for the determination of the total number of unique cases across DCIOs without leveraging additional data sources.

⁸According to DCIS officials, as with the NCIS case category field, this field is generally selected based on an investigator's assessment of the most pressing aspect of a case and should, but may not always, be updated, if the focus of the case changes.

⁹Investigators at the MCIOs enter data into case management systems using a combination of structured and narrative data fields. Investigators at DCIS enter data into their case management system using structured fields. The structured fields are intended for certain discrete pieces of data, such as suspect name or sentence type, and may restrict the types of characters that can be entered, or rely on drop-down menus to prescribe the types of data that can be recorded. The narrative fields are open-ended fields that allow investigators to describe the investigation more broadly, based on available information. The completeness of the structured and narrative fields varies based on a range of factors, including the specific DCIO's case management system and policies for data entry. We focused our analysis on the DCIOs' structured fields.

¹⁰Specifically, in a testing sample of 72 cases, the estimated error rate for the model was 0.03, with a 95 percent confidence interval of [0.0-0.07]. The estimated error rate for the keyword searches was 0.26, with a 95 percent confidence interval of [0.17-0.38].

Figure 14: Steps Taken to Identify Cases of Alleged or Adjudicated Procurement Fraud



Sources: GAO analysis of Department of Defense data; stas111/stock.adobe.com (icons). | GAO-24-105358

Accessible Data for Figure 14: Steps Taken to Identify Cases of Alleged or Adjudicated Procurement Fraud

Case and record data provided by Defense Criminal Investigative Organizations

- Cases closed from fiscal year (FY) 2015 through FY 2021
 - Defense Criminal Investigative Service
 - Categories such as product substitution and false claims
 - 2,145 cases
 - Air Force Office of Special Investigations
 - Categories such as bribery and wire fraud
 - 1,208 cases
 - Naval Criminal Investigative Service
 - Categories such as product substitution and antitrust
 - 444 cases
 - Army Criminal Investigation Division
 - Categories such as bribery and wire fraud
 - 906 cases

Identifying alleged or adjudicated procurement fraud cases

- Steps taken to identify alleged or adjudicated procurement fraud cases
 - Defense Criminal Investigative Service
 - Analysis of structured data field
 - 1,165 cases
 - Air Force Office of Special Investigations
 - Use of natural language processing model and manual review of narrative field
 - 564 cases
 - Naval Criminal Investigative Service
 - 444 cases
 - Army Criminal Investigation Command
 - Use of natural language processing model and manual review of narrative field
 - 520 cases

Sources: GAO analysis of Department of Defense data; stas111/stock.adobe.com (icons). | GAO-24-105358

Notes: The Naval Criminal Investigative Service provided data for criminal cases related to alleged or adjudicated procurement fraud according to a case category field completed by investigators. The Army Criminal Investigation Division provided data for cases opened and closed from fiscal year 2015 through fiscal year 2021. We took steps, where possible, to restrict our analysis to full investigations where Defense Criminal Investigative Organizations (DCIO) had lead or joint roles. For example, we excluded any cases with no identified suspects, as well as limited assistance inquiries. The total counts of cases that we present in this figure take into account those analysis steps. The case data provided by DCIOs may overlap, where DCIOs conducted joint investigations.

- **Number and type of suspects.** For each DCIO, we took steps to identify the number and type of known suspects involved with the alleged or adjudicated procurement fraud cases. Specifically, we used suspect identifiers, such as suspect name and Social Security number, where available, to calculate the range in the number of

known suspects involved with a case for each DCIO.¹¹ We also used the suspect identifiers to calculate the extent to which cases with one known suspect, as compared with cases with multiple known suspects, involved offenses adjudicated as fraud.¹² For DCIS, we performed additional analysis of suspect type, such as the extent to which known suspects were individuals or businesses, and suspects' relationship to the government, such as the extent to which known suspects were contractors or subcontractors. The other DCIOs did not have these data.

- **Number and types of investigated offenses and offenses for which remedies were pursued.** For each DCIO, we took steps to identify the number and types of known investigated offenses and known offenses for which remedies were pursued that were involved with the alleged or adjudicated procurement fraud cases. Specifically, we used data collected by each DCIO on offenses to calculate the number of cases and known suspects with known investigated offenses and offenses for which remedies were pursued. We also identified the most prevalent types of investigated offenses, and offenses for which remedies were pursued, based on the numbers of unique cases listing these offense types.

The offense data we used for these analyses may be incomplete. We found that the data that investigators enter in the DCIOs' offense fields can vary due to factors such as

- the structure of the DCIO's case management system, including whether data are entered manually or using drop-down menus;
- investigator discretion; and
- the information available at the time of data entry.

¹¹Our analysis did not account for possible misspellings or other errors in data entry that might inflate the count of unique suspect identifiers. We used suspect name to identify unique suspects for AFOSI and NCIS and a suspect identification number for USACID. We used a combination of suspect name and Social Security number to identify unique suspects for DCIS.

¹²We defined adjudicated offenses as offenses that were ultimately adjudicated through a judicial or other adjudicative system as fraud. We defined a case as involving an adjudicated offense if it involved at least one offense adjudicated as fraud. Our data likely do not include all adjudicative information. Cases with multiple known suspects might be more likely to involve adjudicated offenses, as per available data, because investigators may have made the decision to focus their time and resources on developing evidence and recording data for these cases.

DCIO officials acknowledged that offense data may be incomplete or outdated. We discuss these limitations in the report.

- **Number and types of adjudicated offenses.** For each DCIO, we took steps to identify the number and types of adjudicated offenses that were involved with alleged procurement fraud cases. We defined adjudicated offenses as offenses that were ultimately adjudicated as fraud through a judicial or other adjudicative system. However, not all of the adjudicated offenses in our analysis may have been related to procurement fraud, because while the cases in our analysis had an alleged procurement fraud focus, they also may have led to other types of adjudicated fraud.

We used data collected by each DCIO on offenses and adjudicative outcomes to calculate the number of cases and known suspects with known adjudicated offenses. We also identified the most prevalent types of adjudicated offenses based on the numbers of unique cases listing these offense types.

As with the data on investigated offenses and offenses for which remedies were pursued, the offense data we used for these analyses may be incomplete. For example, investigators may not always have insight into the results of trial or other judicial proceedings or record the results. In addition, we reviewed the data and consulted with DCIO officials to determine the best structured fields to use for this analysis. Nevertheless, our analysis may not have captured all cases involving adjudicated offenses, or all adjudicated offenses involved with a case, if these outcomes were not recorded in the fields we used for analysis.¹³

- **Other case outcomes.** For each DCIO, we took steps to identify data on other case outcomes, aside from adjudicated offenses, resulting from the alleged and adjudicated procurement fraud cases.

We examined available data on financial impacts of adjudicated procurement fraud cases. Specifically, for DCIS, we used a data field representing the estimated dollar loss to the federal government, as estimated by investigators at the onset of an investigation, to analyze the estimated financial amount lost due to fraud for cases we identified with at

¹³Some of the structured fields we used to determine which cases involved adjudicated procurement fraud were blank or unknown for most cases. Blank or unknown values could be expected where a case did not lead to an adjudicative outcome.

least one adjudicated offense.¹⁴ The other DCIOs did not have data fields illustrating the estimated dollar loss to the federal government.¹⁵

We examined data on sentences imposed for participants of adjudicated fraud. The data available for analysis varied by DCIO. However, for all DCIOs, we used available data to examine selected sentences, including the types and quantities of the sentences, for suspects we identified with at least one adjudicated offense.¹⁶

- We examined data on reasons for case clearance. The data available for analysis varied by DCIO. However, for all DCIOs, we used available data to examine the extent to which cases were cleared, such as due to prosecution declination, as well as available reasons for clearance, such as weak or insufficient evidence.

As with the offense data, the case outcome data we used for these analyses may be incomplete, including because investigators may not always have insight into this stage of the case or record the data, even when known.

- **Case duration.** For each DCIO, we took steps to calculate the range and average length of the alleged or adjudicated procurement fraud cases. On the basis of available data, we used case open and closed dates to perform these calculations. For NCIS, we also used a data field containing the date of NCIS's submission of a case for

¹⁴DCIS documentation specifies that this estimate is based on an investigator's subjective assessment of the facts surrounding a case, and the investigator does not need to obtain objective evidence to support the estimate. However, according to the documentation, the estimate should be reasonable and based on information documented in the case initiation or other investigative report, which, in some instances, must be reviewed by supervisors. The documentation also states that the estimate should be updated throughout the course of an investigation, if necessary, although officials told us that there is no process in place to update the estimates.

¹⁵NCIS officials stated that information on estimated dollar loss to the federal government is documented in reports in NCIS investigative files and not in a structured data field.

¹⁶We analyzed the total amounts of sanctions ordered for suspects in the NCIS data. We could not calculate the total amounts for specific types of sanctions because the data we received from NCIS did not distinguish between sanction types and amounts where suspects received multiple sanctions. However, the internal data available to NCIS officials does offer this distinction. Further, according to NCIS officials, it is possible that where multiple suspects within a case collectively owed an amount, the amount was duplicated for each suspect's records in the data we received. We took steps to exclude any duplicate sanction amounts within a case to prevent possible overcounting. However, it is, therefore, possible that we undercounted total sanction amounts, where multiple suspects within a case did receive the same, but separate, sanction amount.

administrative or judicial decision to calculate the average duration of NCIS's portion of an investigation.

While we identified incompleteness and other limitations in the case management data, we found that the data can, nevertheless, provide DOD officials with insight on characteristics of alleged and adjudicated fraud schemes and trends from the associated monitoring and detection activities.

We assessed the extent to which DOD's practices align with principles in the *Standards for Internal Control in the Federal Government*, specifically related to using quality information to achieve an entity's objectives.¹⁷ Additionally, we assessed the extent to which DOD's practices align with a relevant leading practice in the third component of the Fraud Risk Framework that agencies establish collaborative relationships with stakeholders, including collaborating and communicating with the OIG to improve its understanding of fraud risks.¹⁸

Illustrative Case Examples

We selected a nongeneralizable sample of eight case examples, two from each DCIO, to provide illustrative information regarding the life cycle of cases investigated. We requested and obtained case file documents, including administrative proceedings documentation from DCIOs and, as necessary, the cognizant suspension and debarment officials. We also reviewed publicly available court documents and information from the System for Award Management; and interviewed DCIO officials. The eight selected case examples are not generalizable to the remaining cases in the DCIO data sets.

We used the following criteria to select procurement fraud cases from the DCIO case management data sets:

- Cases that were investigated by each of the four DCIOs as either the lead, sole, or joint investigator.
- Cases that are closed and resulted in adverse findings or actions against the contractor.

¹⁷GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

¹⁸GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015).

- Cases illustrating a variety of the four remedies: contractual, civil, administrative, criminal as outlined in DOD Instruction 7050.05.¹⁹
- Cases illustrating a variety of offenses.

As secondary criteria, we also considered cases' geographical dispersion and availability of public information.

We selected an initial sample of 22 cases by identifying and reviewing information in variable fields that were relevant to the selection criteria within each of the DCIO data sets for cases involving alleged procurement fraud. In identifying the relevant variable fields, we relied on information gleaned from the DCIOs' case-management system documentation and interviews with knowledgeable officials.

After drawing the initial sample, we reviewed the cases to ensure that they were procurement fraud cases that met the criteria. We also considered the sampled cases' geographic dispersion and the presence or absence of publicly available information. For the initial sample of cases, we requested additional case documentation from the DCIOs, including, for example, the Records of Investigation. We also researched the availability of publicly available information from publicly available court documents included in the Public Access to Court Electronic Records system, and the System for Award Management.²⁰

After reviewing the case information available for each case of the initial sample, we selected two cases from each DCIO to use as illustrative case examples. The final selection of eight procurement fraud cases was based on a review of the same criteria noted above.

We conducted this performance audit from August 2021 to February 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that

¹⁹Department of Defense, Instruction 7050.05, *Coordination of Remedies for Fraud and Corruption Related to Procurement Activities* (May 12, 2014, incorporating change 1, effective July 7, 2020).

²⁰The General Services Administration's System for Award Management is the central registration point for businesses seeking contracts with the federal government. The System for Award Management also contains information on contractors that have been excluded from receiving federal contracts, such as due to suspensions and debarments.

**Appendix I: Objectives, Scope, and
Methodology**

the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Summary of Eight Selected Defense Criminal Investigative Organization Procurement Fraud Cases

The figures and tables below summarize the information we obtained through our review of eight procurement fraud cases that were closed by a Defense Criminal Investigative Organization (DCIO) between fiscal years 2015 and 2021. We reviewed Department of Defense (DOD) information regarding selected cases from each of the four DCIOs: Air Force Office of Special Investigations, U.S. Army Criminal Investigation Division, Defense Criminal Investigative Service, and Naval Criminal Investigative Service. We also reviewed publicly available court documents involving these cases. For each DCIO, we selected two cases to summarize in the figures and tables below. See appendix I for additional details on the methodology that we used to select the cases.

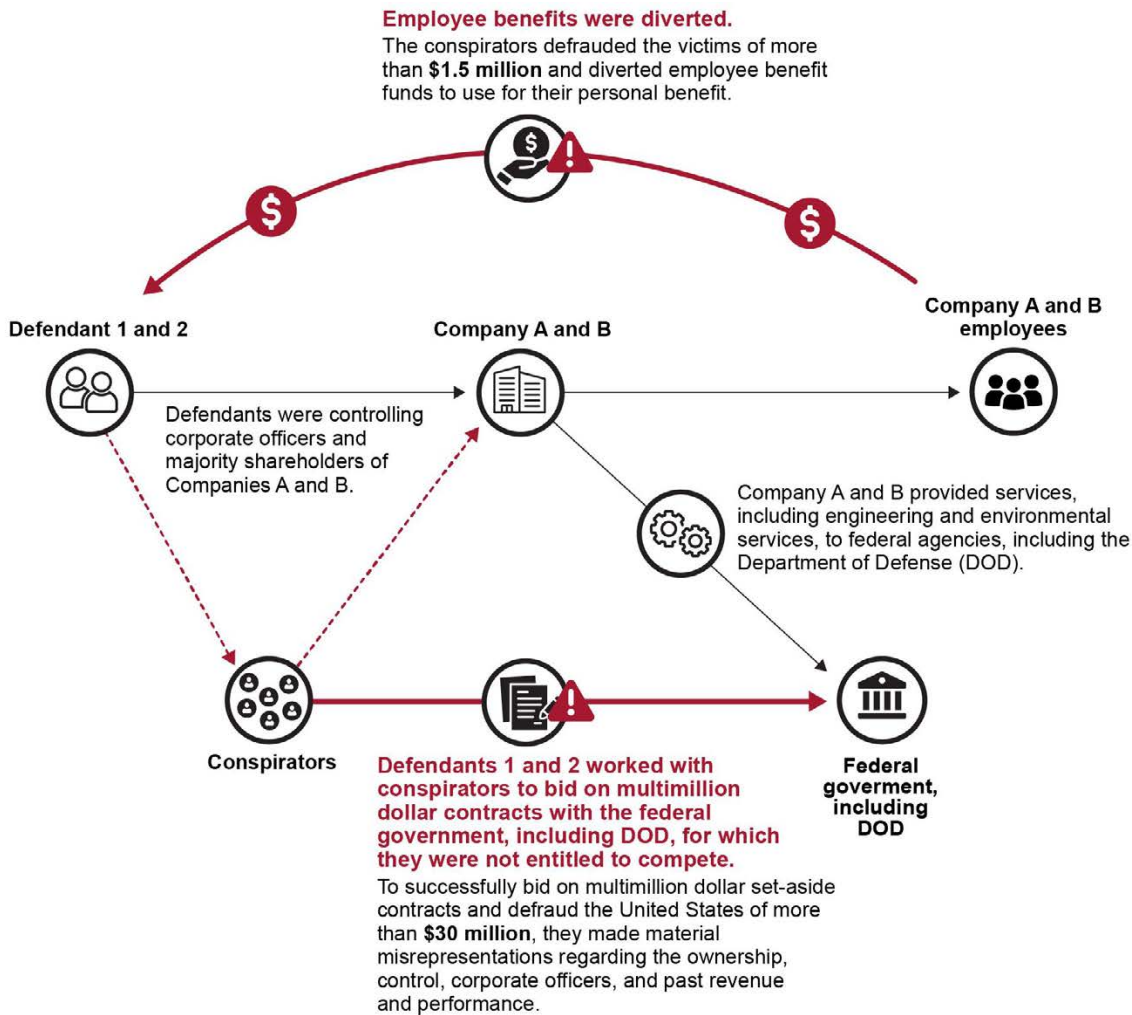
In the figures and tables below, we summarize the general fraud scheme(s) that were employed. We also summarize the offenses that were investigated or adjudicated, how the case originated, other DCIOs or federal agencies that were involved, the suspects that were identified, and the approximate dates of the scheme(s) and investigative case duration. Finally, we summarize the remedies pursued against the defendants and conspirators, including administrative and criminal remedies, and the outcome of the case. Not all suspects of an investigation may have had procurement fraud-related offenses adjudicated against them and, therefore, not all suspects may be included in the case outcome summaries.

To summarize case outcomes, we relied on available administrative proceedings documentation and publicly available court documentation, as appropriate. In summarizing the case outcomes, we did not include all outcome details. For example, we generally did not include standard or other conditions of probation, such as home confinement or community service requirements. Regarding the financial judgments listed, we provide available information about the fines, assessments, restitution, and forfeiture amounts. However, these amounts may not reflect the total extent of actual fraud that was committed. Because of fraud's deceptive

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

nature, financial losses may not be identified, and such losses are difficult to reliably estimate.

Figure 15: Case 1 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case



Sources: GAO analysis of federal court documents and Department of Defense information; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Accessible Text for Figure 15: Case 1 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case

Employee benefits were diverted.

The conspirators defrauded the victims of more than \$1.5 million and diverted employee benefit funds to use for their personal benefit.

Defendant 1 and 2

Defendants were controlling corporate officers and majority shareholders of Companies A and B.

Company A and B

Company A and B employees

Company A and B provided services, including engineering and environmental services to federal agencies, including the Department of Defense (DOD).

Conspirators

Federal government, including DOD

Defendants 1 and 2 worked with conspirators to bid on multimillion dollar contracts with the federal government, including DOD, for which they were not entitled to compete.

To successfully bid on multimillion dollar set-aside contracts and defraud the United States of more than \$30 million, they made material misrepresentations regarding the ownership, control, corporate officers, and past revenue and performance.

Sources: GAO analysis of federal court documents and Department of Defense information; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Table 4: Case 1 – Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021

Case number: offenses investigated and adjudicated	DCIO	Summary
Case 1: <ul style="list-style-type: none"> • Bank fraud • Conspiracy to commit wire fraud • Embezzlement from an employee benefit plan • Money laundering • Tax evasion • Tax fraud • Wire fraud 	<ul style="list-style-type: none"> • Air Force Office of Special Investigations 	<p>Fraud scheme: Defendants 1 and 2 were married and were the controlling corporate officers and majority shareholders of Companies A and B. These companies were two Maryland corporations that provided services, including engineering and environmental services, to federal agencies. The Department of Defense (DOD) was among those agencies receiving services.</p> <p>This case involved two different fraud schemes. Defendants 1 and 2 carried out both schemes with Defendants 3, 4, 5, and 6. The first scheme was to defraud service contract employees of Companies A and B, the United States, and Employee Retirement Income Security Act of 1974 (ERISA) plans so that the conspirators could divert employee benefit monies and personally enrich themselves. The second scheme was to defraud the United States so that Companies A and B could successfully bid on multimillion dollar set-aside contracts with the federal government, including with DOD, for which they were not entitled to compete.</p> <p>To perpetrate the first scheme, conspirators engaged in a variety of acts to defraud victims of more than \$1.5 million in money, benefits, and property. Specifically, they diverted employee benefit funds to their bank accounts so that they could use the money for their personal benefit. They also misrepresented to Company A and B employees that the monies were being held by a third-party administrator and that the employees would be receiving mandated benefits. The conspirators created various entities with no legitimate business purpose, that is, "shell companies," to hide and facilitate the distribution of funds to members of the conspiracy and created fake and fraudulent invoices in an attempt to cover up the illegal distributions for their benefit.</p> <p>To perpetrate the second scheme and defraud the United States of more than \$30 million, the conspirators engaged in a variety of acts. Specifically, they made material misrepresentations regarding Company A and B ownership, control, and corporate officers. The conspirators also made material misrepresentations regarding the past revenue and performance of Companies A and B. Conspirators concealed Defendant 1's role at Company A, falsely portrayed Companies A and B as separate and distinct companies, presented fraudulent documents concerning the scope of the companies' prior work, and underreported revenues and income so that Companies A and B could bid on certain contracts.</p>

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Case number: offenses investigated and adjudicated	DCIO	Summary
Case 1: <ul style="list-style-type: none"> • Bank fraud • Conspiracy to commit wire fraud • Embezzlement from an employee benefit plan • Money laundering • Tax evasion • Tax fraud • Wire fraud 	<ul style="list-style-type: none"> • Air Force Office of Special Investigations 	<p>Case origination: Information provided by Defense Criminal Investigative Service (DCIS)</p> <p>Other DCIOs/federal agencies involved: DCIS; Naval Criminal Investigative Service; Department of Labor – Racketeering and Fraud Investigations; Internal Revenue Service – Criminal Investigations; Small Business Administration Office of Inspector General</p> <p>Suspects identified: Six suspects identified</p> <p>Approximate dates of scheme: 2007-2014</p> <p>Approximate investigative case duration: 2014-2017</p> <p>Remedies/outcome (as indicated in DCIO case file and publicly available court documentation):^a</p> <p>Defendant 1 – Pled guilty to one count of conspiracy to commit wire fraud and one count of tax evasion. Sentenced to 96 months in prison and 3 years’ supervised release and was ordered to pay a \$200 assessment and \$2,092,961 in restitution. Ordered to forfeit interest in certain property, including a money judgment in the amount of \$30 million. Debarred from federal government contracting for a period between 2014 and 2029.</p> <p>Defendant 2 – Pled guilty to one count of conspiracy to commit wire fraud and one count of tax evasion. Sentenced to 12 months and 1 day in prison and 3 years’ supervised release and was ordered to pay a \$200 assessment and \$2,092,961 in restitution. Debarred from federal government contracting for a period between 2014 and 2022.</p> <p>Defendant 3 – Pled guilty to one count of conspiracy to commit wire fraud and one count of tax fraud. Sentenced to probation for 3 years and was ordered to pay a \$200 assessment and \$857,097 in restitution. Debarred from federal government contracting for a period between 2016 and 2022.</p> <p>Defendant 4 – Pled guilty to one count of conspiracy to commit wire fraud and one count of tax fraud. Sentenced to probation for 3 years and was ordered to pay a \$200 assessment and \$851,762 in restitution. Ordered to forfeit interest in \$10 million in U.S. currency. Debarred from federal government contracting for a period between 2016 and 2022.</p> <p>Defendant 5 – Pled guilty to one count of conspiracy to commit wire fraud and one count of tax evasion. Sentenced to probation for 3 years and was ordered to pay a \$200 assessment and \$699,000 in restitution. Debarred from federal government contracting for a period between 2016 and 2022.</p> <p>Defendant 6 – Pled guilty to one count of bank fraud and one count of money laundering. Sentenced to prison for time served and supervised release for 3 years and was ordered to pay a \$200 assessment and about \$1,355,143 in restitution. Ordered to forfeit \$1,145,000</p>

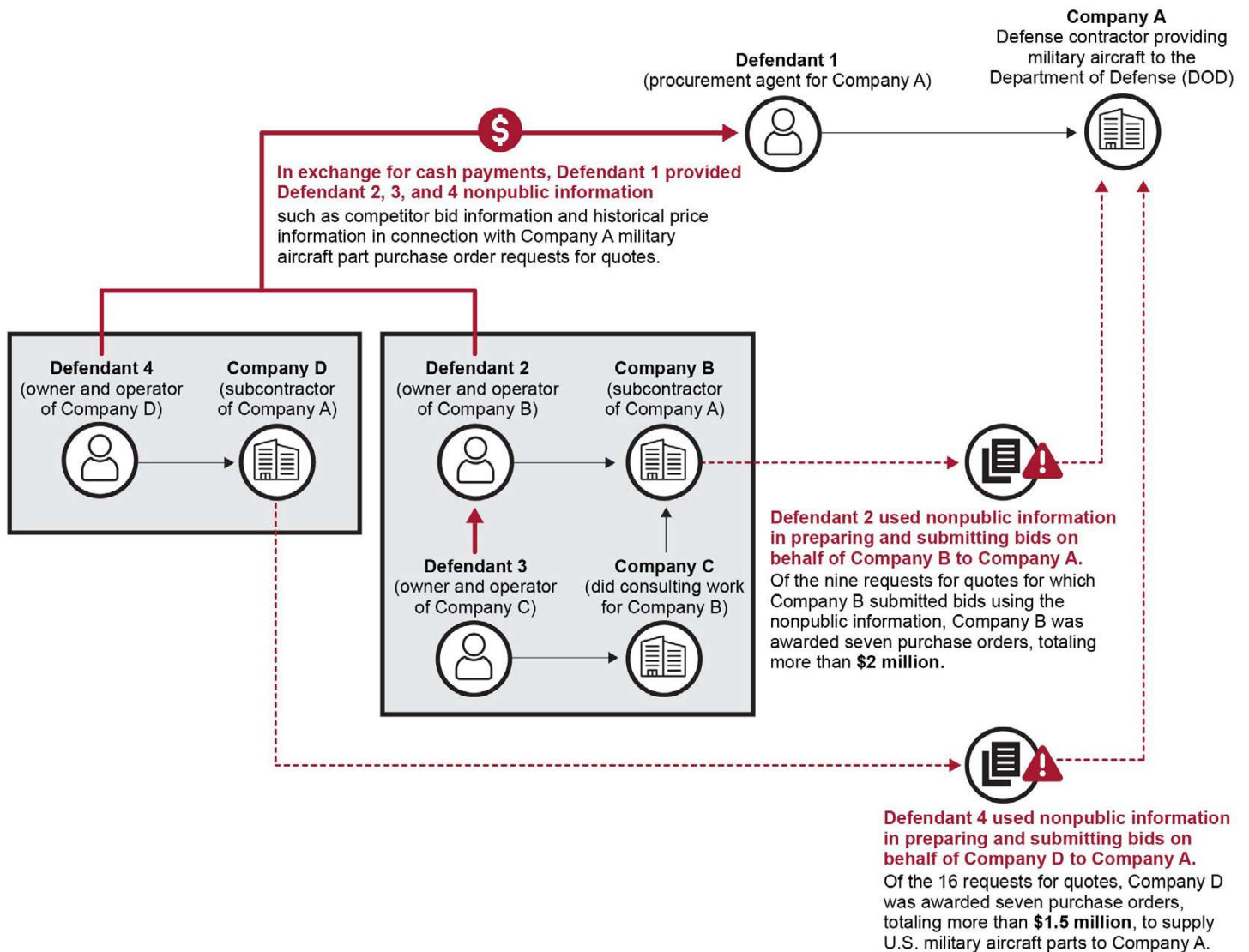
Source: GAO analysis of federal court documents and DOD information. | GAO-24-105358

Note: Debarment refers to an action taken to exclude a contractor from government contracting and government-approved subcontracting for a reasonable, specified period. A contractor that is excluded is “debarred.” 48 C.F.R. § 2.101.

^aThe dollar amounts specified in the financial judgments, for example, the amounts of assessments and restitution, may not reflect the extent of actual fraud that was committed. Because of fraud’s deceptive nature, financial losses may not be identified, and such losses are difficult to reliably estimate.

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Figure 16: Case 2 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case



Sources: GAO analysis of federal court documents and DOD information; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Accessible Text for Figure 16: Case 2 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case

Company A

Defense contractor providing military aircraft to the Department of Defense (DOD)

Defendant 1 (procurement agent for Company A)

In exchange for cash payments, Defendant 1 provided Defendant 2, 3, and 4 nonpublic information such as competitor bid information and historical price information in connection with Company A military part purchase order request for quotes.

Defendant 4 (owner and operator of Company D)

Company D (subcontractor of Company A)

Defendant 2 (owner and operator of Company B)

Company B (subcontractor of Company A)

Defendant 3 (owner and operator of Company C)

Company C (did consulting work for Company B)

Defendant 2 used nonpublic information in preparing and submitting bids on behalf of Company B to Company A.

Of the nine requests for quotes for which Company B submitted bids using the nonpublic information, Company B was awarded seven purchase orders totaling more than \$2 million.

Defendant 2 used nonpublic information in preparing and submitting bids on behalf of Company D to Company A.

Of the 16 requests for quotes, Company D was awarded seven purchase orders, totaling more than \$1.5 million, to supply U.S. military aircraft parts to Company A.

Sources: GAO analysis of federal court documents and DOD information; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Table 5: Case 2 - Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021

Case number: offenses investigated or adjudicated	DCIO	Summary
Case 2: <ul style="list-style-type: none"> • Bribery • Mail fraud • Money laundering • Structuring transactions to evade reporting requirements • Wire fraud 	Air Force Office of Special Investigations	<p>Fraud scheme: Defendant 1 was a procurement agent for Company A, a defense contractor providing military aircraft to the Department of Defense (DOD). Defendant 2 was the owner and operator of Company B, a subcontractor to Company A. Defendant 3 was the owner and operator of Company C, which did consulting work for Company B. Defendant 4 was the owner and operator of Company D, a subcontractor to Company A.</p> <p>Defendant 1 provided Company B, through Defendants 2 and 3, and without the knowledge of Company A, nonpublic information. This information presumably gave Company B an advantage when submitting bids in response to Company A's requests for quotes. The nonpublic information included competitor bid information and historical price information in connection with Company A military aircraft-part purchase order requests for quotes. Defendant 2 used that information in preparing and submitting bids on behalf of Company B to Company A in response to approximately nine different Company A requests for quotes. In exchange for the nonpublic information, Defendants 2 and 3 made cash payments, in person and via mail, to Defendant 1. Of the nine requests for quotes for which Company B submitted bids using the nonpublic information, Company B was awarded seven purchase orders, totaling more than \$2 million.</p> <p>Defendants 1 and 4 carried out a similar scheme, where Defendant 4 used nonpublic bid information provided by Defendant 1 to prepare and submit bids on behalf of Company D to Company A in response to approximately 16 different Company A requests for quotes. In exchange for the nonpublic information, Defendant 4 made cash payments to Defendant 1. Of those 16 requests for quotes, Company D was awarded seven purchase orders, totaling more than \$1.5 million, to supply U.S. military aircraft parts to Company A.</p> <p>According to investigative case files, Defendant 1 had received an estimated \$231,000 in bribes by September 2013.</p>

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Case number: offenses investigated or adjudicated	DCIO	Summary
Case 2: <ul style="list-style-type: none"> • Bribery • Mail fraud • Money laundering • Structuring transactions to evade reporting requirements • Wire fraud 	Air Force Office of Special Investigations	<p>Other DCIOs/federal agencies involved: DCIS, Federal Bureau of Investigation (FBI), Naval Criminal Investigative Service, Internal Revenue Service, National Aeronautics and Space Administration Office of the Inspector General</p> <p>Suspects identified: Ten suspects identified</p> <p>Approximate dates of scheme: 2009-2013</p> <p>Approximate investigative case duration: 2013-2015</p> <p>Remedies/outcome (as indicated in DCIO case file and publicly available court documentation):^a</p> <p>Defendant 1 – Pled guilty to one count of mail fraud, three counts of wire fraud, and one count of structuring transactions to evade reporting requirements. Sentenced to 20 months in prison and 24 months’ supervised release and was ordered to pay a \$500 assessment and to forfeit certain property. Suspended from government contracting in October 2013 and subsequently debarred for a period between 2014 and 2018.</p> <p>Defendant 2 – Pled guilty to one count of mail fraud and two counts of wire fraud. Sentenced to 15 months in prison and 3 years’ supervised release. Ordered to pay a \$300 assessment and a \$50,000 fine and to forfeit certain property. Suspended from government contracting in October 2013 and subsequently debarred for a period between 2015 and 2018.</p> <p>Defendant 3 – Pled guilty to one count of mail fraud and two counts of wire fraud. Sentenced to 15 months in prison and 3 years’ supervised release. Ordered to pay a \$300 assessment and a \$2,000 fine and to forfeit certain property. Defendant 3 and Company C were suspended from government contracting in October 2013 and subsequently debarred for a period between 2014 and 2018.</p> <p>Defendant 4 – Pled guilty to one count of wire fraud. Defendant 4 was sentenced to 18 months in prison and 36 months’ supervised release. Ordered to pay a \$100 assessment and a \$10,000 fine and to forfeit certain property. Suspended from government contracting in October 2013 and was subsequently debarred for a period between 2014 and 2018. Company D was debarred for a period between 2013 and 2016.</p>

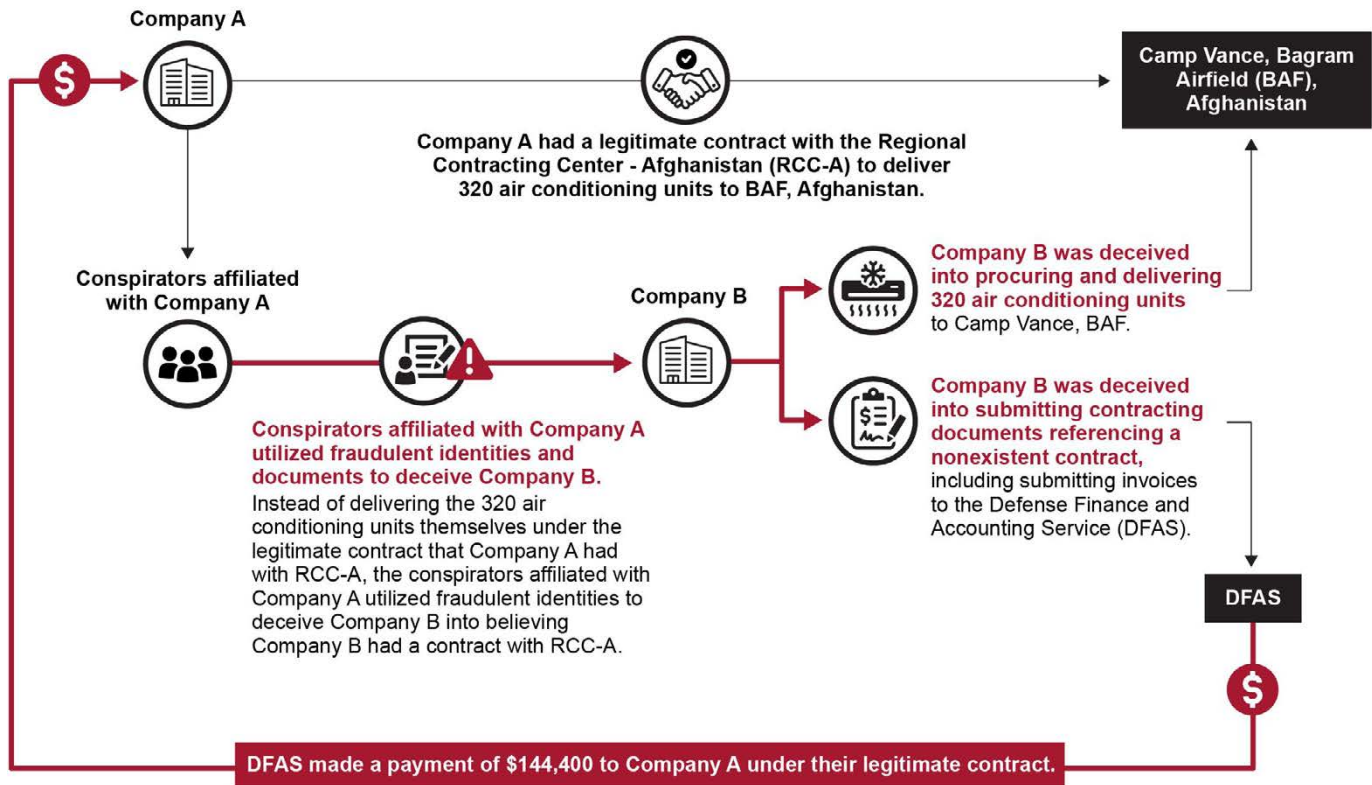
Source: GAO analysis of federal court documents and DOD information. | GAO-24-105358

Note: Suspension refers to the action taken to disqualify a contractor temporarily from government contracting and government-approved subcontracting. A contractor that is disqualified is “suspended.” Suspension is an action imposed pending the completion of investigation or legal proceedings, when it has been determined that immediate action is necessary to protect the government’s interests. Debarment refers to an action taken to exclude a contractor from government contracting and government-approved subcontracting for a reasonable, specified period. A contractor that is excluded is “debarred.” 48 C.F.R. §§ 2.101 and 9.407-1.

^aThe dollar amounts specified in the financial judgments, for example, the amounts of assessments and restitution, may not reflect the extent of actual fraud that was committed. Because of fraud’s deceptive nature, financial losses may not be identified, and such losses are difficult to reliably estimate.

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Figure 17: Case 3 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case



Sources: GAO analysis of Department of Defense information; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Accessible Text for Figure 17: Case 3 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case

Company A

Company A had a legitimate contract with the Regional Contracting Center – Afghanistan (RCC-A) to deliver 320 air conditioning units to BAF, Afghanistan.

Camp Vance, Bagram Airfield (BAF), Afghanistan

Conspirators affiliated with Company A

Conspirators affiliated with Company A utilized fraudulent identities and documents to deceive Company B.

Instead of delivering the 320 air conditioning units themselves under the legitimate contract that Company A had with RCC-A, the conspirators affiliated with Company A utilized fraudulent identities to deceive Company B into believing Company B had a contract with RCC-A.

Company B

Company B was deceived into procuring and delivering 320 air conditioning units to Camp Vance, BAF.

Company B was deceived into submitting contracting documents referencing a nonexistent contract, including submitting invoices to the Defense Finance and Accounting Service (DFAS)

DFAS

DFAS made a payment of \$144,400 to Company A under their legitimate contract.

Sources: GAO analysis of Department of Defense information; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Table 6: Case 3 - Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021

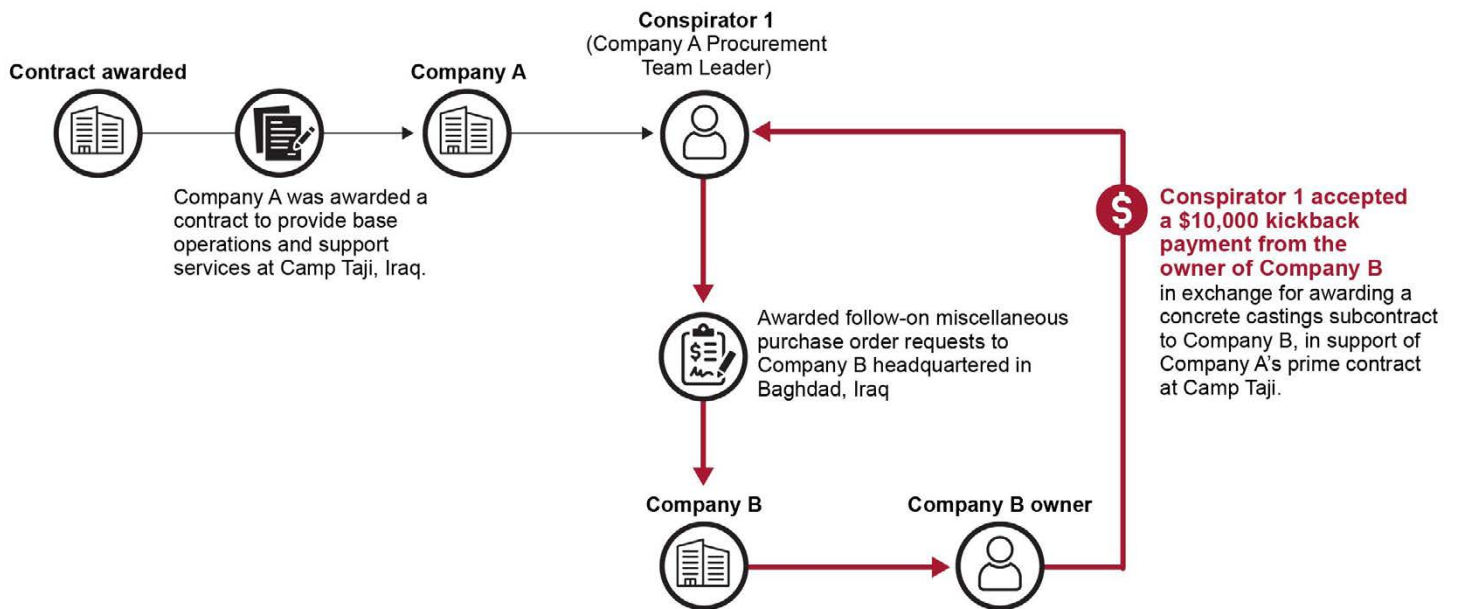
Case number: offenses investigated or adjudicated	DCIO	Summary
Case 3: • False claims • False statements	Army Criminal Investigation Division	Fraud scheme: Company A had a legitimate contract with the Regional Contracting Center - Afghanistan (RCC-A) to deliver 320 air conditioning units to Camp Vance, Bagram Airfield (BAF), Afghanistan. Conspirator 1 was the President/Owner of Company A; Conspirator 2 was its Co-President; and Conspirator 3 was a Contract Manager for Company A.
Case 3: • False claims • False statements	Army Criminal Investigation Division	<p>The conspirators fraudulently misrepresented themselves as contracting officers from RCC-A by surreptitiously stealing the identities of two individuals. Instead of delivering the 320 air conditioning units themselves under the legitimate contract that Company A had with RCC-A, the conspirators utilized these fraudulent identities to deceive Company B, and its owner, Victim 1, into believing Victim 1/Company B had a contract with RCC-A and into procuring and delivering the 320 air conditioning units to Camp Vance, BAF.</p> <p>To perpetrate the scheme, the conspirators created and utilized fictitious email accounts of contracting officers and drafted fictitious invoices and contracting documents.</p> <p>After Company B completed the delivery of the air conditioning units, the conspirators at Company A submitted an electronic invoice for payment. After confirmation and acceptance of the air conditioning units, an electronic request to the Defense Finance and Accounting Service (DFAS) was triggered to make a payment to Company A in the amount of \$144,400 under their legitimate contract. Company A received this payment fraudulently because the conspirators had tricked the victims, Company B and Victim 1, into delivering the air conditioning units. After receipt of the payment, the conspirators withdrew all of the funds from their business account and fled Afghanistan.</p> <p>Later, Company B submitted the invoices and contracting documents to DFAS in support of the payment in the amount of \$144,400 for the delivery of 320 air conditioning units. Because the documents referenced a nonexistent contract, Company B and Victim 1 (and another of Victim 1's companies) were initially identified as suspects, rather than victims.</p> <p>Case origination: Notification from RCC-A that Company B filed a potentially fraudulent claim in support of a nonawarded contract.</p> <p>Other DCIOs/federal agencies involved: Defense Criminal Investigative Service, Special Inspector General for Afghanistan Reconstruction</p> <p>Suspects identified: Seven suspects identified</p> <p>Approximate dates of scheme: 2018</p> <p>Approximate investigative case duration: 2018-2019</p> <p>Remedies/outcome (as indicated in DCIO case file):^a The four Company A conspirators, including Company A, were debarred from federal government contracting for almost 5 years for a period between 2019 and 2024. They fled Afghanistan, and no additional remedies were pursued.</p>

Source: GAO analysis of Department of Defense information. | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

^aDebarment refers to an action taken to exclude a contractor from government contracting and government-approved subcontracting for a reasonable, specified period. A contractor that is excluded is "debarred." 48 C.F.R. § 2.101.

Figure 18: Case 4 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case



Sources: GAO analysis of Department of Defense information; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

Accessible Text for Figure 18: Case 4 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case

Contract awarded

Company A was awarded a contract to provide base operations and support services to Camp Taji, Iraq.

Company A

Conspirator 1 (Company A Procurement Team Leader)

Awarded follow-on miscellaneous purchase order requests to Company B headquartered in Baghdad, Iraq

Company B

Company B owner

Conspirator 1 accepted a \$10,000 kickback payment from the owner of Company B in exchange for awarding a concrete castings subcontract to Company B, in support of Company A's prime contract at Camp Taji.

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Sources: GAO analysis of Department of Defense information; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Table 7: Case 4 - Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021

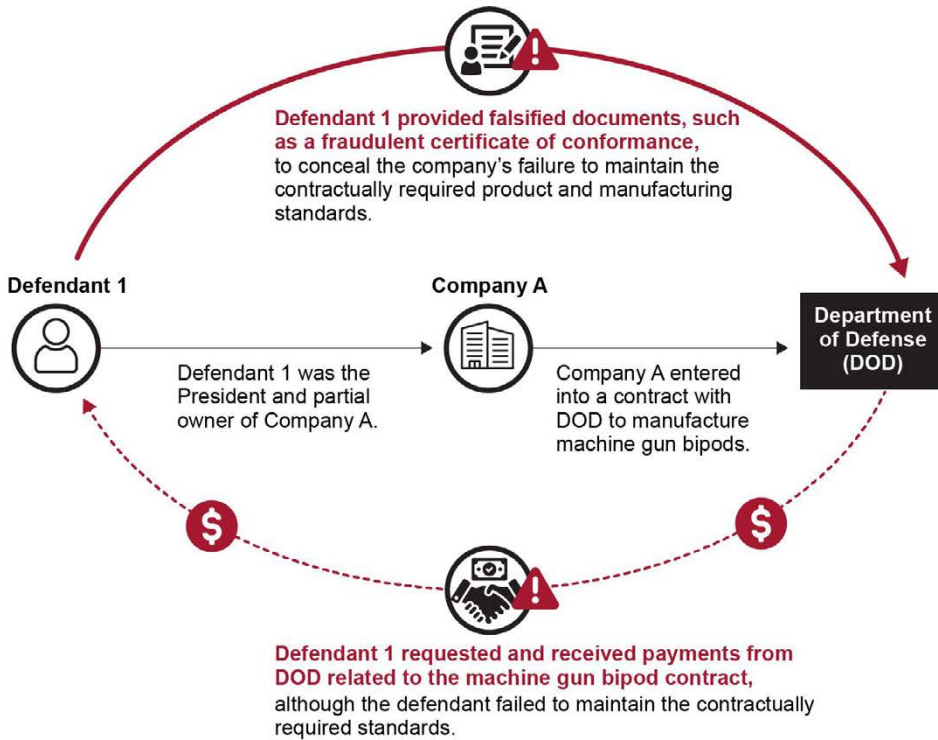
Case number: offenses investigated or adjudicated	DCIO	Summary
Case 4: <ul style="list-style-type: none"> • Conspiracy • Kickbacks 	Army Criminal Investigation Division	<p>Fraud scheme: In 2015, a Base Operations and Support contract was awarded to Company A to provide base operations support at Camp Taji, Iraq. Conspirator 1 was the Company A Procurement Team Leader and, as such, awarded the follow-on miscellaneous purchase order requests to subcontractors and vendors, including to a Contracting Company B (Conspirator 3) headquartered in Baghdad, Iraq.</p> <p>Between October 2016 and November 2016, Conspirator 1 accepted a \$10,000 kickback payment and, on several occasions, accepted B12 injectable syringes from the owner of the Contracting Company B (Conspirator 2). Conspirator 1 did so in exchange for awarding a concrete castings subcontract to Company B, in support of Company A's prime contract at Camp Taji. Conspirator 4 was a Company A employee at Camp Taji who acted as a go-between for Conspirators 1 and 2 to deliver the kickback payments and syringes.</p> <p>Case origination: Investigation was developed based on information reported in 2018.</p> <p>Other DCIOs/federal agencies involved: Defense Criminal Investigative Service</p> <p>Suspects identified: Four suspects identified</p> <p>Approximate dates of scheme: 2016</p> <p>Approximate investigative case duration: 2018-2021</p> <p>Remedies/outcome (as indicated in DCIO case file):^a</p> <p>Conspirator 1 – Debarred from government contracting for a period between 2021 and 2025; employment with Company A terminated; barred from all installations under Combined Joint Task Force, Operation Inherent Resolve jurisdiction or control</p> <p>Conspirator 2 – Debarred from government contracting for a period between 2021 and 2023</p> <p>Conspirator 3 – Debarred from government contracting for a period between 2021 and 2023</p> <p>Conspirator 4 – Employment terminated by Company A</p>

Source: GAO analysis of Department of Defense information. | GAO-24-105358

^aDebarment refers to an action taken to exclude a contractor from government contracting and government-approved subcontracting for a reasonable, specified period. A contractor that is excluded is "debarred." 48 C.F.R. § 2.101.

Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases

Figure 19: Case 5 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case



Sources: GAO analysis of federal court documents and DOD information; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Accessible Text for Figure 19: Case 5 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case

Defendant 1

Defendant 1 was the president and partial owner of Company A.

Company A

Company A entered into a contract with DOD to manufacture machine gun bipods.

Department of Defense (DOD)

Defendant 1 provided falsified documents, such as a fraudulent certificate of conformance, to conceal the company's failure to maintain the contractually required product and manufacturing standards.

Defendant 1 requested and received payments from DOD related to the machine gun bipod contract, although the defendant failed to maintain the contractually required standards.

Sources: GAO analysis of federal court documents and DOD information; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Table 8: Case 5 - Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021

Case number: offenses investigated or adjudicated	DCIO	Summary
Case 5: <ul style="list-style-type: none"> • False statements • Wire fraud 	Defense Criminal Investigative Service (DCIS)	<p>Fraud scheme: Defendant 1 was the President and partial owner of Company A, which had entered into a contract with the Department of Defense (DOD) to manufacture machine gun bipods. The bipods are a device used by infantrymen to steady machine guns. The contract contained provisions that required Company A to (1) comply with a high-quality product standard, (2) establish and maintain a system of inspections to ensure that the bipods conformed with contractual specifications and to maintain a record of those inspections that could be produced to DOD, and (3) deliver bipods to DOD only if those bipods were inspected and found to conform with the contractual specifications. In addition to the payment for completed bipods, Company A was entitled to request "progress payments" to cover the manufacturing expenses before delivering the bipods.</p> <p>From 2012 to 2013, Defendant 1 submitted requests for payments to DOD under the contract, although Company A had failed to maintain the contractually required high-quality product and manufacturing standards. Defendant 1 then provided purposefully falsified documents to DOD inspectors to conceal the company's failure to maintain the contractually required standards.</p> <p>As a result of the invoices that Defendant 1 submitted to DOD, DOD wired payments, totaling about \$124,200, to Company A. All the payments were made by means of interstate wire transfers.</p> <p>In June 2013, an inspector with the Defense Contract Management Agency (DCMA) inspected Company A's headquarters and manufacturing plant. The inspector asked for Company A's certificates of conformance for several bipod components and materials, including a compression spring that was an essential part of the bipod assembly. Defendant 1 provided the inspector with a copy of what was purported to be a certificate of conformance for the spring generated by a third-party manufacturer that had tested it. The inspector later learned from the spring manufacturer that the certificate that Defendant 1 had provided was fraudulent. The spring manufacturer had never performed any work for Company A.</p>

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Case number: offenses investigated or adjudicated	DCIO	Summary
Case 5: <ul style="list-style-type: none"> • False statements • Wire fraud 	Defense Criminal Investigative Service (DCIS)	<p>In August 2013, the DCMA inspector submitted one of the bipods manufactured by Company A to a military engineer for testing. The engineer’s preliminary test result found many deficiencies, including that the compression spring was broken.</p> <p>The inspector issued a series of Corrective Action Reports to Company A, mandating that Company A address deficiencies in its manufacturing process. Defendant 1 subsequently informed the inspector that Company A had hired an outside consultant to review its system for complying with high-quality product standards. In November 2013, after the inspector requested that Defendant 1 forward a certificate showing that Company A was in compliance with the high-quality standards, Defendant 1 forwarded the inspector a copy of a certificate provided by a third-party auditing company stating that Company A was in compliance with those standards. When the inspector contacted the auditing company, the auditing company informed the inspector that the certificate was fraudulent and that Company A’s certification had in fact expired in 2010.</p> <p>Case origination: DCIS received information from the DCMA regarding a fraudulent certificate of conformance provided by Company A.</p> <p>Other DCIOs/federal agencies involved: Army Criminal Investigation Division</p> <p>Suspects identified: One suspect identified</p> <p>Approximate dates of scheme: 2012-2013</p> <p>Approximate investigative case duration: 2013-2018</p> <p>Remedies/outcome (as indicated in DCIO case file and publicly available court documentation):^a</p>

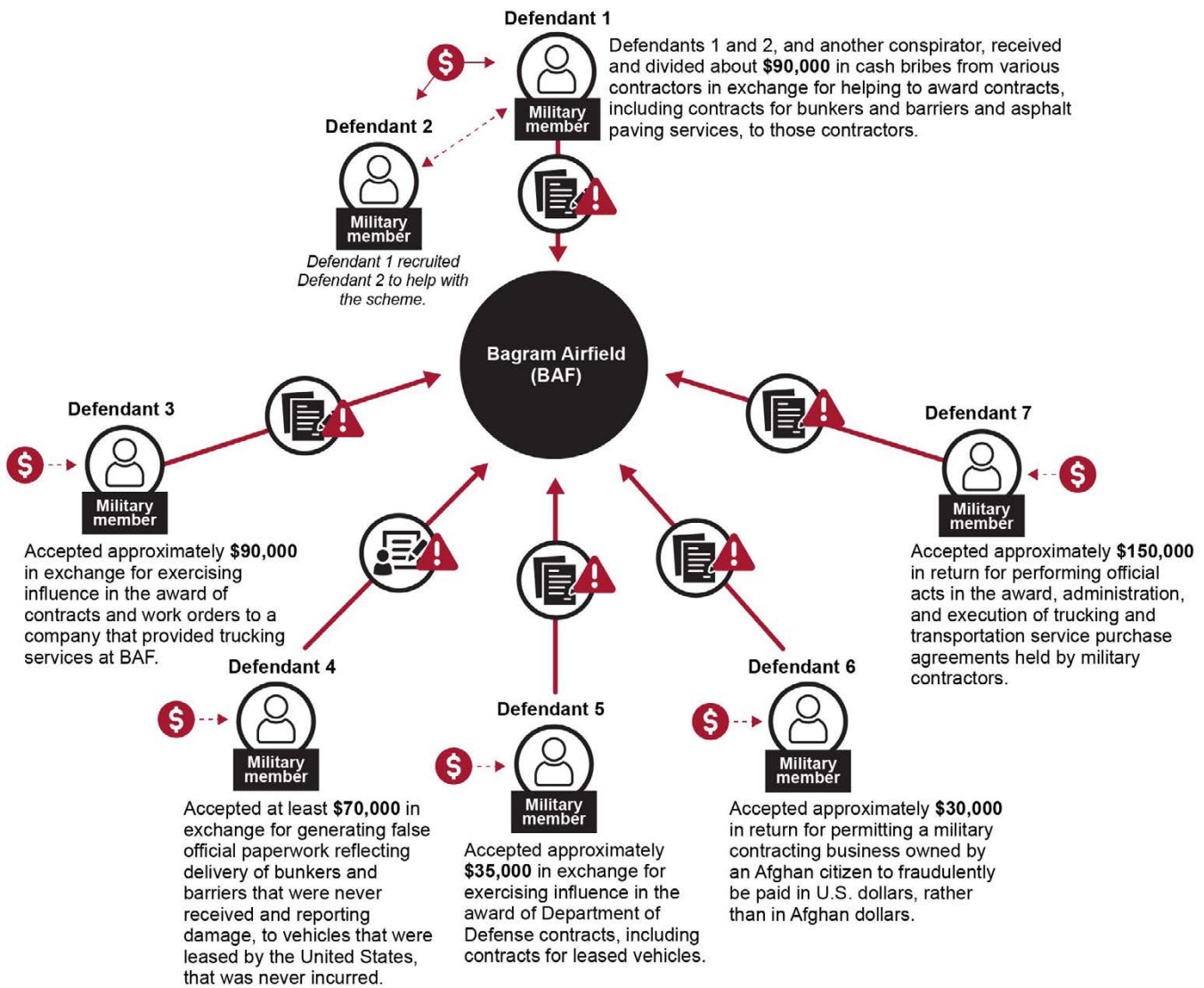
Source: GAO analysis of federal court documents and DOD information. | GAO-24-105358

Note: Debarment refers to an action taken to exclude a contractor from government contracting and government-approved subcontracting for a reasonable, specified period. A contractor that is excluded is “debarred.” 48 C.F.R. § 2.101.

^aThe dollar amounts specified in the financial judgments, for example, the amounts of assessments and restitution, may not reflect the extent of actual fraud that was committed. Because of fraud’s deceptive nature, financial losses may not be identified, and such losses are difficult to reliably estimate.

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Figure 20: Case 6 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case



Sources: GAO analysis of federal court documents and Department of Defense information; Icons-Studio/stock.adobe.com. | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Accessible Data for Figure 20: Case 6 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case

Bagram Airfield (BAF)

Defendants 1 and 2, and another conspirator, received and divided about \$90,000 in cash bribes from various contractors in exchange for helping to award contracts, including contracts for bunkers and barriers and asphalt paving services, to those contractors.

Defendant 2 (Military member)

Defendant 1 recruited Defendant 2 to help with the scheme.

Defendant 3 (Military member)

Accepted approximately \$90,000 in exchange for exercising influence in the award of contracts and work orders to a company that provided trucking services at BAF.

Defendant 4 (Military member)

Accepted at least \$70,000 in exchange for generating false official paperwork reflecting delivery of bunkers and barriers that were never received and reporting damage, to vehicles that were leased by the United States, that never incurred.

Defendant 5 (Military member)

Accepted approximately \$35,000 in exchange for exercising influence in the award of Department of Defense contracts, including contracts for leased vehicles.

Defendant 6 (Military member)

Accepted approximately \$30,000 in return for permitting a military contracting business owned by an Afghan citizen to fraudulently be paid in U.S. dollars, rather than in Afghan dollars.

Defendant 7 (Military member)

Accepted approximately \$150,000 in return for performing official acts in the award, administration, and execution of trucking and transportation service purchase agreements held by military contractors.

Sources: GAO analysis of federal court documents and Department of Defense information; Icons-Studio/stock.adobe.com. | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Table 9: Case 6 - Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021

Case number: offenses investigated or adjudicated	DCIO	Summary
Case 6: <ul style="list-style-type: none"> • Bribery • Conspiracy to commit bribery • Conspiracy to commit mail fraud • Corruption • Money laundering • Money laundering conspiracy • Receipt of stolen property 	Defense Criminal Investigative Service (DCIS)	<p>Fraud scheme: This case was initiated to investigate possible corruption in the contracting office at the Bagram Air Force Base (AFB), Afghanistan. The case involved the investigation of over 30 suspects and resulted in the criminal prosecution of 20 suspects who were involved in multiple fraud schemes regarding the contracting of various services at Bagram Airfield (BAF). One of the schemes involved 10 different suspects.</p> <p>Defendant 1 was an Army Major assigned as head of Base Operations. As head of Base Operations, Defendant 1 received requests for acquisition from different military components at BAF. Defendant 1 was offered bribes from various contractors in exchange for helping to award contracts, including contracts for bunkers and barriers and asphalt paving services. Defendant 1 recruited Defendant 2, an Air Force Master Sergeant deployed as a Contracting Officer to BAF, to help with this scheme. Defendant 2 awarded multiple contracts to different contractors in return for cash payments totaling about \$90,000, which Defendant 2 divided with Defendant 1 and another conspirator.</p> <p>Defendant 3 was a Sergeant in the U.S. Army assigned to the Transportation Operations Support Office and responsible for administering transportation services provided by Department of Defense (DOD) contractors, including trucks used to transport goods from BAF to destinations throughout Afghanistan. Defendant 3 could issue work orders and could influence which contractor received contracts. Defendant 3 accepted approximately \$90,000 from a conspirator working for a DOD contractor that provided trucking services at BAF, in exchange for exercising influence in the award of DOD contracts and work orders to that contractor.</p> <p>Defendant 4 was a First Lieutenant in the U.S. Army. This defendant was responsible for inspecting and documenting deliveries of various goods and services, including bunkers and barriers, from government contractors to BAF. Defendant 4 was also responsible for generating official paperwork through which such contractors were paid. Defendant 4 generated false official paperwork reflecting delivery of bunkers and barriers that were never received and reporting damage to vehicles leased by the United States, which, in fact, was never incurred. Using this false official paperwork, conspirator contractors claimed and collected payments from the United States, in return for which conspirator contractors gave Defendant 4 money and other things of value. Defendant 4 accepted at least \$70,000 in bribes from conspirator contractors.</p>

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

<p>Case 6:</p> <ul style="list-style-type: none"> • Bribery • Conspiracy to commit bribery • Conspiracy to commit mail fraud • Corruption • Money laundering • Money laundering conspiracy • Receipt of stolen property 	<p>Defense Criminal Investigative Service (DCIS)</p>	<p>Defendant 5 was a Captain in the U.S. Army National Guard and served as the motor pool officer, controlling a fleet of leased vehicles. Defendant 5 also oversaw and verified the delivery of goods, such as barriers. Defendant 5 accepted approximately \$35,000 from multiple DOD contractors in exchange for exercising influence in the award of DOD contracts, including contracts for leased vehicles. Defendant 5 also accepted cash in return for fraudulently inflating the number of concrete barriers delivered to BAF.</p> <p>Defendant 6 was a Staff Sergeant in the U.S. Army and worked in the Finance Office. This defendant was responsible for making payments to DOD contractors for goods and services provided at BAF. When presented with a properly signed Material Inspection and Receiving Report, Defendant 6 would arrange for the contractors to be paid, usually in cash. Defendant 6 accepted approximately \$30,000 in return for permitting a military contracting business owned by an Afghan citizen to fraudulently be paid in U.S. dollars, rather than in Afghan dollars pursuant to the relevant regulations in place.</p> <p>Defendant 7 was a Sergeant with the U.S. Army and was responsible for trucking and transportation services, also called “line-haul” services, and participated in evaluating, recommending, and facilitating the award of line-haul purchase agreements at BAF. After the purchase agreements were awarded, Defendant 7 had authority to order trucking services associated with those agreements. Defendant 7 also served as the verifying official for monthly invoices submitted by the line-haul contractors. In this role, the defendant verified the accuracy of the invoices and, by the defendant’s signature alone, the United States was obligated to pay the contractors for services rendered. In exchange for \$50,000, Defendant 7 facilitated the award of a line-haul purchase agreement to a conspirator corporation. The conspirator corporation wired the money to an account in Hawaii owned by Defendant 8. Defendant 8 was a First Sergeant with the U.S. Army who had overall supervisory responsibility for approximately 40 enlisted soldiers, including Defendant 7. Defendant 7 also accepted approximately \$150,000 in return for performing official acts in the award, administration, and execution of the line-haul purchase agreements held by military contractors.</p> <p>Other DCIOs/federal agencies involved: Army Criminal Investigation Division Suspects identified: Over 30 suspects were identified. Approximate dates of scheme: 2003-2009 Approximate investigative case duration: 2005-2015 Remedies/outcome (as indicated in DCIO case file and publicly available court documentation):a Defendant 1 – Pled guilty to four counts of conspiracy to commit bribery, three counts of bribery, and one count of conspiracy to commit mail fraud. Sentenced to 60 months in prison and 2 years’ supervised release. Ordered to pay \$800 assessment, \$500,000 restitution. Defendant 2 – Pled guilty to three counts of conspiracy to commit bribery and three counts of bribery. Sentenced to 40 months in prison and 1 year supervised release. Ordered to pay \$600 assessment; \$130,000 restitution. As part of a plea agreement, Defendant 2 agreed not to solicit or accept employment with the U.S. government and not to solicit, conduct, or attempt to conduct any business with the U.S. government for a period of 3 years from the date of sentencing. Defendant 3 – Pled guilty to one count of bribery and one count of money laundering conspiracy. Sentenced to 18 months in prison and 3 years’ supervised release. Ordered to pay \$200 special assessment; \$90,000 restitution. Received a reduction in rank and a discharge order. The order reduced Defendant 3’s rank</p>
--	--	---

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Case number: offenses investigated or adjudicated	DCIO	Summary
		<p>from E-6 to E-1 and separated Defendant 3 from the U.S. Army under an “other than Honorable Condition.”</p> <p>Defendant 4 – Pled guilty to one count of conspiracy to commit bribery and defraud the United States and one count of bribery. Sentenced to 15 months in prison and 2 years’ supervised release. Ordered to pay \$200 assessment; \$98,000 restitution.</p> <p>Defendant 5 – Pled guilty to three counts of bribery. Sentenced to 15 months in prison and 1 year supervised release. Ordered to pay \$300 assessment; \$115,000 restitution.</p> <p>Defendant 6 – Pled guilty to one count of bribery. Sentenced to 1 year and 1 day in prison and 1 year supervised release. Ordered to pay \$100 assessment; \$30,000 restitution. Debarred from government contracting for about 4 years, from 2011 to 2015.</p> <p>Defendant 7 – Pled guilty to one count of conspiracy to defraud the United States and to commit bribery and one count of bribery. Sentenced to 51 months in prison and 3 years’ supervised release. Ordered to pay \$200 assessment; \$200,000 restitution.</p> <p>Defendant 8 – Pled guilty to one count of conspiracy to defraud the United States and to commit bribery. Sentenced to 31 months in prison and 3 years’ supervised release. Ordered to pay \$100 assessment; \$50,000 restitution.</p> <p>Defendant 9 – Pled guilty to one count of paying a gratuity to a public official. Sentenced to 18 months in prison and 1 year supervised release. Ordered to pay \$100 assessment; \$30,000 fine; \$50,000 restitution.</p> <p>Defendant 10 – Pled guilty to one count of paying a gratuity to a public official. Sentenced to 6 months in prison and 1 year supervised release. Ordered to pay \$100 assessment; \$20,000 fine; \$50,000 restitution.</p> <p>Defendant 11 – Pled guilty to one count of conspiracy. Sentenced to imprisonment for 2 months; 6 months’ supervised release. Ordered to pay \$100 assessment; \$27,000 restitution.</p> <p>Defendant 12 – Pled guilty to one count of conspiracy to defraud the United States and to commit an offense against the United States. Sentenced to probation for 3 years. Ordered to pay \$400 assessment; \$500,000 fine; \$62,500 restitution.</p> <p>Defendant 13 – Pled guilty to one count of conspiracy to commit bribery. Sentenced to 45 days in prison and 1 year supervised release. Ordered to pay \$100 assessment; \$30,000 restitution.</p> <p>Defendant 14 – Pled guilty to one count of conspiracy to defraud the United States by bribery. Sentenced to 1 year probation. Ordered to pay \$400 assessment; \$500,000 fine; \$125,000 restitution.</p> <p>Defendant 15 – Pled guilty to one count of paying a gratuity to a public official. Sentenced to 2 years’ probation. Ordered to pay \$400 assessment; \$50,000 fine; \$50,000 restitution.</p>

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Case number: offenses investigated or adjudicated	DCIO	Summary
Case 6: <ul style="list-style-type: none"> • Bribery • Conspiracy to commit bribery • Conspiracy to commit mail fraud • Corruption • Money laundering • Money laundering conspiracy • Receipt of stolen property 	Defense Criminal Investigative Service (DCIS)	Defendant 16 – Defendant was charged in 2009, but charges were dismissed in 2022 without being adjudicated. Defendant 17 – Pled guilty to one count of receipt of stolen property. Sentenced to 6 months in prison and 2 years' supervised release. Ordered to pay \$100 assessment; \$100,000 restitution; forfeiture of currency seized from safe deposit box for \$16,700. Defendant 18 – Pled guilty to one count of receiving and accepting illegal gratuity. Sentenced to 90 days in prison and 1 year supervised release. Ordered to pay \$100 assessment; \$10,000 fine; \$20,000 restitution. Suspended from government contracting. Defendant 19 – Pled guilty to one count of receipt of stolen property. Sentenced to probation for 3 years. Ordered to pay \$7,000 restitution. Defendant 20 – Pled guilty to one count of bribery of a public official. Ordered to pay \$400 assessment; \$1,040,000 fine

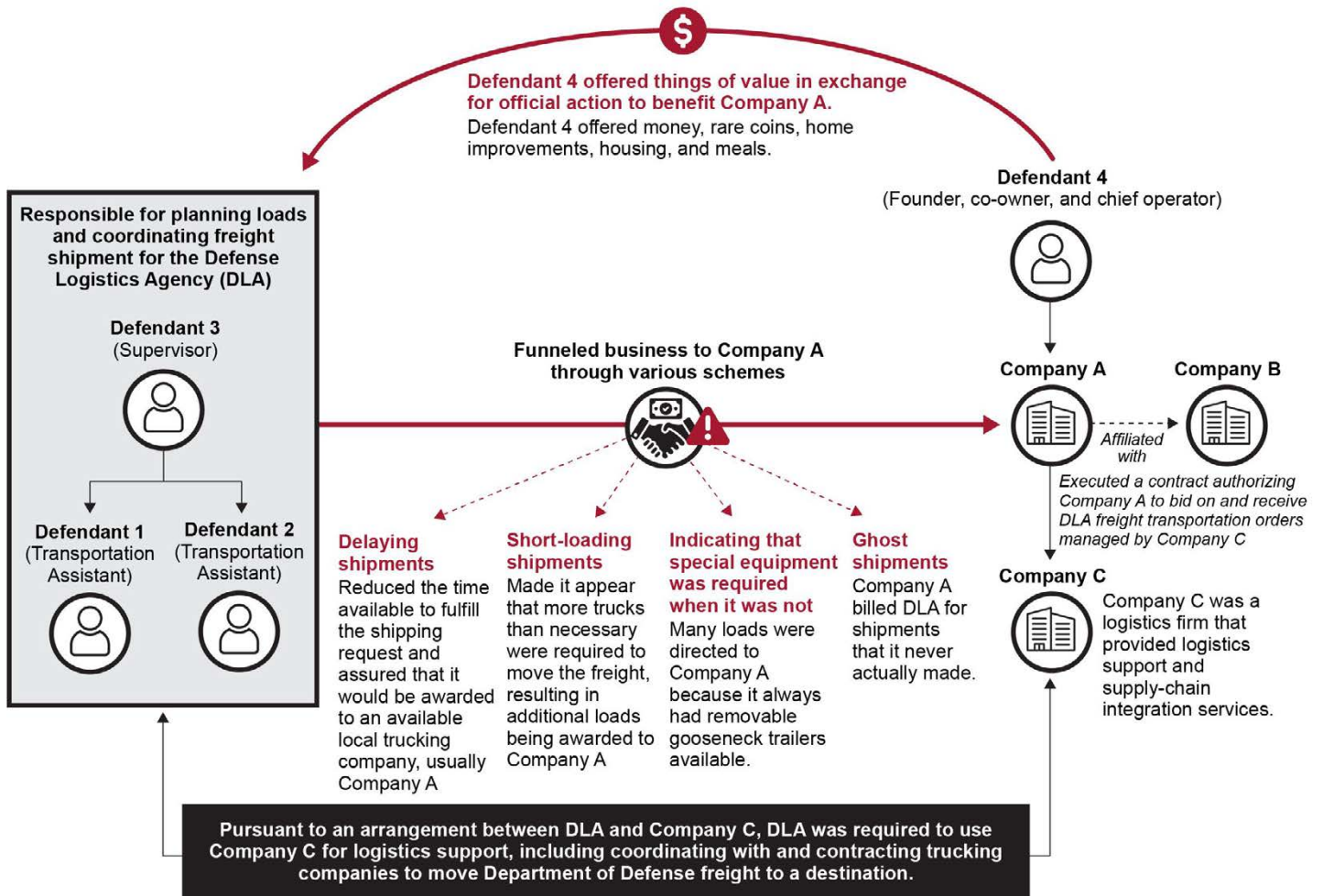
Source: GAO analysis of federal court documents and DOD information. | GAO-24-105358

Note: Suspension refers to the action taken to disqualify a contractor temporarily from government contracting and government-approved subcontracting. A contractor that is disqualified is "suspended." Suspension is an action imposed pending the completion of an investigation or legal proceedings, when it has been determined that immediate action is necessary to protect the government's interests. Debarment refers to an action taken to exclude a contractor from government contracting and government-approved subcontracting for a reasonable, specified period. A contractor that is excluded is "debarred." 48 C.F.R. §§ 2.101 and 9.407-1.

^aThe dollar amounts specified in the financial judgments, for example, the amounts of assessments and restitution, may not reflect the extent of actual fraud that was committed. Because of fraud's deceptive nature, financial losses may not be identified, and such losses are difficult to reliably estimate.

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Figure 21: Case 7 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case



Sources: GAO analysis of federal court documents and Department of Defense information; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Accessible Text for Figure 21: Case 7 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Responsible for planning loads and coordinating freight shipment for Defense Logistics Agency (DLA)

Defendant 3 (Supervisor)

Defendant 1 (Transportation Assistant)

Defendant 2 (Transportation Assistant)

Funneled business to Company A through various schemes

Delaying shipments

Reduced the time available to fulfill the shipping request and assured that it would be awarded to an available local trucking company, usually Company A

Short-loading shipments

Made it appear that more trucks than necessary were required to move the freight, resulting in additional loads being awarded to Company A

Indicating that special equipment was required when it was not

Many loads were directed to Company A because it always had removable gooseneck trailers available.

Ghost shipments

Company A billed DLA for shipments that it never actually made.

Defendant 4 (Founder, co-owner, and chief operator)

Defendant 4 offered things of value in exchange for official action to benefit Company A.

Defendant 4 offered money, rare coins, home improvements, housing, and meals.

Company A

Affiliated with Company B

Executed a contract authorizing Company A to bid on and receive DLA freight transportation orders managed by Company C

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Company C

Company C was a logistics firm that provided logistics support and supply-chain integration services.

Pursuant to an arrangement between DLA and Company C, DLA was required to use Company C for logistics support, including coordinating with and contracting trucking companies to move Department of Defense freight to a destination.

Sources: GAO analysis of federal court documents and Department of Defense information; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Table 10: Case 7 - Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021

Case number: offenses investigated or adjudicated	DCIO	Summary
<p>Case 7:</p> <ul style="list-style-type: none"> • Bribery • Conspiracy to defraud the United States • Destruction of records in federal investigation • Obstruction of an official proceeding • Scheme to deprive the United States of money, property, and honest services by wire fraud • Theft of government property 	<p>Naval Criminal Investigative Service</p>	<p>Fraud scheme: Defendant 1 was a Transportation Assistant in the Traffic Office at the Defense Logistics Agency (DLA), located at the Marine Corps Logistics Base (MCLB) Albany, Georgia. Defendant 1 was responsible for planning loads and coordinating freight shipment for DLA. In 2009, Defendant 1 became the Lead Transportation Assistant in the Traffic Office. Defendant 2 was also a Transportation Assistant in the Traffic Office, working under Defendant 3, who was the supervisor for the Traffic Office. As the supervisor, Defendant 3 was responsible for managing freight shipment for DLA within the United States and abroad. Defendant 3 was also responsible for supervising employees in the Traffic Office who were planning shipments, as well as employees who were responsible for loading freight onto trucks for transport.</p> <p>Defendant 4 was the founder, co-owner, and chief operator of Company A and its affiliated entity, Company B. Company A was a trucking company and transportation broker in Georgia. In 2008, Company A executed a contract with Company C. The contract authorized Company A to bid on and receive DLA freight transportation orders managed by Company C and to service those orders either directly or by brokering them to other trucking companies. Company C was a logistics firm that provided logistics support and supply-chain integration services. In February 2009, Company C and DLA officially implemented the Defense Transportation Coordination Initiative at MCLB-Albany, under which DLA was required to use Company C for logistics support, including coordinating with and contracting trucking companies to move DOD freight to a destination.</p> <p>Defendant 4 identified DLA public officials at MCLB-Albany who could help Company A, including Defendants 1, 2, and 3. Defendant 4 offered and provided these officials with things of value, including money, rare coins, home improvements, housing, and meals, in exchange for official actions to benefit Company A. Specifically, Defendants 1, 2, and 3 defrauded DOD by improperly awarding Company A DLA freight transportation orders. They limited Company C's ability to select any company other than Company A to fill DLA transportation orders and planned overpriced transportation loads through unnecessary shipping specifications and premium-priced-service requirements. In exchange, Defendant 4 gave things of value to Defendant 1 worth approximately \$523,662; gave things of value to Defendant 2 worth approximately \$156,000; and gave things of value to Defendant 3 worth approximately \$209,800.</p>

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Case number: offenses investigated or adjudicated	DCIO	Summary
		<p>More specifically, Defendant 1 and other conspirators, including Defendants 2, 3, and 4, funneled business to Company A through various schemes that resulted in millions of dollars in overcharges to the U.S. government. For example, they delayed and short-loaded shipments. Additionally, they required removable gooseneck trailers when they were not needed and created ghost shipments. Delaying shipments assured that they would be awarded to an available local trucking company, usually Company A. Short-loading shipments referred to the practice of making it appear that more trucks than necessary were required to move the freight, resulting in additional loads being awarded to Company A. Indicating that removable gooseneck trailers were required for a shipment resulted in many loads being directed to Company A because it always had removable gooseneck trailers available. Creating ghost shipments was a practice where Company A billed DLA for shipments that it never actually made.</p> <p>To conceal this fraud, Defendant 4 directed Defendant 5 to alter government paperwork. For example, Defendant 4 instructed Defendant 5 to alter Government Bills of Lading and prepare substitute Company A bills of lading reflecting the unauthorized revised specifications. Defendant 5 also sometimes certified the completion of freight transportation services to DLA and Company C before the shipments were actually delivered.</p> <p>In a separate scheme, Defendant 4 also offered bribes to Defendant 6, a contractor for the Fleet Support Division, in exchange for official action to help identify surplus equipment in serviceable condition and to steal that equipment from MCLB-Albany. Defendant 4 then sold the surplus equipment, including bulldozers, cranes, and front-end loaders.</p> <p>Case origination: This investigation was initiated pursuant to the receipt of a Defense Criminal Investigative Service (DCIS) report regarding a hotline complaint. The anonymous complaint was received originally by GAO's FraudNet hotline, which forwarded it to a DOD hotline. The complaint alleged that a Transportation Security Manager at the Marine Corps Logistics Center in Albany, Georgia, later identified as Defendant 3, received and provided gifts to drivers and a transportation agent in exchange for having the drivers ship freight destined to other bases.</p> <p>Other DCIOs/federal agencies involved: DCIS, Army Criminal Investigation Division, DLA Office of the Inspector General</p> <p>Suspects identified: Eight suspects identified</p> <p>Approximate dates of scheme: 2006-2012</p> <p>Approximate investigative case duration: 2008-2016</p> <p>Remedies/outcome (as indicated in DCIO case file and publicly available court documentation):^a</p> <p>Defendant 1 – Pled guilty to two counts of bribery of a public official. Sentenced to 84 months in prison and 3 years' supervised release. Ordered to pay a total of \$200 in assessments and \$573,662 in restitution. Debarred from government contracting for about 10 years, from 2013 to 2023.</p>

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Case number: offenses investigated or adjudicated	DCIO	Summary
<p>Case 7:</p> <ul style="list-style-type: none"> • Bribery • Conspiracy to defraud the United States • Destruction of records in federal investigation • Obstruction of an official proceeding • Scheme to deprive the United States of money, property, and honest services by wire fraud • Theft of government property 	<p>Naval Criminal Investigative Service</p>	<p>Defendant 2 – Found guilty of 15 counts of a scheme to deprive the United States of money, property, and honest services by wire fraud after a plea of not guilty, with 12 counts dismissed. Found guilty of one count of bribery after a plea of not guilty. Found guilty of one count of obstruction of an official proceeding after a plea of not guilty. Sentenced to 120 months in prison and 3 years’ supervised release. Ordered to pay a \$1,700 assessment and restitution of about \$15,410,152. Defendant 2 and Defendant 2’s construction company were debarred from government contracting for about 16 years, from 2014 to 2030.</p> <p>Defendant 3 – Pled guilty to two counts of bribery of a public official. Sentenced to 96 months in prison and to 3 years’ supervised release. Ordered to pay a total of \$200 in assessments and \$284,808 in restitution. Debarred from government contracting for about 14 years, from 2013 to 2027..</p> <p>Defendant 4 – Found guilty on all 54 counts after a plea of not guilty. Found guilty of 43 counts of a scheme to deprive the United States of money, property, and honest services by wire fraud; five counts of bribery; one count of theft of government property; four counts of obstruction of an official proceeding; and one count of destruction of records in a federal investigation. Sentenced to 264 months in prison and 3 years’ supervised release. Ordered to pay a \$5,400 assessment and restitution of about \$18,860,314. Defendant 4 and Defendant 4’s company were debarred from government contracting for about 28 years, from 2014 to 2042.</p> <p>Defendant 5 – Pled guilty to one count of conspiracy to defraud the United States. Sentenced to 6 months in prison and 3 years’ supervised release. Ordered to pay a \$100 assessment and restitution of \$905,685. Debarred from government contracting for about 5 years, from 2014 to 2019.</p> <p>Defendant 6 – Found guilty on all 15 counts after a plea of not guilty. Found guilty of 13 counts of a scheme to deprive the United States of money, property, and honest services by wire fraud; one count of bribery; and one count of theft of government property. Sentenced to 60 months in prison and 3 years’ supervised release. Ordered to pay a \$1,500 assessment and restitution of \$513,600. Defendant 6 and Defendant 6’s company were debarred from government contracting for about 11 years, from 2014 to 2025</p>

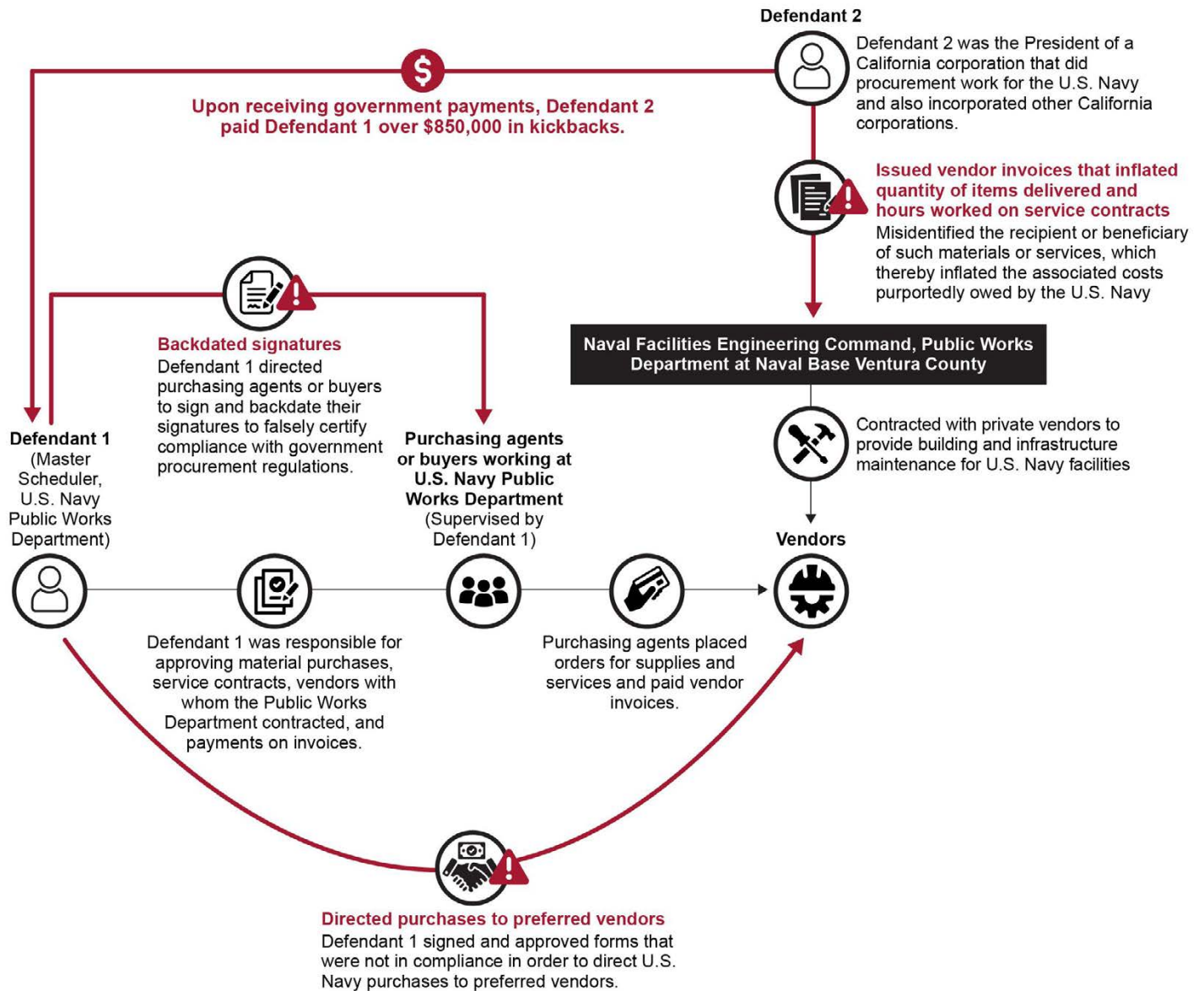
Source: GAO analysis of federal court documents and Department of Defense information. | GAO-24-105358

Note: Debarment refers to an action taken to exclude a contractor from government contracting and government-approved subcontracting for a reasonable, specified period. A contractor that is excluded is “debarred.” 48 C.F.R. § 2.101.

^aThe dollar amounts specified in the financial judgments, for example, the amounts of assessments and restitution, may not reflect the extent of actual fraud that was committed. Because of fraud’s deceptive nature, financial losses may not be identified, and such losses are difficult to reliably estimate.

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Figure 22: Case 8 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case



Sources: GAO analysis of federal court documents and Department of Defense information; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Accessible Text for Figure 22: Case 8 Summary of Procurement Fraud Scheme from Defense Criminal Investigative Organization Case

Defendant 1 (Master Scheduler, U.S. Navy Public Works Department)

Defendant 1 was responsible for approving material purchases, service contracts, vendors with whom the Public Works Department contracted, and payments on invoices.

Purchasing agents or buyers working at U.S. Navy Public Works Department (Supervised by Defendant 1)

Purchasing agents placed orders for supplies and services and paid vendor invoices.

Vendors

Naval Facilities Engineering Command, Public Works Department at Naval Base Ventura County

Contracted with private vendors to provide building and infrastructure maintenance for U.S. Navy facilities

Backdated signatures

Defendant 1 directed purchasing agents or buyers to sign and backdate their signatures to falsely certify compliance with government procurement regulations.

Defendant 1 signed and approved forms that were not in compliance in order to direct U.S. Navy purchases to preferred vendors.

Misidentified the recipient or beneficiary of such materials or services, which thereby inflated the associated costs purportedly owed by the U.S. Navy

Defendant 2

Defendant 2 was the President of a California corporation that did procurement work for the U.S. Navy and also incorporated other California corporations.

Upon receiving government payments, Defendant 2 paid Defendant 1 over \$850,000 in kickbacks.

Sources: GAO analysis of federal court documents and Department of Defense information; Icons-Studio/stock.adobe.com (icons). | GAO-24-105358

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Table 11: Case 8 - Summary of Defense Criminal Investigative Organization (DCIO) Procurement Fraud Case Closed between Fiscal Years 2015 and 2021

Case number: offenses investigated or adjudicated	DCIO	Summary
<p>Case 8:</p> <ul style="list-style-type: none"> • Acceptance of bribes • Conflicts of interest • Conspiracy to commit bribery • Conspiracy to defraud the United States, submit false claims, and commit bribery • False, fictitious, and fraudulent claims against the United States • False statement • Subscription to false tax returns 	<p>Naval Criminal Investigative Service</p>	<p>Fraud scheme: Defendant 1 was the Master Scheduler for the Naval Facilities Engineering Command, Public Works Department, at Naval Base Ventura County. The Public Works Department was responsible for facilities maintenance and management and would occasionally contract with private vendors to provide building and infrastructure. As Master Scheduler, Defendant 1 was responsible for approving material purchases, service contracts, vendors with whom the Public Works Department contracted, and payments on invoices. Defendant 1 supervised the Public Works Department purchasing agents (also known as buyers or Government Purchase Card (GPC) holders), who interacted directly with Public Works Department vendors, placed orders for supplies and services, and paid vendor invoices. Defendant 1 also incorporated and operated a company in California and purchased 85 percent of another company's shares.</p> <p>A conspirator included a relative of Defendant 1 who was also the Chief Executive Officer of a California company engaged in the plumbing, heating, and air-conditioning business. Defendant 2 was another conspirator and was the President of a California company that did procurement work for the U.S. Navy and also incorporated other California companies.</p> <p>Defendants 1 and 2, along with another conspirator (Defendant 1's relative) and other unknown conspirators, engaged in the scheme to defraud the U.S. Navy. Specifically, Defendant 1 signed and approved Material Request Forms and Government Purchase Card Requisition Forms (GPCR) that were not in compliance with Government Procurement Regulations in order to direct U.S. Navy purchases to preferred vendors. Defendant 1 backdated the signature on GPCRs to make it falsely appear as if the GPCRs had been properly authorized through the required process. Defendant 1 also directed conspirator GPC holders to sign and backdate their signatures on GPCRs to falsely certify compliance with government procurement regulations.</p> <p>Conspirators, including Defendant 2, along with other unknown conspirators, caused the issuance of vendor invoices that inflated the quantity of items delivered and the hours worked on service contracts and misidentified the recipient or beneficiary of such materials or services, which thereby inflated the associated costs purportedly owed by the U.S. Navy. Conspirators' companies also failed to supply material or services in response to GPCRs but still issued invoices requesting the U.S. Navy to provide payment. The conspirators also used GPC numbers, expiration dates, and credit card verification numbers, given to them by Defendant 1, to implement charges to GPC accounts. Upon receiving government payments, Defendant 2 paid Defendant 1 kickbacks in cash or issued checks payable to one of Defendant 1's companies. From 2011 to 2014, Defendant 2 paid over \$850,000 in kickbacks to Defendant 1's companies.</p>

**Appendix II: Summary of Eight Selected
Defense Criminal Investigative Organization
Procurement Fraud Cases**

Case number: offenses investigated or adjudicated	DCIO	Summary
<p>Case 8:</p> <ul style="list-style-type: none"> • Acceptance of bribes • Conflicts of interest • Conspiracy to commit bribery • Conspiracy to defraud the United States, submit false claims, and commit bribery • False, fictitious, and fraudulent claims against the United States • False statement • Subscription to false tax returns 	<p>Naval Criminal Investigative Service</p>	<p>Case origination: Homeland Security Investigations and the Naval Criminal Investigative Service initiated this investigation based on an anonymous tip that Defendant 1 had been embezzling funds from the Naval Facilities Engineering Command Southwest, Public Works Department.</p> <p>Other DCIOs/federal agencies involved: Homeland Security Investigations; Defense Criminal Investigative Service; Internal Revenue Service; FBI</p> <p>Suspects identified: Two suspects identified</p> <p>Approximate dates of scheme: 2008-2014</p> <p>Approximate investigative case duration: 2013-2019</p> <p>Remedies/outcome (as indicated in DCIO case file and publicly available court documentation):^a</p> <p>Defendant 1 – Pled guilty to one count of conspiracy to defraud the United States, submit false claims, and commit bribery and one count of subscription to false tax returns. Sentenced to 70 months in prison and 2 years’ supervised release. Ordered to pay a \$200 special assessment and about \$1,077,718 restitution. Defendant 1 and Defendant 1’s companies were debarred from government contracting for almost 9 years, from 2019 to 2028.</p> <p>Defendant 2 – Pled guilty to one count of conspiracy to commit bribery. Sentenced to 18 months in prison and 2 years’ supervised release. Ordered to pay a \$100 special assessment and \$846,150 restitution. Defendant 2 and Defendant 2’s companies were debarred from government contracting for about 3 years, from 2019 to 2022</p>

Source: GAO analysis of federal court documents and Department of Defense information. | GAO-24-105358

Note: Debarment refers to an action taken to exclude a contractor from government contracting and government-approved subcontracting for a reasonable, specified period. A contractor that is excluded is “debarred.” 48 C.F.R. § 2.101.

^aThe dollar amounts specified in the financial judgments, for example, the amounts of assessments and restitution, may not reflect the extent of actual fraud that was committed. Because of fraud’s deceptive nature, financial losses may not be identified, and such losses are difficult to reliably estimate.

Appendix III: Department of Defense Reporting to Congress on Procurement Fraud

In the past, Congress has requested and mandated that the Department of Defense (DOD) describe and quantify procurement fraud. In responding, DOD has used Defense Criminal Investigative Organization (DCIO) data in some of those instances. Specifically, in 2022, DOD was asked to report to Congress on the total value and quantity of contracts in which DOD entered with contractors indicted for, settled charges of, been fined by any federal department or agency for, or convicted of fraud in connection with any contract or other transaction with the federal government.¹ Additionally, in 2017 and 2009, DOD was mandated and requested, respectively, to report to Congress regarding various procurement fraud matters.²

DOD Response to Request from Congress on Audit Progress and Fraud Prevention (October 2022)

In July 2022, two U.S. Senators asked DOD to provide an assessment of the total value and quantity of contracts entered into for the previous 5 fiscal years with contractors that have been

- indicted for,
- settled charges of,
- been fined by any federal department or agency for, or
- have been convicted of fraud in connection with any contract or other transaction with the federal government.

¹Bernard Sanders, U.S. Senator, and Charles E. Grassley, U.S. Senator, letter to the Honorable Lloyd J. Austin III, Secretary, Department of Defense (July 27, 2022).

²National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Div. A, § 889, 131 Stat. 1283, 1508 (2017) and 155 Cong. Rec. H15007-02, H15043 (daily ed. Dec. 16, 2009).

In a response dated October 2022, DOD acknowledged the importance of assessing the total awards by contractor against its related settlements.³ DOD noted that this assessment is particularly important, as it relates to fraud, but stated that the data are not centralized within DOD. Furthermore, the response did not provide specific numbers regarding the request for an assessment of the total value and quantity of contracts. However, it did note that the DOD Office of Inspector General (OIG) could provide financial recovery amounts for cases in which the Defense Criminal Investigative Service was the lead investigative agency.

Report to Congress on Defense Contracting Fraud (December 2018)

The National Defense Authorization Act for Fiscal Year 2018 required that DOD submit to Congress a report on contracting fraud. The report was to include

- (1) a summary of fraud-related criminal convictions and civil judgments or settlements over the previous 5 fiscal years;
- (2) a listing of contractors that within the previous 5 fiscal years had performed contracts for DOD and were debarred or suspended from federal contracting based on a criminal conviction for fraud;
- (3) an assessment of the total value of DOD contracts entered into during the previous 5 fiscal years with contractors that have been indicted for, settled charges of, been fined by any federal department or agency for, or been convicted of fraud in connection with any contract or other transaction entered into with the federal government; and
- (4) recommendations by the DOD OIG or other appropriate DOD official regarding how to penalize contractors repeatedly involved in fraud in connection with contracts or other transactions entered into with the federal government, including an update on implementation by DOD of any previous such recommendations.

³Department of Defense, *DOD Audit Progress and Fraud Prevention*, Letters to Bernard Sanders, U.S. Senator, and Charles E. Grassley, U.S. Senator (Oct. 27, 2022).

**Appendix III: Department of Defense Reporting
to Congress on Procurement Fraud**

DOD submitted a report in December 2018 addressing the above requests and covering a reporting period from fiscal years 2013 to 2017.⁴ To develop the report, DOD obtained data from sources including the DCIOs, DOD OIG, the Department of Justice (DOJ), and the Federal Procurement Data System—Next Generation (FPDS-NG).⁵ In response to the reporting requirements, DOD reported that

- there were 1,059 cases resulting in 1,087 criminal convictions, from which \$368,670,055 was recovered in fines and penalties; \$370,194,702 was recovered through restitution, and \$53,361,358 was recovered through forfeiture of property. During the 5-year reporting period, there were 443 cases resulting in civil judgments or settlements, resulting in \$5,858,180,290 recovered (see table 12).

Table 12: Recovered Funds from Department of Defense (DOD) Contracting Fraud Cases from Fiscal Years 2013 to 2017, as Reported in 2018

Category	Number of DOD's contracting fraud cases resulting in monetary judgments	Amount of recoveries (in USD)
Criminal conviction	1,059	<ul style="list-style-type: none"> • 368,670,055 in fines and penalties • 370,194,702 in restitution • 53,361,358 in property forfeiture
Civil judgments and settlements	443	5,858,180,290

Source: Department of Defense 2018 Report to Congress on Defense Contracting Fraud. | GAO-24-105358

- during the relevant 5-year period, there were nine contractor entities that performed contracts for DOD and were debarred or suspended from federal contracting based on a criminal conviction for fraud. These nine entities performed 469 contract actions, with a net contract value of negative \$1,529,965.73 as a result of contract terminations and de-obligations following criminal conviction;
- there were 168 contractors that fell into the third reporting category, totaling 15,963,513 contract actions, with total contract obligations valued at \$334,305,246,152. Of these contract actions, 94 percent were from one contractor entity, and 76 percent of the total contract obligations were from two major defense companies. The remaining

⁴Department of Defense, *Report to Congress: Section 889 of the FY 2018 NDAA Report on Defense Contracting Fraud* (Dec. 20, 2018).

⁵ FPDS-NG is a comprehensive, web-based tool for agencies to report procurement contract actions; it contains a searchable database of contract information that provides a capability to examine data across government agencies.

165 contractors accounted for 4 percent of the total contract actions and 24 percent of the total contract obligations; and

- that the DOD OIG does not recommend specific penalties for contractors involved in fraud on contracts or other transactions. However, DOD OIG reports have consistently made recommendations seeking refunds for contract overpayments; identifying needs to renegotiate contracts; improving competition; identifying whether DOD received fair and reasonable pricing; and addressing suspension and disbarment, as appropriate. Furthermore, DOD OIG reports that find inappropriate actions on the part of DOD employees may also recommend that management consider all appropriate administrative remedies available.

DOD officials explained to us that they encountered challenges in developing the 2018 report to Congress. Identified challenges included obtaining, compiling, and analyzing the data. Officials told us that data were compiled from DOJ and the DCIOs, manually reviewed, and queried against systems such as the System for Award Management and the FPDS-NG. Data were obtained from 54 DOJ U.S. Attorneys' Offices, and these offices captured data differently than the DCIOs, making analysis challenging. Additionally, DOJ did not have a central database repository to record criminal convictions and civil penalties involving procurement fraud, and DOD components all have separate reporting processes. Officials also noted challenges related to data input errors. For example, when querying a DCIO case management system using keyword searches, officials encountered data input errors related to certain data fields that were relevant to the data request. Officials also pointed out that, since many cases are investigated jointly with other investigative entities, there may be multiple cases open against one individual, meaning that the DCIO data had to be compared against the DOJ data to avoid double-counting cases of fraud.

Report to Congress on Contracting Fraud (October 2011)

In 2009, the Explanatory Statement accompanying the Department of Defense Appropriations Act, 2010, contained a provision for DOD to conduct a study on defense contracting fraud and to submit a report containing the findings of the study to the congressional defense

committees.⁶ The report was to contain an assessment of the total value of DOD contracts entered into with contractors that had been indicted for, settled charges of, been fined by any federal department or agency for, or been convicted of fraud in connection with any contract or other transaction entered into with the federal government over the past 10 years. The report was also to include recommendations regarding how to penalize contractors who are repeatedly involved in contract fraud allegations.

DOD submitted a report in October 2011 addressing the above requests and covering a reporting period from fiscal years 2001 to 2010.⁷ To develop the report, DOD obtained data from DOJ, the DCIOs, and FPDS.

- Regarding criminal convictions, DOJ identified 54 DOD contractor companies that were criminally charged with fraudulent practices over the 10-year reporting period. The funds obligated to these contractors subsequent to conviction and total funds obligated for the 10-year period were \$33,079,743 and \$254,503,167, respectively. DOD also reported that the DCIOs identified additional contractors that were criminally convicted of fraud during the period between 2007 and 2009 but were not included in the DOJ database; the total amount obligated to those contractors subsequent to the convictions was \$61,414.
- Regarding civil settlements and judgments, DOD reported that for the 10-year reporting period, DOJ identified more than 300 DOD companies that entered into settlement agreements or had civil judgments rendered against them. The dollars obligated to these contractors subsequent to the settlement or judgment, and the total dollars obligated to them over the 10-year period, totaled \$398,081,775,397 and \$572,870,228,456, respectively. DOD also reported additional contractors for the 2007-2009 period that met the reporting criteria but were not in the DOJ database; these additional contractors were identified in the DCIO data. The dollars obligated to these contractors subsequent to settlement or judgment were \$822,867,482.

⁶155 Cong. Rec. H15007-02, H15043. Under section 1014 of the Department of Defense Appropriations Act, 2010, the Explanatory Statement of the Chairman of the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives, as printed in the Congressional Record, serves as the Conference Report's Joint Explanatory Statement. Department of Defense Appropriations Act, 2010, Pub. L. No. 111-118, Div. B § 1014, 123 Stat. 3409, 3474 (2009).

⁷Department of Defense, *Report to Congress on Contracting Fraud* (October 2011).

- Regarding recommendations for penalties for contractors who are repeatedly involved in contract fraud allegations, DOD reported that there are existing remedies available that include criminal and civil penalties and contractual and administrative remedies. DOD reported, however, that its main efforts were focused on detection and prevention and that DOD would be taking actions to increase awareness and training with regard to fraudulent contracting acts.
- Regarding the actions DOD has taken to strengthen its policies and safeguards against contractor fraud, DOD reported that it had initiated several efforts. Among other actions, the report stated that DOD had established a Panel on Contracting Integrity and a Procurement Fraud Working Group. The purpose of the panel was to review DOD's progress to eliminate vulnerabilities in the contracting system that allow fraud, waste, and abuse and to recommend changes in law, regulations, and policy. The Procurement Fraud Working Group was established to provide a DOD-wide and interagency forum of information exchange, legislative and policy development, and continuing education with regard to current issues, future trends, investigative strategies, and appropriate remedies and enforcement problems in the procurement fraud arena.

DOD noted several challenges with developing this report to Congress. For example, the report stated that there were initial challenges associated with the contracts awarded by other federal departments or agencies. Based in part on this challenge and as discussed in its report, DOD decided to use data obtained through DOJ for the 10-year period. DOD obtained data on fraud-related actions for the 10-year period from DOJ and the associated obligation data from FPDS.

DOD also reported additional challenges related to obtaining complete data and analyzing the data. Differences in the DOJ and DCIO case management systems may explain why some relevant cases identified in the DCIO data may not have been included in the data provided by DOJ. Specifically, the DOJ case management system does not identify defendants by their status as government contractors and may not identify certain cases as fraud cases due to the method of categorizing cases in that system. For example, a case categorized as bribery, rather than procurement fraud, may not have been captured in the data DOJ provided. DOD reported that ensuring that all cases involving fraud were reported would require opening thousands of case files, which was not feasible, given time and resource limitations.

Additionally, in the report, DOD expressed concerns with analyzing the data over a 10-year period, during which contractors may have merged, changed names, or dissolved. The DOJ data did not contain the physical address associated with the contracting entities or the Dun and Bradstreet Data Universal Numbering System (DUNS) identifier that is used in the federal contracting process to identify contractors.⁸ DOD reported that they relied on the entity names provided in the DOJ data to search for obligation data. Without the DUNS identifier, it was difficult for DOD to guarantee that all data associated with a particular entity was captured. Furthermore, it was possible that an entity may have been erroneously included in the data collection.

⁸On April 4, 2022, the federal government stopped using the DUNS number to uniquely identify entities. Entities doing business with the federal government now use the Unique Entity ID created in SAM.gov.

Appendix IV Comments from the Department of Defense

**Appendix IV Comments from the Department
of Defense**



COMPTROLLER

OFFICE OF THE UNDER SECRETARY OF DEFENSE

1100 DEFENSE PENTAGON
WASHINGTON, DC 20301-1100

January 30, 2024

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

Dear Mr. Bagdoyan:

Enclosed is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report GAO-24-105358SU, "DOD FRAUD RISK MANAGEMENT: Enhanced Data Analytics Can Help Manage Fraud Risks," dated January 2024 (GAO Code 105358).

We appreciate the opportunity to provide comments. My point of contact is Ms. Angela Palma (angela.d.palma2.civ@mail.mil or 571-516-4363).

Sincerely,

STEFFENS.THOMA
S.CHARLES.10293
42870

Digitally signed by
STEFFENS THOMAS CHARLES
1029342870
Date: 2024.01.30 15:09:31 -0500

Thomas C. Steffens
Deputy Chief Financial Officer

Enclosure:
Consolidated DoD Response to GAO 105358

**Appendix IV Comments from the Department
of Defense**

**GAO DRAFT REPORT DATED JANUARY 1, 2024
GAO-24-105358SU (GAO CODE 105358)**

**“DoD FRAUD RISK MANAGEMENT: Enhanced Data Analytics Can Help Manage
Fraud Risks”**

**DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS**

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense should ensure that the Under Secretary of Defense (Comptroller) revises DoD’s Fraud Risk Management Strategy to establish data analytics as a method for preventing, detecting, and responding to fraud.

DoD RESPONSE: Respectfully non-concur. Below are examples and references for where DoD has already accomplished the work reflected the recommendation. In the DoD’s Fraud Risk Management Strategy, the Under Secretary of Defense (Comptroller) has established data analytics as a method for preventing, detecting, and responding to fraud.

As an example, the DoD Fraud Risk Strategy states (page 4) the “DoD is subject to requirements in the Payment Integrity Information Act of 2019 (PIIA).” The Strategy also states (page 1) the PIIA “requires and encourages agencies to use data analytics to identify, prevent, and respond to fraud and adopt an anti-fraud culture within their programs.” Page 6 reiterates that “DoD’s FRM Strategy defines activities for assessing, identifying, and managing fraud risks based on the requirements of the PIIA and OMB, considering the leading practices outlined in the GAO Framework.”

Additionally, the Strategy (page 11) says “Components should develop fraud analytics based on high-risk areas identified through the Fraud Risk Assessment.” It notes components “should produce actionable results from analytics, measurable fraud reduction outcomes, and other implementation activities to reduce fraud.”

Page 24 of the draft report states “Strategy generally refers to data analytics activities but does not discuss what or how data analytics are to be used. For example, designing and implementing edit checks, data matching, and data mining; combining data across programs to facilitate analytics; and pursuing access to external data.” However, the DoD Strategy already includes examples of techniques in the list of Fraud Control Activities. Specifically, Principle 6 (page 24) highlights that “Management performs data activities to help with fraud risk management including data mining and data matching techniques.”

Notably, the Department is already employing data analytics. For example, the Defense Finance and Accounting Service (DFAS) utilizes the Advana Improper Payment Detection (IPD) tool for the early identification and prevention of improper payments for seven entitlement systems. Daily, these entitlement systems send prepayment invoice files to the Advana tool, where they run through a series of business rules called Integrity Checks. The prepayment checks look for key indicators to prevent duplicate payments, overpayments, wrong vendor payments and

**Appendix IV Comments from the Department
of Defense**

various types of recoupment errors. If an invoice from the daily file meets the criteria of an Integrity Check, it will flag a ticket in the Advana IPD tool for a DFAS technician to manually review. Technicians review tickets within 24 hours of flagging, and if paying the invoice would lead to an improper payment, the technician will initiate corrective action in the source system to prevent the invoice from disbursing. This tool has prevented the improper payment of over \$14 billion in total since inception. DoD 7000.14-R, Financial Management Regulation, Volume 4, Chapter 14 “Payment Integrity,” September 2023, outlines payment integrity processes and requires DoD Components to implement PIIA.

Of note, the Office of the Under Secretary of Defense (Comptroller) (OUSD(C)) uses two fraud data analytics tools within Advana; the Deputy Chief Financial Officer (DCFO) Risk Management and Internal Control (RMIC) Team developed the Fraud Risk Register dashboard, which is an aggregation of fraud risks submitted through the Statement of Assurance (SOA) Program where Components are required to assess the risk of fraud when conducting their annual risk assessment. Components utilize a risk-based approach to identify, assess, and understand potential fraud risks and take appropriate action to mitigate them. Please note that fraud risks relate to a list of areas identified by the PIIA, and the Office of Management and Budget (OMB). DCFO utilizes the highest priority fraud risks with Department-wide impact to drive internal control testing efforts. Additionally, the RMIC Team has developed the Fraud Controls Matrix dashboard which displays the fraud risk control assessments submitted through the SOA Program. The inputs were also aligned with the leading practices from GAO’s FRM Framework.

Finally, besides the Fraud Risk Management Strategy, two recent Secretary of Defense memoranda have stressed the importance of implementing enterprise risk management and strengthening the internal control environment. The memoranda are: “Expectations for Supporting Department of Defense Financial Statement Audits,” dated October 13, 2023, and “Fiscal Year 2024 Financial Statement Audit Priorities,” dated November 30, 2023. Both set strong and committed tone-at-the-top expectations for effective DoD financial management.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense should ensure that the Under Secretary of Defense (Comptroller) identifies and documents in DoD’s Fraud Risk Management Strategy which entity has the necessary authority to ensure that fraud-related data analytics activities are planned and implemented.

DoD RESPONSE: Respectfully non-concur, as the Strategy already identifies the entity responsible for planning and implementing fraud-related data analytics activities. The Strategy (page 9) defines OUSD(C)/Enterprise Financial Transformation (EFT) as the entity for leading data analytics efforts and to provide the analytics infrastructure for fraud risk management analytics products. Further, the Strategy (page 10) cites the Fraud Reduction Task Force as leading the Department’s analytic activities for high-priority risks. The Task Force is the cross-enterprise strategic team of subject matter experts, which includes internal controls and analytics representatives from each PSA and Component of the DoD (page 9).

Appendix IV Comments from the Department of Defense

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense should ensure that the Under Secretary of Defense (Comptroller) revises DoD’s Fraud Risk Management Strategy to clarify and document roles and responsibilities related to data analytics activities.

DoD RESPONSE: Respectfully non-concur, based on the Strategy (page 9) already defining OUSD(C)/EFT as the entity responsible for leading data analytics efforts and providing the analytics infrastructure for fraud risk management analytics products. Further, the Strategy (page 10) cites the Fraud Reduction Task Force as leading the Department’s analytic activities for high-priority risks. The Task Force is the cross-enterprise strategic team of subject matter experts, which includes internal controls and analytics representatives from each Principal Staff Assistant (PSA) and Component of the DoD (page 9).

The DoD Fraud Risk Management Strategy states up front (page 1) [the PIIA] “requires and encourages agencies to use data analytics to identify, prevent, and respond to fraud and adopt an anti-fraud culture within their programs.” To emphasize this, page 4 documents: “DoD is subject to requirements in the Payment Integrity Information Act of 2019 (PIIA).”

Additionally, the Strategy (page 11) directs “Components should develop fraud analytics based on high-risk areas identified through the Fraud Risk Assessment.” It further says components, “should produce actionable results from analytics, measurable fraud reduction outcomes, and other implementation activities to reduce fraud.”

Components have been advised to develop analytics to assist with fraud detection and take corrective action to remediate. At a minimum, Components are required to identify fraud risks related to a list of areas identified by the Fraud Reduction and Data Analytics Act of 2015 (FRDAA), PIIA, and OMB.

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense should ensure that the Under Secretary of Defense (Comptroller) incorporates and documents timelines for designing and implementing data analytics activities into Fraud Risk Management Strategy.

DoD RESPONSE: Respectfully non-concur, given timelines for designing and implementing data analytics activities are already included in the DoD Fraud Risk Management Strategy. Figure 4 on page 16 provides a timeline for fraud risk management activities. The schedule includes dates for the aggregation of fraud risks and GAO FRM Framework assessments to begin. The assessments include the following direction:

Per the GAO FRM Framework, [Management] collects and analyzes data on fraud trends and control deficiencies, a process that reflects the “lessons learned” element of monitoring and evaluation.

Additionally, Fraud Principle 6 in the Strategy (pages 23 and 24) states “[Management] performs data analytics activities to help with fraud risk management including data mining and data matching techniques.”

**Appendix IV Comments from the Department
of Defense**

Lastly, the Strategy also includes the requirement of timelines in the list of Fraud Control Activities. Specifically, Principle 5 (page 23) states, “Management has created timelines for implementing fraud risk management activities, as appropriate, including monitoring and evaluations.”

RECOMMENDATION 5: The GAO recommends that the Inspector General of DoD should improve the usability of its procurement fraud investigative data for fraud risk management purposes. Specific actions should include ensuring that data in structured fields are complete, accessible, and readily subject to analysis and aggregation.

DoD RESPONSE: The Inspector General of the Department of Defense’s response has been provided directly to GAO and is not included herein.

RECOMMENDATION 6: The GAO recommends that the Secretary of the Air Force, in collaboration with the Inspector General of DoD and the other military departments, should improve the usability of its respective procurement fraud investigative data by DoD for fraud risk management purposes. Specific action should include ensuring data in structured fields are complete, accessible, and readily subject to analysis and aggregation.

DoD RESPONSE: The Secretary of the Air Force, Inspector General (SAF/IG) partially concurs with the one recommendation made to the Secretary of the Air Force (Recommendation 6, page 71 of the Draft GAO report). Not all data in structured fields should be required to be completed. Not all fields are relevant to every case or case type. SAF/IG concurs key fields for procurement fraud investigations should be required to be completed, and a review of structured fields will be completed by Headquarters Air Force Office of Special Investigations (AFOSI) to identify required fields.

Additionally, SAF/IG is submitting critical comments for its Technical Review of the draft report as it mischaracterizes information provided by AFOSI. The report also inaccurately captures datapoints previously clarified and provided by AFOSI during their engagements with the GAO between 6 Aug 21 – 30 Nov 23. SAF/IG provides the following general observations driving this non-concur and welcomes the opportunity for further discussion with the GAO. For additional technical issues related to this draft report, please see attachment Comments Resolution Matrix (Tab 2). AFOSI also conducted a Security-Sensitivity Review of this draft report and found no issues.

AFOSI acknowledges there are limitations with AFOSI’s current case management system, Investigative Information Management System (I2MS), regarding collecting and aggregating data for fraud cases; however, AFOSI does not agree with GAO’s interpretation of the data provided, nor can AFOSI validate the report findings without understanding which AFOSI cases were included and excluded from analysis. Further, AFOSI is moving to a new case management system, ORION, which is currently in its roll-out phase with a full implementation target date of 31 Mar 24. ORION will address many of the issues raised in this report, to include collecting data related to fraud schemes and more accurate collection of disposition data.

**Appendix IV Comments from the Department
of Defense**

Additionally, AFOSI previously provided written responses to GAO's questions; however, many of these were not accurately captured in the current report and in some cases, the report directly contradicted the information provided by AFOSI. During previous engagements with the GAO, AFOSI representatives worked to assist GAO in understanding and correctly interpreting the data in the format exported from AFOSI systems. These efforts included discussions with agents and case management system administrators, as well as a case management system demonstration. Despite these efforts, the report does not accurately reflect the provided information.

RECOMMENDATION 7: The GAO recommends that the Secretary of the Army, in collaboration with the Inspector General of DoD and the other military departments, should improve the usability of its respective procurement fraud investigative data by DoD for fraud risk management purposes. Specific actions should include ensuring data in structured fields are complete, accessible, and readily subject to analysis and aggregation.

DoD RESPONSE: Concur. The Secretary of the Army, in collaboration with the Inspector General of DoD and the other Military Departments, will improve the usability of its respective procurement fraud investigative data by DoD for fraud risk management purposes. Specific actions will include ensuring data in structured fields are complete, accessible, and readily subject to analysis and aggregation.

RECOMMENDATION 8: The GAO recommends that the Secretary of the Navy, in collaboration with the Inspector General of DoD and the other military departments, should improve the usability of its respective procurement fraud investigative data by DoD for fraud risk management purposes. Specific action should include ensuring data in structured fields are complete, accessible, and readily subject to analysis and aggregation.

DoD RESPONSE: Non-Concur. NCIS non concurs with the report as written and provides the following general issues with the report. However, NCIS is willing to change the non-concur to concur if the specific items outlined in the attached "Comments Resolution Matrix" are addressed (Tab 3).

NCIS concurs there are limitations with its case management system, Consolidated Law Enforcement Operations Center (CLEOC), regarding collecting and aggregating data for procurement fraud cases; however, NCIS does not agree with GAO's interpretation of the data provided, nor can NCIS validate the report findings without access to the final data set (which was not provided to NCIS) used for GAO's analysis.

NCIS provided written responses to a number of GAO's questions and participated in multiple conversations with GAO to assist their analysis of the requested data. Despite the collaboration, GAO's interpretation of the data is not accurately captured in the GAO report. During one in-person meeting, requested by NCIS, GAO personnel were painstakingly briefed on the original data set by NCIS representatives, in an effort to explain the correct interpretation of multiple rows and columns, which aggregate the complete mosaic depicting how an investigative data should be interpreted. Despite these efforts, there appeared to be residual confusion from GAO on how to properly read and interpret the data provided.

**Appendix IV Comments from the Department
of Defense**

RECOMMENDATION 9: The GAO recommends that the Comptroller should collaborate with the Inspector General of DoD and Secretaries of the Navy, Air Force, and Army, respectively, to obtain and analyze relevant information from closed adjudicated procurement fraud cases.

DoD RESPONSE: Concur. Comptroller will collaborate with the Department of Defense Office of Inspector General, and Secretaries of the Navy, Air Force, and Army to obtain and analyze relevant information from closed adjudicated procurement fraud cases.

RECOMMENDATION 10: The GAO recommends that the Secretary of Defense should ensure that the Under Secretary of Defense (Comptroller) revises DoD's Fraud Risk Management Strategy to obtain and analyze relevant information from closed alleged and adjudicated procurement fraud cases from the Defense Criminal Investigative Organizations.

DoD RESPONSE: Concur. OUSD(C) will revise DoD's Fraud Risk Management Strategy to obtain and analyze relevant information from closed alleged and adjudicated procurement fraud cases from the Defense Criminal Investigative Organizations and Secretaries of the Navy, Air Force, and Army.

Currently, the 2023 DoD FRM Strategy (page 11) assigns the Components the responsibility to review and mitigate potential fraud cases and to provide feedback on fraud reduction efforts to improve the DoD-wide fraud analytics framework. Further, the Strategy (pages 10 and 11) lists that the Fraud Reduction Task Force is responsible for producing actionable results from analytics, measurable fraud reduction outcomes, and other implementation activities to reduce fraud.

Lastly, the OUSD(C) regularly collaborates with Defense Criminal Investigative Organizations. For instance, the OUSD(C) Financial Management Policy and Reporting Directorate works with the Procurement Fraud Working Group and the Deputy Chief Information Officers to identify and define confirmed fraud. Additionally, the Defense Criminal Investigative Service presented during the monthly Fraud Reduction Task Force office hours held in June 2023. Earlier in the year, OUSD(Acquisition and Sustainment), Defense Pricing and Contracting Office, and the DoD Office of General Counsel presented during the 2023 OUSD(C) and Office of the Director of Administration and Management jointly-held the RMIC Townhall.

RECOMMENDATION 11: The Inspector General of DOD should collaborate, as appropriate, with the military departments and relevant stakeholders, on the development of leading practices towards improving the usability of their respective procurement fraud investigative data by DOD for fraud risk management purposes.

DoD RESPONSE: The Inspector General of the Department of Defense's response has been provided directly to GAO and is not included herein.

Accessible Text for Appendix IV Comments from the Department of Defense

January 30, 2024

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

Dear Mr. Bagdoyan:

Enclosed is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report GAO-24-105358SU, "DOD FRAUD RISK MANAGEMENT: Enhanced Data Analytics Can Help Manage Fraud Risks," dated January 2024 (GAO Code 105358).

We appreciate the opportunity to provide comments. My point of contact is Ms. Angela Palma (angela.d.palma2.civ@mail.mil or 571-516-4363).

Sincerely,

STEFFENS.THOMA
S.CHARLES.10293
42870

Digitally signed by
STEFFENS.THOMAS.CHARLES.
1029342870
Date: 2024.01.30 15:09:31 -05'00'

Thomas C. Steffens
Deputy Chief Financial Officer

Enclosure:
Consolidated DoD Response to GAO 105358

**GAO DRAFT REPORT DATED JANUARY 1, 2024 GAO-24-105358SU (GAO
CODE 105358)**

**“DoD FRAUD RISK MANAGEMENT: Enhanced Data Analytics Can Help
Manage Fraud Risks”**

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense should ensure that the Under Secretary of Defense (Comptroller) revises DoD’s Fraud Risk Management Strategy to establish data analytics as a method for preventing, detecting, and responding to fraud.

DoD RESPONSE: Respectfully non-concur. Below are examples and references for where DoD has already accomplished the work reflected the recommendation. In the DoD’s Fraud Risk Management Strategy, the Under Secretary of Defense (Comptroller) has established data analytics as a method for preventing, detecting, and responding to fraud.

As an example, the DoD Fraud Risk Strategy states (page 4) the “DoD is subject to requirements in the Payment Integrity Information Act of 2019 (PIIA).” The Strategy also states (page 1) the PIIA “requires and encourages agencies to use data analytics to identify, prevent, and respond to fraud and adopt an anti-fraud culture within their programs.” Page 6 reiterates that “DoD’s FRM Strategy defines activities for assessing, identifying, and managing fraud risks based on the requirements of the PIIA and OMB, considering the leading practices outlined in the GAO Framework.”

Additionally, the Strategy (page 11) says “Components should develop fraud analytics based on high-risk areas identified through the Fraud Risk Assessment.” It notes components “should produce actionable results from analytics, measurable fraud reduction outcomes, and other implementation activities to reduce fraud.”

Page 24 of the draft report states “Strategy generally refers to data analytics activities but does not discuss what or how data analytics are to be used. For example, designing and implementing edit checks, data matching, and data mining; combining data across programs to facilitate analytics; and pursuing access to external data.” However, the DoD Strategy already includes examples of techniques in the list of Fraud Control Activities. Specifically, Principle 6 (page 24) highlights that “Management performs data activities to help with fraud risk management including data mining and data matching techniques.”

Notably, the Department is already employing data analytics. For example, the Defense Finance and Accounting Service (DFAS) utilizes the Advana Improper Payment Detection (IPD) tool for the early identification and prevention of improper payments for seven entitlement systems. Daily, these entitlement systems send prepayment invoice files to the Advana tool, where they run through a series of business rules called Integrity Checks. The prepayment checks look for key indicators to prevent duplicate payments, overpayments, wrong vendor payments and various types of recoupment errors. If an invoice from the daily file meets the criteria of an Integrity Check, it will flag a ticket in the Advana IPD tool for a DFAS technician to manually review. Technicians review tickets within 24 hours of flagging, and if paying the invoice would lead to an improper payment, the technician will initiate corrective action in the source system to prevent the invoice from disbursing. This tool has prevented the improper payment of over \$14 billion in total since inception. DoD 7000.14-R, Financial Management Regulation, Volume 4, Chapter 14 “Payment Integrity,” September 2023, outlines payment integrity processes and requires DoD Components to implement PIIA.

Of note, the Office of the Under Secretary of Defense (Comptroller) (OUSDC) uses two fraud data analytics tools within Advana; the Deputy Chief Financial Officer (DCFO) Risk Management and Internal Control (RMIC) Team developed the Fraud Risk Register dashboard, which is an aggregation of fraud risks submitted through the Statement of Assurance (SOA) Program where Components are required to assess the risk of fraud when conducting their annual risk assessment. Components utilize a risk-based approach to identify, assess, and understand potential fraud risks and take appropriate action to mitigate them. Please note that fraud risks relate to a list of areas identified by the PIIA, and the Office of Management and Budget (OMB). DCFO utilizes the highest priority fraud risks with Department-wide impact to drive internal control testing efforts. Additionally, the RMIC Team has developed the Fraud Controls Matrix dashboard which displays the fraud risk control assessments submitted through the SOA Program. The inputs were also aligned with the leading practices from GAO’s FRM Framework.

Finally, besides the Fraud Risk Management Strategy, two recent Secretary of Defense memoranda have stressed the importance of implementing enterprise risk management and strengthening the internal control environment. The memoranda are: “Expectations for Supporting Department of Defense Financial Statement Audits,” dated October 13, 2023, and “Fiscal Year 2024 Financial Statement Audit Priorities,” dated November 30, 2023. Both set strong and committed tone-at-the-top expectations for effective DoD financial management.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense should ensure that the Under Secretary of Defense (Comptroller) identifies and documents in DoD’s Fraud Risk Management Strategy which entity has the

necessary authority to ensure that fraud-related data analytics activities are planned and implemented.

DoD RESPONSE: Respectfully non-concur, as the Strategy already identifies the entity responsible for planning and implementing fraud-related data analytics activities. The Strategy (page 9) defines OUSD(C)/Enterprise Financial Transformation (EFT) as the entity for leading data analytics efforts and to provide the analytics infrastructure for fraud risk management analytics products. Further, the Strategy (page 10) cites the Fraud Reduction Task Force as leading the Department's analytic activities for high-priority risks. The Task Force is the cross-enterprise strategic team of subject matter experts, which includes internal controls and analytics representatives from each PSA and Component of the DoD (page 9).

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense should ensure that the Under Secretary of Defense (Comptroller) revises DoD's Fraud Risk Management Strategy to clarify and document roles and responsibilities related to data analytics activities.

DoD RESPONSE: Respectfully non-concur, based on the Strategy (page 9) already defining OUSD(C)/EFT as the entity responsible for leading data analytics efforts and providing the analytics infrastructure for fraud risk management analytics products. Further, the Strategy (page 10) cites the Fraud Reduction Task Force as leading the Department's analytic activities for high-priority risks. The Task Force is the cross-enterprise strategic team of subject matter experts, which includes internal controls and analytics representatives from each Principal Staff Assistant (PSA) and Component of the DoD (page 9).

The DoD Fraud Risk Management Strategy states up front (page 1) [the PIIA] "requires and encourages agencies to use data analytics to identify, prevent, and respond to fraud and adopt an anti-fraud culture within their programs." To emphasize this, page 4 documents: "DoD is subject to requirements in the Payment Integrity Information Act of 2019 (PIIA)."

Additionally, the Strategy (page 11) directs "Components should develop fraud analytics based on high-risk areas identified through the Fraud Risk Assessment." It further says components, "should produce actionable results from analytics, measurable fraud reduction outcomes, and other implementation activities to reduce fraud."

Components have been advised to develop analytics to assist with fraud detection and take corrective action to remediate. At a minimum, Components are required to identify fraud risks related to a list of areas identified by the Fraud Reduction and Data Analytics Act of 2015 (FRDAA), PIIA, and OMB.

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense should ensure that the Under Secretary of Defense (Comptroller) incorporates and documents timelines for designing and implementing data analytics activities into Fraud Risk Management Strategy.

DoD RESPONSE: Respectfully non-concur, given timelines for designing and implementing data analytics activities are already included in the DoD Fraud Risk Management Strategy.

Figure 4 on page 16 provides a timeline for fraud risk management activities. The schedule includes dates for the aggregation of fraud risks and GAO FRM Framework assessments to begin. The assessments include the following direction:

Per the GAO FRM Framework, [Management] collects and analyzes data on fraud trends and control deficiencies, a process that reflects the “lessons learned” element of monitoring and evaluation.

Additionally, Fraud Principle 6 in the Strategy (pages 23 and 24) states “[Management] performs data analytics activities to help with fraud risk management including data mining and data matching techniques.”

Lastly, the Strategy also includes the requirement of timelines in the list of Fraud Control Activities. Specifically, Principle 5 (page 23) states, “Management has created timelines for implementing fraud risk management activities, as appropriate, including monitoring and evaluations.”

RECOMMENDATION 5: The GAO recommends that the Inspector General of DoD should improve the usability of its procurement fraud investigative data for fraud risk management purposes. Specific actions should include ensuring that data in structured fields are complete, accessible, and readily subject to analysis and aggregation.

DoD RESPONSE: The Inspector General of the Department of Defense’s response has been provided directly to GAO and is not included herein.

RECOMMENDATION 6: The GAO recommends that the Secretary of the Air Force, in collaboration with the Inspector General of DoD and the other military departments, should improve the usability of its respective procurement fraud investigative data by DoD for fraud risk management purposes. Specific action should include ensuring data in structured fields are complete, accessible, and readily subject to analysis and aggregation.

DoD RESPONSE: The Secretary of the Air Force, Inspector General (SAF/IG) partially concurs with the one recommendation made to the Secretary of the Air Force (Recommendation 6, page 71 of the Draft GAO report). Not all data in structured fields should be required to be completed. Not all fields are relevant to every case or case type. SAF/IG concurs key fields for procurement fraud investigations should be required to be completed, and a review of structured fields will be completed by Headquarters Air Force Office of Special Investigations (AFOSI) to identify required fields.

Additionally, SAF/IG is submitting critical comments for its Technical Review of the draft report as it mischaracterizes information provided by AFOSI. The report also inaccurately captures datapoints previously clarified and provided by AFOSI during their engagements with the GAO between 6 Aug 21 – 30 Nov 23. SAF/IG provides the following general observations driving this non-concur and welcomes the opportunity for further discussion with the GAO. For additional technical issues related to this draft report, please see attachment Comments Resolution Matrix (Tab 2). AFOSI also conducted a Security-Sensitivity Review of this draft report and found no issues.

AFOSI acknowledges there are limitations with AFOSI's current case management system, Investigative Information Management System (I2MS), regarding collecting and aggregating data for fraud cases; however, AFOSI does not agree with GAO's interpretation of the data provided, nor can AFOSI validate the report findings without understanding which AFOSI cases were included and excluded from analysis. Further, AFOSI is moving to a new case management system, ORION, which is currently in its roll-out phase with a full implementation target date of 31 Mar 24. ORION will address many of the issues raised in this report, to include collecting data related to fraud schemes and more accurate collection of disposition data.

Additionally, AFOSI previously provided written responses to GAO's questions; however, many of these were not accurately captured in the current report and in some cases, the report directly contradicted the information provided by AFOSI. During previous engagements with the GAO, AFOSI representatives worked to assist GAO in understanding and correctly interpreting the data in the format exported from AFOSI systems. These efforts included discussions with agents and case management system administrators, as well as a case management system demonstration. Despite these efforts, the report does not accurately reflect the provided information.

RECOMMENDATION 7: The GAO recommends that the Secretary of the Army, in collaboration with the Inspector General of DoD and the other military departments, should improve the usability of its respective procurement fraud investigative data by DoD for fraud risk management purposes. Specific actions should include ensuring

data in structured fields are complete, accessible, and readily subject to analysis and aggregation.

DoD RESPONSE: Concur. The Secretary of the Army, in collaboration with the Inspector General of DoD and the other Military Departments, will improve the usability of its respective procurement fraud investigative data by DoD for fraud risk management purposes. Specific actions will include ensuring data in structured fields are complete, accessible, and readily subject to analysis and aggregation.

RECOMMENDATION 8: The GAO recommends that the Secretary of the Navy, in collaboration with the Inspector General of DoD and the other military departments, should improve the usability of its respective procurement fraud investigative data by DoD for fraud risk management purposes. Specific action should include ensuring data in structured fields are complete, accessible, and readily subject to analysis and aggregation.

DoD RESPONSE: Non-Concur. NCIS non concurs with the report as written and provides the following general issues with the report. However, NCIS is willing to change the non-concur to concur if the specific items outlined in the attached “Comments Resolution Matrix” are addressed (Tab 3).

NCIS concurs there are limitations with its case management system, Consolidated Law Enforcement Operations Center (CLEOC), regarding collecting and aggregating data for procurement fraud cases; however, NCIS does not agree with GAO’s interpretation of the data provided, nor can NCIS validate the report findings without access to the final data set (which was not provided to NCIS) used for GAO’s analysis.

NCIS provided written responses to a number of GAO’s questions and participated in multiple conversations with GAO to assist their analysis of the requested data. Despite the collaboration, GAO’s interpretation of the data is not accurately captured in the GAO report. During one in- person meeting, requested by NCIS, GAO personnel were painstakingly briefed on the original data set by NCIS representatives, in an effort to explain the correct interpretation of multiple rows and columns, which aggregate the complete mosaic depicting how an investigative data should be interpreted. Despite these efforts, there appeared to be residual confusion from GAO on how to properly read and interpret the data provided.

RECOMMENDATION 9: The GAO recommends that the Comptroller should collaborate with the Inspector General of DoD and Secretaries of the Navy, Air Force, and Army, respectively, to obtain and analyze relevant information from closed adjudicated procurement fraud cases.

DoD RESPONSE: Concur. Comptroller will collaborate with the Department of Defense Office of Inspector General, and Secretaries of the Navy, Air Force, and Army to obtain and analyze relevant information from closed adjudicated procurement fraud cases.

RECOMMENDATION 10: The GAO recommends that the Secretary of Defense should ensure that the Under Secretary of Defense (Comptroller) revises DoD's Fraud Risk Management Strategy to obtain and analyze relevant information from closed alleged and adjudicated procurement fraud cases from the Defense Criminal Investigative Organizations.

DoD RESPONSE: Concur. OUSD(C) will revise DoD's Fraud Risk Management Strategy to obtain and analyze relevant information from closed alleged and adjudicated procurement fraud cases from the Defense Criminal Investigative Organizations and Secretaries of the Navy, Air Force, and Army.

Currently, the 2023 DoD FRM Strategy (page 11) assigns the Components the responsibility to review and mitigate potential fraud cases and to provide feedback on fraud reduction efforts to improve the DoD-wide fraud analytics framework. Further, the Strategy (pages 10 and 11) lists that the Fraud Reduction Task Force is responsible for producing actionable results from analytics, measurable fraud reduction outcomes, and other implementation activities to reduce fraud.

Lastly, the OUSD(C) regularly collaborates with Defense Criminal Investigative Organizations. For instance, the OUSD(C) Financial Management Policy and Reporting Directorate works with the Procurement Fraud Working Group and the Deputy Chief Information Officers to identify and define confirmed fraud. Additionally, the Defense Criminal Investigative Service presented during the monthly Fraud Reduction Task Force office hours held in June 2023. Earlier in the year, OUSD(Acquisition and Sustainment), Defense Pricing and Contracting Office, and the DoD Office of General Counsel presented during the 2023 OUSD(C) and Office of the Director of Administration and Management jointly-held the RMIC Townhall.

RECOMMENDATION 11: The Inspector General of DOD should collaborate, as appropriate, with the military departments and relevant stakeholders, on the development of leading practices towards improving the usability of their respective procurement fraud investigative data by DOD for fraud risk management purposes.

DoD RESPONSE: The Inspector General of the Department of Defense's response has been provided directly to GAO and is not included herein.

Appendix V Comments from the Department of Defense Office of Inspector General

**Appendix V Comments from the Department of
Defense Office of Inspector General**



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

January 25, 2024

Seto Bagdoyan
Director of Audits
Forensic Audits and Investigative Service
U.S. Government Accountability Office
Washington, DC 20510

Dear Mr. Bagdoyan:

Thank you for the opportunity to review the U.S. Government Accountability Office (GAO) draft report, DoD Fraud Risk Management: Enhanced Data Analytics Can Help Manage Fraud Risks (GAO-24-105358SU). We also appreciate that your team took the time to meet with Department of Defense Office of Inspector General (DoD OIG) representatives to discuss our concerns with the draft report and several of the recommendations.

We concur with the recommendations and have technical comments on some of the specific wording in the finding. Our concurrence reflects and is contingent upon the edits your team agreed to make to the report after our January 17, 2024, meeting and the additional technical comments we make in this response. Our specific comments are as follows.

- Recommendation 5:
 - Draft report states: The Inspector General of DOD, in collaboration with the military departments, should improve the usability of its respective procurement fraud investigative data by DOD for fraud risk management purposes. Specific actions should include ensuring data in structured fields are complete, accessible, and readily subject to analysis and aggregation.
 - GAO-proposed revision: The Inspector General of DOD should improve the usability of its procurement fraud investigative data for fraud risk management purposes. Specific actions should include ensuring that data in structured fields are complete, accessible, and readily subject to analysis and aggregation.
 - Our response: We concur with revised recommendation 5. We will review our procurement fraud investigative data in the case management system and identify and implement changes to ensure that, when possible, data in structured fields are complete, accessible, and able to be analyzed and aggregated. We plan to complete this action by the end of 2026.
- Recommendations 6, 7, and 8:
 - Our response: Although not directed to the DoD Inspector General, we concur with recommendations 6, 7, and 8. We will collaborate with the Secretaries of the Military Departments, when requested and as appropriate, to improve the usability of procurement fraud investigative data.

**Appendix V Comments from the Department of
Defense Office of Inspector General**

- Recommendation 9:
 - Draft report states: The Comptroller should collaborate with the Inspector General of DOD and the Secretaries of the Navy, Air Force, and Army, respectively, to obtain and analyze relevant information from closed alleged and adjudicated procurement fraud cases.
 - GAO-proposed revision: The Comptroller should collaborate with the Inspector General of DOD and the Secretaries of the Navy, Air Force, and Army, respectively, to obtain and analyze relevant information from adjudicated procurement fraud cases.
 - Our response: Although not directed to the DoD Inspector General, we concur with recommendation 9. We will collaborate with the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD, by providing, when requested and as appropriate, relevant information from adjudicated procurement fraud cases.
- New Recommendation 11: The Inspector General of DOD should collaborate, as appropriate, with the Military Departments and relevant stakeholders, on the development of leading practices towards improving the usability of their respective procurement fraud investigative data by DOD for fraud risk management purposes.
 - Our response: We concur with recommendation 11. We will collaborate, as appropriate, with the Military Departments and relevant stakeholders to improve the usability of Military Department and DoD OIG procurement fraud investigative data. We may consider relevant oversight work in this area. We intend to conclude this effort by the end of 2026.
- Technical Comment on Page 31 (PDF Page 35):
 - Draft report states: While DOD’s strategy identifies DCIS as an information source, it does not outline the use of information from case management data.
 - GAO-proposed revision: While DOD’s strategy identifies DCIS as an information source, it does not outline the use of information from case management data. Additionally, DCIS officials told us that while the DOD OIG Audit Directorate reviewed a draft of the strategy, DCIS has not reviewed or concurred with DOD’s strategy.
 - Our response: The proposed revision does not fully address our concerns. We request that the language be edited to: “While the DOD’s strategy identifies DCIS as an information source, it does not outline the use of information from case management data. Although the draft strategy was informally reviewed within the DoD OIG, the Under Secretary of Defense (Comptroller)/Chief Financial Officer did not formally coordinate the strategy with the DoD OIG in accordance with established DoD coordination processes. An issuance that requires specific

**Appendix V Comments from the Department of
Defense Office of Inspector General**

actions from the DoD OIG requires formal coordination and ultimately approval from the IG or Principal Deputy IG, which did not occur.” The published strategy, “Fraud Risk Management Strategy and Guidance,” Version 2.0, August 2023, contains inaccuracies about the DoD OIG’s and DCIS’s roles, responsibilities, authorities, and standard practices. We will work with the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD, to make the appropriate corrections.

- Technical Comment on Page 53 (PDF Page 57)
 - Draft report states: According to the available data, of the DCIS cases we identified, at least 683 involved suspects for who charges were cleared due to prosecution declination.
 - GAO-proposed revision: According to the available data, of the 1,165 DCIS cases we identified, at least 683 involved suspects for whom there was a prosecution declination. The data also showed that of the 1,165 cases, there were 388 cases where there was a prosecution declination for all suspects.
 - Our response: The proposed revision addresses our concerns and we request no additional changes.
- Technical Comment on Page 62 (PDF Pg 66)
 - Draft report states: DCIS’s Special Agents Manual Notes that CRIMS is the principal reporting system.
 - GAO-proposed revision: a DCIS policy manual notes that the Case Reporting and Information Management System (CRIMS) is the principal reporting system.
 - Our response: The proposed revision addresses our concerns and we request no additional changes.
- Technical Comment on Page 63 (PDF Pg 67):
 - Draft report states: Specifically, the strategy states that DCIS maintains regular communication with the Comptroller, ODA&M, and Principal Staff Assistants regarding existing and potential fraud cases and emerging trends to help improve fraud risk assessment prevention, detection, and mitigation across the Department.
 - GAO-proposed revision: Specifically, the strategy states that DCIS maintains regular communication with the Comptroller, ODA&M, and Principal Staff Assistants regarding existing and potential fraud cases and emerging trends to help improve fraud risk assessments, prevention, detection, and mitigation across the department. As stated above, DCIS officials told us that while the DOD OIG Audit Directorate reviewed a draft of the strategy, DCIS has not reviewed or concurred with the strategy. DCIS officials told us that DOD OIG does not

**Appendix V Comments from the Department of
Defense Office of Inspector General**

participate in the management of DOD programs or operations, but has shared information with DOD on a variety of topics, including fraud trends and how to report fraud.¹ DCIS officials also said they provide case outcomes for specific cases to program officials, when appropriate, and clarified that DCIS does not share information on ongoing, existing, or closed investigative cases that have not been made public by the U.S. Courts...*Footnote 1*: DCIS officials also noted that the DOD OIG is an independent entity; thus, DCIS is not required to share information with DOD.

- Our Response: The proposed revision does not fully address our concerns. We request that you revise the following sentence:

As written: “As stated above, DCIS officials told us that while the DOD OIG Audit Directorate reviewed a draft of the strategy, DCIS has not reviewed or concurred with the strategy.”

Revise to: “Although the draft strategy was informally reviewed within the DoD OIG, the Under Secretary of Defense (Comptroller)/Chief Financial Officer did not formally coordinate the strategy with the DoD OIG in accordance with established DoD coordination processes. An issuance that requires specific actions from the DoD OIG requires formal coordination and ultimately approval from the IG or Principal Deputy IG, which did not occur.”

We appreciate the professionalism and collegiality with which your team approached this engagement and, in particular, GAO’s consideration of the DoD OIG’s concerns. My point of contact for this matter is Mr. Grant Fleming, DCIS Deputy Director, at 703-604-8300, grant.fleming@dodig.mil.

Very truly yours,



Robert P. Storch
Inspector General

Accessible Text for Appendix V Comments from the Department of Defense Office of Inspector General

January 25, 2024

Seto Bagdoyan
Director of Audits
Forensic Audits and Investigative Service
U.S. Government Accountability Office
Washington, DC 20510

Dear Mr. Bagdoyan:

Thank you for the opportunity to review the U.S. Government Accountability Office (GAO) draft report, DoD Fraud Risk Management: Enhanced Data Analytics Can Help Manage Fraud Risks (GAO-24-105358SU). We also appreciate that your team took the time to meet with Department of Defense Office of Inspector General (DoD OIG) representatives to discuss our concerns with the draft report and several of the recommendations.

We concur with the recommendations and have technical comments on some of the specific wording in the finding. Our concurrence reflects and is contingent upon the edits your team agreed to make to the report after our January 17, 2024, meeting and the additional technical comments we make in this response. Our specific comments are as follows.

- Recommendation 5:
 - Draft report states: The Inspector General of DOD, in collaboration with the military departments, should improve the usability of its respective procurement fraud investigative data by DOD for fraud risk management purposes. Specific actions should include ensuring data in structured fields are complete, accessible, and readily subject to analysis and aggregation.
 - GAO-proposed revision: The Inspector General of DOD should improve the usability of its procurement fraud investigative data for fraud risk management purposes. Specific actions should include

ensuring that data in structured fields are complete, accessible, and readily subject to analysis and aggregation.

- Our response: We concur with revised recommendation 5. We will review our procurement fraud investigative data in the case management system and identify and implement changes to ensure that, when possible, data in structured fields are complete, accessible, and able to be analyzed and aggregated. We plan to complete this action by the end of 2026.
- Recommendations 6, 7, and 8:
 - Our response: Although not directed to the DoD Inspector General, we concur with recommendations 6, 7, and 8. We will collaborate with the Secretaries of the Military Departments, when requested and as appropriate, to improve the usability of procurement fraud investigative data.
- Recommendation 9:
 - Draft report states: The Comptroller should collaborate with the Inspector General of DOD and the Secretaries of the Navy, Air Force, and Army, respectively, to obtain and analyze relevant information from closed alleged and adjudicated procurement fraud cases.
 - GAO-proposed revision: The Comptroller should collaborate with the Inspector General of DOD and the Secretaries of the Navy, Air Force, and Army, respectively, to obtain and analyze relevant information from adjudicated procurement fraud cases.
 - Our response: Although not directed to the DoD Inspector General, we concur with recommendation 9. We will collaborate with the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD, by providing, when requested and as appropriate, relevant information from adjudicated procurement fraud cases.
- New Recommendation 11: The Inspector General of DOD should collaborate, as appropriate, with the Military Departments and relevant stakeholders, on the development of leading practices towards improving the usability of their respective procurement fraud investigative data by DOD for fraud risk management purposes.

- Our response: We concur with recommendation 11. We will collaborate, as appropriate, with the Military Departments and relevant stakeholders to improve the usability of Military Department and DoD OIG procurement fraud investigative data. We may consider relevant oversight work in this area. We intend to conclude this effort by the end of 2026.
- Technical Comment on Page 31 (PDF Page 35):
 - Draft report states: While DOD’s strategy identifies DCIS as an information source, it does not outline the use of information from case management data.
 - GAO-proposed revision: While DOD’s strategy identifies DCIS as an information source, it does not outline the use of information from case management data. Additionally, DCIS officials told us that while the DOD OIG Audit Directorate reviewed a draft of the strategy, DCIS has not reviewed or concurred with DOD’s strategy.
 - Our response: The proposed revision does not fully address our concerns. We request that the language be edited to: “While the DOD’s strategy identifies DCIS as an information source, it does not outline the use of information from case management data. Although the draft strategy was informally reviewed within the DoD OIG, the Under Secretary of Defense (Comptroller)/Chief Financial Officer did not formally coordinate the strategy with the DoD OIG in accordance with established DoD coordination processes. An issuance that requires specific actions from the DoD OIG requires formal coordination and ultimately approval from the IG or Principal Deputy IG, which did not occur.” The published strategy, “Fraud Risk Management Strategy and Guidance,” Version 2.0, August 2023, contains inaccuracies about the DoD OIG’s and DCIS’s roles, responsibilities, authorities, and standard practices. We will work with the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD, to make the appropriate corrections.
- Technical Comment on Page 53 (PDF Page 57)
 - Draft report states: According to the available data, of the DCIS cases we identified, at least 683 involved suspects for who charges were cleared due to prosecution declination.

- GAO-proposed revision: According to the available data, of the 1,165 DCIS cases we identified, at least 683 involved suspects for whom there was a prosecution declination. The data also showed that of the 1,165 cases, there were 388 cases where there was a prosecution declination for all suspects.
- Our response: The proposed revision addresses our concerns and we request no additional changes.
- Technical Comment on Page 62 (PDF Pg 66)
 - Draft report states: DCIS's Special Agents Manual Notes that CRIMS is the principal reporting system.
 - GAO-proposed revision: a DCIS policy manual notes that the Case Reporting and Information Management System (CRIMS) is the principal reporting system.
 - Our response: The proposed revision addresses our concerns and we request no additional changes.
- Technical Comment on Page 63 (PDF Pg 67):
 - Draft report states: Specifically, the strategy states that DCIS maintains regular communication with the Comptroller, ODA&M, and Principal Staff Assistants regarding existing and potential fraud cases and emerging trends to help improve fraud risk assessment prevention, detection, and mitigation across the Department.
 - GAO-proposed revision: Specifically, the strategy states that DCIS maintains regular communication with the Comptroller, ODA&M, and Principal Staff Assistants regarding existing and potential fraud cases and emerging trends to help improve fraud risk assessments, prevention, detection, and mitigation across the department. As stated above, DCIS officials told us that while the DOD OIG Audit Directorate reviewed a draft of the strategy, DCIS has not reviewed or concurred with the strategy. DCIS officials told us that DOD OIG does not participate in the management of DOD programs or operations, but has shared information with DOD on a variety of topics, including fraud trends and how to report fraud.¹ DCIS officials also said they provide case outcomes for specific cases to program officials, when appropriate, and clarified that DCIS does not share information on ongoing, existing, or closed investigative cases that have not been

made public by the U.S. Courts...Footnote 1: DCIS officials also noted that the DOD OIG is an independent entity; thus, DCIS is not required to share information with DOD.

- Our Response: The proposed revision does not fully address our concerns. We request that you revise the following sentence:

As written: “As stated above, DCIS officials told us that while the DOD OIG Audit Directorate reviewed a draft of the strategy, DCIS has not reviewed or concurred with the strategy.”

Revise to: “Although the draft strategy was informally reviewed within the DoD OIG, the Under Secretary of Defense (Comptroller)/Chief Financial Officer did not formally coordinate the strategy with the DoD OIG in accordance with established DoD coordination processes. An issuance that requires specific actions from the DoD OIG requires formal coordination and ultimately approval from the IG or Principal Deputy IG, which did not occur.”

We appreciate the professionalism and collegiality with which your team approached this engagement and, in particular, GAO’s consideration of the DoD OIG’s concerns. My point of contact for this matter is Mr. Grant Fleming, DCIS Deputy Director, at 703-604-8300, grant.fleming@dodig.mil.

Very truly yours,

Robert P. Storc
Inspector General

Error! No text of specified style in document.

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact:

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

Staff Acknowledgments:

In addition to the contact named above, Heather Dunahoo and Mariana Calderón (Assistant Directors), Joy Myers and Yue Pui Chin (Analysts in Charge), David Ballard, Priyanka Sethi Bansal, Pamela Davidson, Flavio Martinez, Héctor M. Meléndez, Jr., Ryan Nary, Samuel Portnow, Elisabeth Schaerr Garlock, and Herrica Telus made key contributions to this report. Also contributing to the report were Colin Fallon, Maria McMullen, James Murphy, Barbara Lewis, and Ariel Vega.

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.

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (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

