



DOD FRAUD RISK MANAGEMENT

DOD Should Expeditiously and Effectively Implement Fraud Risk Management Leading Practices

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

Testimony

Before the Subcommittee on Government Operations,
Committee on Oversight and Government Reform,
House of Representatives

For Release on Delivery Expected at 10:00 a.m. ET Wednesday, June 4, 2025

GAO-25-108500

United States Government Accountability Office

Accessible Version

GAO Highlights

For more information, contact Seto J. Bagdoyan at bagdoyans@gao.gov.

Highlights of [GAO-25-108500](#), a testimony before the Subcommittee on Government Operations, Committee on Oversight and Government Reform, House of Representatives

DOD FRAUD RISK MANAGEMENT

DOD Should Expeditiously and Effectively Implement Fraud Risk Management Leading Practices

Why GAO Did This Study

DOD is responsible for almost half of the federal government's discretionary spending and spends more on contracting than all other federal agencies combined. The scope and scale of this activity makes DOD inherently susceptible to fraud that can threaten DOD's financial position and put the warfighter in increased danger.

In February 2025, GAO expanded DOD's financial management area on GAO's High Risk List to include fraud risk management at DOD. An effective system of internal controls can help DOD produce reliable, useful, and timely financial information and prevent and detect fraud.

This testimony discusses the status of DOD's efforts to implement fraud risk management leading practices, as well as DOD's response to prior GAO recommendations. It is based primarily on GAO work from 2019 through 2024 related to DOD fraud risk management. Details on GAO's methodology can be found in each of the reports cited in this statement.

What GAO Found

The full extent of fraud affecting the Department of Defense (DOD) is not known but is potentially significant. DOD reported almost \$11 billion in confirmed fraud over 7 years, an amount that reflects a small fraction of DOD's potential fraud exposure. GAO has previously reported on fraud at DOD, including cases where:

- a shell company fraudulently provided defective parts to DOD, leading to the grounding of 47 fighter aircraft; and
- a contractor bribed officials for classified information and preferential treatment, ultimately defrauding DOD of tens of millions of dollars.

DOD has taken initial steps to implement a fraud risk management approach that aligns with leading practices in GAO's *Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework). In accordance with statutory requirements, the Office of Management and Budget requires agencies to implement the leading practices from the Fraud Risk Framework.

DOD's initial steps include designating a dedicated entity to oversee fraud risk management activities. DOD also requires military components to identify and report fraud risks, providing guidance, tools, and training for them to do so.

However, the department needs sustained effort to effectively prevent, detect, and respond to fraud. DOD leadership has not demonstrated a strong commitment to fraud risk management and should take action in three key areas (see figure).

DOD Should Take Action in Key Areas to Manage Fraud Risks



Fully establish an organizational culture conducive to fraud risk management



Comprehensively assess risks and compile a fraud risk profile



Issue an antifraud strategy that includes control activities that align with leading practices

Source: GAO recommendations. | GAO-25-108500

Accessible Data for DOD Should Take Action in Key Areas to Manage Fraud Risks

- Plan and conduct regular fraud risk assessments that align with leading practices
- Comprehensively assess risks and compile a fraud risk profile
- Obtain and analyze relevant information on adjudicated procurement fraud cases

Source: GAO recommendations. | GAO-25-108500

GAO has made 17 recommendations across three DOD fraud risk management reports since 2019. Thirteen of these recommendations have not been implemented as of May 2025, including two that will be designated as priority recommendations—recommendations that can save money, help Congress make decisions, and substantially improve or transform government agencies. For example, GAO found that DOD could save \$100 million or more by implementing fraud risk management recommendations related to using data analytics to prevent, detect, and respond to fraud.

Despite taking some actions to close or implement GAO's recommendations, DOD has repeatedly delayed implementing several of these recommendations. For example, DOD has delayed updating its antifraud strategy five times over 7 months. Without a comprehensive antifraud strategy that effectively aligns with leading practices, DOD remains at substantial risk of fraud against its vast resources.

Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee:

Thank you for the opportunity to discuss the Department of Defense's (DOD) efforts to implement fraud risk management leading practices, as well as DOD's response to prior GAO recommendations.

We have previously reported that DOD has not taken effective steps to develop a robust fraud risk management program, and its leadership has not demonstrated a strong commitment to managing fraud risk.¹ As a result, in February 2025 we expanded DOD's financial management area on GAO's High Risk List to include fraud risk management.² The lack of an effective fraud risk management program, combined with financial management weaknesses, compounds DOD's failure to establish a strong internal control environment. This, in turn, increases opportunities for fraudulent actions against DOD's vast resources.

DOD spends over \$1 trillion annually to support the military and its operations.³ This spending makes up almost half of the federal government's total discretionary spending. In fiscal year 2024, it obligated about \$445 billion for contracting activity, an amount higher than all other federal agencies combined. The scope and scale of this activity—which includes contracts on major weapon systems, support for military bases, information technology, and consulting services—makes DOD inherently susceptible to fraud, including procurement fraud.⁴ In this regard, procurement fraud can occur when an agency has weak controls, as well as programs with high spending levels and complex design.

The full extent of fraud affecting DOD is not known but is potentially significant. In 2018, DOD reported to Congress that it had recovered more than \$6.6 billion from adjudicated defense contracting fraud cases from fiscal years 2013 through 2017.⁵ Separately, for fiscal years 2017 through 2024, DOD

¹GAO, *Defense Procurement: Ongoing DOD Fraud Risk Assessment Efforts Should Include Contractor Ownership*, [GAO-20-106](#) (Washington, D.C.: Nov. 25, 2019); *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 *DOD Fraud Risk Management: Enhanced Data Analytics Can Help Manage Fraud Risks*, [GAO-24-105358](#) (Washington, D.C.: Feb. 27, 2024).

²GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, [GAO-25-107743](#) (Washington, D.C.: Feb. 25, 2025). GAO's High-Risk Series identifies government operations with serious vulnerability to fraud, waste, abuse, and mismanagement or that need transformation.

³This value represents outlays, which are the issuance of checks, disbursement of cash, or electronic transfer of funds made to liquidate a federal obligation. Outlays during a fiscal year may be for payment of obligations incurred in prior years or in the same year.

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 can rationalize committing fraud. Fraud risk can exist even if actual fraud has not occurred. When fraud risks can be identified and mitigated, fraud may be less likely to happen.

⁵Department of Defense, *Report on Defense Contracting Fraud*, 5-070E775 (December 2018). Recovered funds include moneys received in fines, penalties, restitution, and forfeiture of property in criminal convictions of fraud and through civil judgments and settlements.

reported almost \$11 billion in confirmed fraud via [PaymentAccuracy.gov](https://www.paymentaccuracy.gov).⁶ Recoveries and confirmed fraud reflect only a small fraction of DOD's potential fraud exposure. They do not include undetected fraud and potential fraud detected by the agency that it has not investigated. DOD officials informed us in November 2024 that they did not believe there was much fraud within the department relative to its overall spending. However, even a small percentage of DOD's \$1 trillion in annual spending lost to fraudsters is a significant diversion of resources from its warfighting mission.

Not only does fraud threaten DOD's financial position, but it can also put the warfighter in increased danger. We previously reported on fraud cases closed by Defense Criminal Investigative Organizations or prosecuted by the Department of Justice.⁷ One such case involved a contractor who used shell companies with opaque ownership structures to falsely claim U.S. ownership and obtain government contracts supplying spare parts for DOD. The contractor sent restricted military data to a foreign manufacturer, who produced defective and nonconforming parts for the U.S.-based shell companies. These parts were ultimately provided to DOD and led to the grounding of 47 fighter aircraft.⁸

My remarks are based primarily on our work from 2019 through 2024 regarding DOD's fraud risk management efforts, as well as our 2025 High Risk List report. More detailed information on the scope and methodology of our prior work can be found within each specific report. We conducted the work on which this testimony is based 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

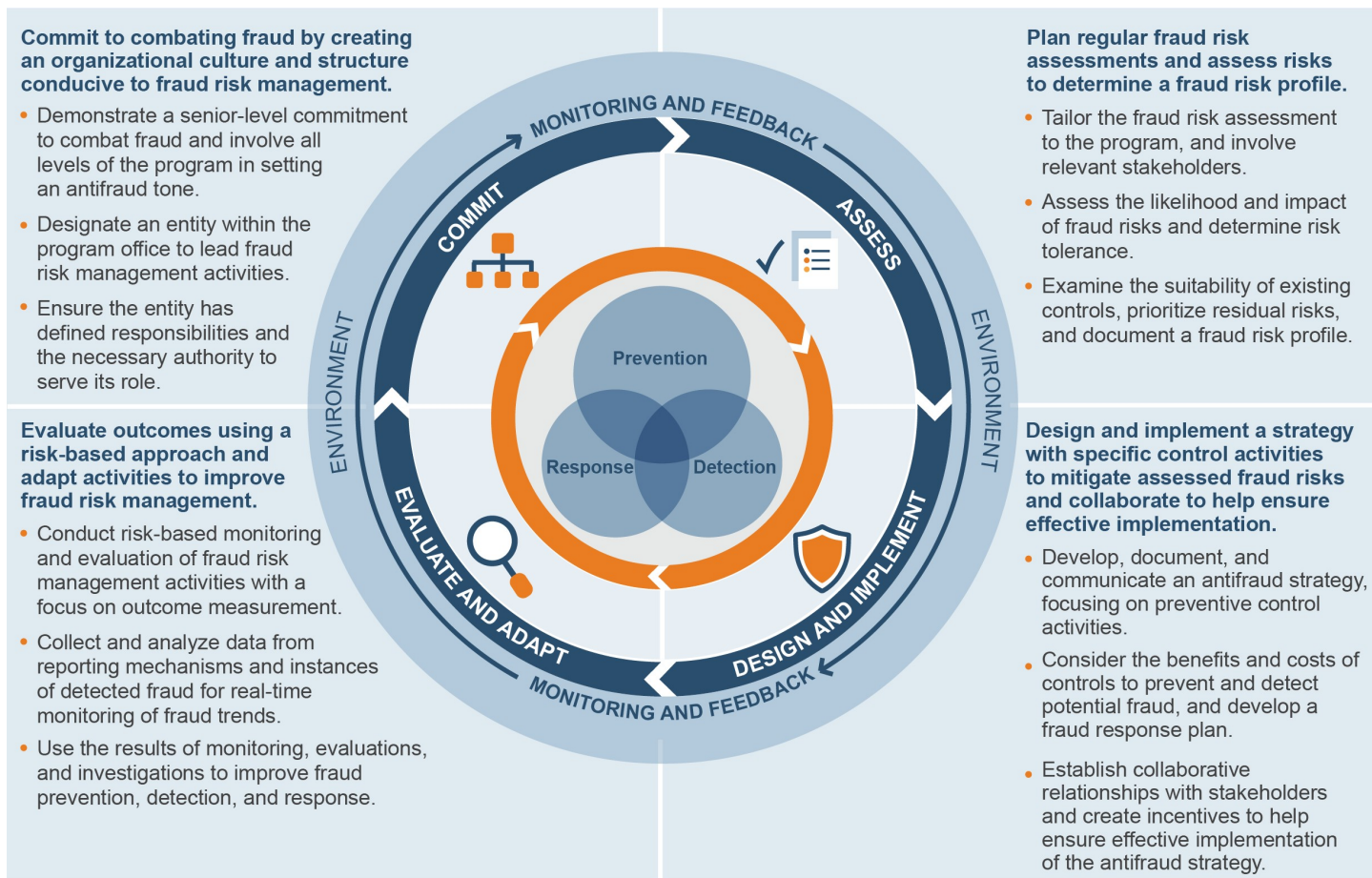
In July 2015, we issued *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework), which contains a comprehensive set of leading practices to guide agency managers in combating fraud in a strategic, risk-based way.⁹ Specifically, the Fraud Risk Framework describes leading practices within four components: commit, assess, design and implement, and evaluate and adapt (see fig.1).

⁶According to the Office of Management and Budget (OMB), confirmed fraud is the amount determined to be fraudulent through the judicial or adjudication process. It represents only those fraud cases that have been confirmed by a court or other adjudicative forum and does not represent anything settled out of court with or without admission of guilt. OMB requires agencies to provide certain information about improper payments and confirmed fraud. OMB publishes this information in a dashboard on [PaymentAccuracy.gov](https://www.paymentaccuracy.gov).

⁷Defense Criminal Investigative Organizations refers to the DOD Office of Inspector General's Defense Criminal Investigative Service, the Army Criminal Investigation Division, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations, collectively. For more information, see [GAO-24-105358](#).

⁸[GAO-20-106](#).

⁹GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015).

Figure 1: The Four Components of the Fraud Risk Management Framework and Selected Leading Practices**Accessible Data for Figure 1: The Four Components of the Fraud Risk Management Framework and Selected Leading Practices**

Column one	Column two
<p>Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.</p> <ul style="list-style-type: none"> • Demonstrate a senior-level commitment to combat fraud and involve all levels of the program in setting an antifraud tone. • Designate an entity within the program office to lead fraud risk management activities. • Ensure the entity has defined responsibilities and the necessary authority to serve its role. 	<p>Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.</p> <ul style="list-style-type: none"> • Tailor the fraud risk assessment to the program, and involve relevant stakeholders. • Assess the likelihood and impact of fraud risks and determine risk tolerance. • Examine the suitability of existing controls, prioritize residual risks, and document a fraud risk profile.

Column one	Column two
<p>Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.</p> <ul style="list-style-type: none"> • Conduct risk-based monitoring and evaluation of fraud risk management activities with a focus on outcome measurement. • Collect and analyze data from reporting mechanisms and instances of detected fraud for real-time monitoring of fraud trends. • Use the results of monitoring, evaluations, and investigations to improve fraud prevention, detection, and response. 	<p>Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.</p> <ul style="list-style-type: none"> • Develop, document, and communicate an antifraud strategy, focusing on preventive control activities. • Consider the benefits and costs of controls to prevent and detect potential fraud, and develop a fraud response plan. • Establish collaborative relationships with stakeholders and create incentives to help ensure effective implementation of the antifraud strategy

Source: GAO. | GAO-25-108500

Since 2016, consistent with the requirements of the Fraud Reduction and Data Analytics Act of 2015 and the Payment Integrity Information Act of 2019, the Office of Management and Budget (OMB) has required agencies, including DOD, to adhere to the Fraud Risk Framework leading practices as part of their efforts to effectively design, implement, and operate internal control systems that address fraud risks.¹⁰ Additionally, in October 2022, OMB issued a Controller Alert, reminding agencies that they must establish financial and administrative controls to identify and assess fraud risks.¹¹ It further reminded agencies that they should adhere to the leading practices in the Fraud Risk Framework to effectively design, implement, and operate an internal control system that addresses fraud risks.

According to DOD, it may face numerous procurement fraud risks. These include bid rigging, inflated prices, counterfeit parts, conflicts of interest, false documentation for contractor payments, and overbilling by contractors.¹² In 2019, we reported on procurement fraud risks faced by DOD, such as those posed by contractors with opaque ownership.¹³ In 2021 and 2024, we further reported on DOD's procurement fraud risks.¹⁴ In these reports, we also reported on illustrative examples of fraud against DOD (see fig. 2).

¹⁰The Fraud Reduction and Data Analytics Act of 2015, enacted in June 2016, required OMB to establish guidelines for federal agencies to create controls to identify and assess fraud risks and to design and implement antifraud control activities. Pub. L. No. 114-186, 130 Stat. 546 (2016). The Fraud Reduction and Data Analytics Act of 2015 was replaced in March 2020 by the Payment Integrity Information Act of 2019, which required these guidelines to remain in effect, subject to modification by OMB, as necessary, and in consultation with GAO. Pub. L. No. 116-117, § 2(a), 134 Stat. 113, 131-132 (2020), codified at 31 U.S.C. § 3357.

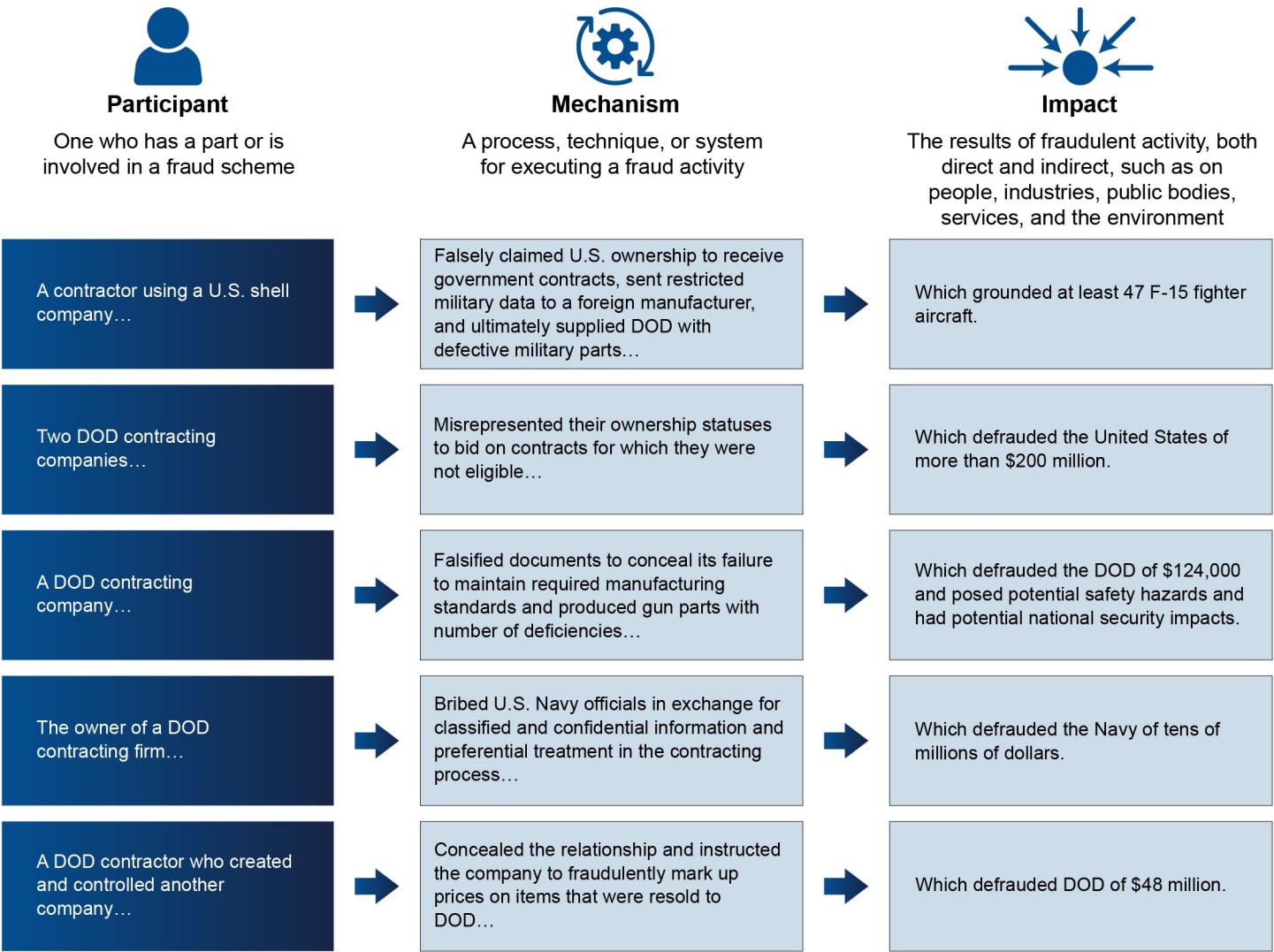
¹¹Office of Management and Budget, *Establishing Financial and Administrative Controls to Identify and Assess Fraud Risk*, [Controller Alert] CA-23-03 (Washington, D.C.: Oct. 17, 2022).

¹²Department of Defense, *Fiscal Year 2020 Department of Defense Statement of Assurance Execution Handbook*, (Jan. 30, 2020).

¹³[GAO-20-106](#). 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.

¹⁴[GAO-21-309](#) and [GAO-24-105358](#).

Figure 2: Illustrative Examples of Fraud Perpetrated Against the Department of Defense



Sources: GAO analysis of federal court documents, Department of Defense (DOD) information, and Department of Justice information; and Icons-Studio/stock.adobe.com (icons). | GAO-25-108500

Accessible Data for Figure 2: Illustrative Examples of Fraud Perpetrated Against the Department of Defense

One who has a part or is involved in a fraud scheme	A process, technique, or system for executing a fraud activity	The results of fraudulent activity, both direct and indirect, such as on people, industries, public bodies, services, and the environment
A contractor using a U.S. shell company...	Falsely claimed U.S. ownership to receive government contracts, sent restricted military data to a foreign manufacturer, and ultimately supplied DOD with defective military parts...	Which grounded at least 47 F-15 fighter aircraft.
Two DOD contracting companies...	Misrepresented their ownership statuses to bid on contracts for which they were not eligible...	Which defrauded the United States of more than \$200 million.

One who has a part or is involved in a fraud scheme	A process, technique, or system for executing a fraud activity	The results of fraudulent activity, both direct and indirect, such as on people, industries, public bodies, services, and the environment
A DOD contracting company...	Falsified documents to conceal its failure to maintain required manufacturing standards and produced gun parts with number of deficiencies...	Which defrauded the DOD of \$124,000 and posed potential safety hazards and had potential national security impacts.
The owner of a DOD contracting firm...	Bribed U.S. Navy officials in exchange for classified and confidential information and preferential treatment in the contracting process...	Which defrauded the Navy of tens of millions of dollars.
A DOD contractor who created and controlled another company...	Concealed the relationship and instructed the company to fraudulently mark up prices on items that were resold to DOD...	Which defrauded DOD of \$48 million.


Sources: GAO analysis of federal court documents, Department of Defense (DOD) information, and Department of Justice information; and Icons-Studio/stock.adobe.com (icons). | GAO-25-108500

DOD Has Begun to Implement Fraud Risk Management Leading Practices But Sustained Effort Is Needed for Full Implementation

DOD Has a Dedicated Entity to Oversee Fraud Risk Management but Has Not Fully Established a Conducive Organizational Culture

Fraud Risk Framework Component

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



Source: GAO. | GAO-25-108500

The first component of the Fraud Risk Framework—commit—calls for managers to create a structure with a dedicated entity to lead fraud risk management activities and an organizational culture to combat fraud at all levels of the agency. DOD has designated its Office of the Under Secretary of Defense (Comptroller) as the dedicated entity to oversee fraud risk management at the department. In this role, the Comptroller leads a Fraud Reduction Task Force—a cross-functional team represented by subject matter experts across the department — to prioritize fraud risks and identify solutions. The Comptroller

also issues guidance on fraud risk management activities, such as fraud-risk-assessment and reporting requirements, and has taken some steps to implement our fraud-related recommendations.

However, as we found in 2021, the Comptroller needs to take additional steps to effectively design and oversee the department's antifraud activities to establish an organizational culture conducive to fraud risk management.¹⁵ Although DOD designated the Comptroller as its dedicated fraud risk management entity, the Comptroller does not have necessary authority over the military components to carry out fraud risk management activities. The Comptroller also has not documented the roles and responsibilities of all oversight officials involved with fraud risk management or the chain of accountability for implementing DOD's fraud-risk-management approach, as we recommended.

Comptroller officials told us in 2021 that they had not yet identified these roles and responsibilities because they were prioritizing financial auditability. Throughout 2024 and 2025, DOD told us that it plans to revise its fraud risk management strategy to address this recommendation and others, and most recently provided a completion deadline of June 2025. We will continue to monitor DOD's promised update to its fraud risk management strategy. Given its significant fraud exposure and requirements for managing fraud risk, DOD leadership needs to give equal consideration to enhancing the department's fraud risk management efforts throughout its many programs and operations as it does to other priorities, such as financial auditability.¹⁶ An effective system of internal controls can help DOD produce reliable, useful, and timely financial information and prevent and detect fraud.

Additionally, words and actions by DOD leadership have called into question its commitment to combating fraud. As previously noted, in November 2024 officials informed us that they did not believe there was much fraud within the department relative to its overall spending. Until DOD officials recognize the threats that fraud pose to its resources and warfighter, it is not well positioned to fight fraud.

Further, DOD has delayed implementing other related recommendations we have made. DOD initially disagreed with more than half of the 17 recommendations made across three reports. Despite subsequently deciding to act in several instances, it has made slow progress in implementation. As a result of these delays, 13 recommendations remain open as of May 2025, including two that will be designated as priority recommendations.¹⁷ These two forthcoming priority recommendations call for DOD to establish data analytics as a method for preventing, detecting, and responding to fraud and to direct components to plan and conduct regular fraud risk assessments that align with leading practices in the Fraud Risk Framework. Together, these recommendations have the potential to significantly

¹⁵[GAO-21-309](#).

¹⁶As of fiscal year 2024, DOD is the only one of the 24 agencies subject to the Chief Financial Officers Act of 1990 that has never obtained an unmodified or "clean" audit opinion on its financial statements, primarily due to serious financial management and system weaknesses. Since 1995, we have designated DOD financial management as a high-risk area. [GAO-25-107743](#).

¹⁷GAO, *Priority Open Recommendations: Department of Defense*, [GAO-25-108042](#) (forthcoming). Priority recommendations are the GAO recommendations that have not been implemented and warrant attention from heads of key departments or agencies because their implementation could save large amounts of money; improve congressional or executive branch decision-making on major issues; eliminate mismanagement, fraud, and abuse; or ensure that programs comply with laws and funds are legally spent, among other benefits.

improve DOD fraud risk management and position the department to better prevent, detect, and respond to fraud.

DOD Provides Some Guidance on Identifying Fraud Risks but Does Not Comprehensively Assess Risks in a Fraud Risk Profile

Fraud Risk Framework Component

Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.



Source: GAO. | GAO-25-108500

The second component of the Fraud Risk Framework—assess—calls for federal managers to plan regular fraud risk assessments and to assess risks to determine a fraud risk profile. Our previous work found that DOD requires components to annually identify fraud risks and report the results of the risk assessments to the Comptroller.¹⁸ DOD provides guidance, tools, and training for military components to conduct fraud risk assessments.

However, DOD does not comprehensively identify and assess risks during the fraud risk assessment process, as called for in leading practices. DOD has assigned the identification, assessment, and reporting of fraud risks to its components, but we found in 2021 that not all components reported on certain types of fraud risk, such as procurement fraud risk.¹⁹ Comptroller officials told us they were aware that these components did not identify any procurement fraud risk in their risk assessments and acknowledged that it is a challenge to have a complete understanding of fraud risks, given that the components' fraud risk assessments varied in completeness and information provided.

In 2023, the Comptroller updated DOD guidance to direct components to plan and conduct regular fraud risk assessments that align with leading practices in the Fraud Risk Framework. We identified some improvements in components' fraud risk assessments as a result. However, we also noted in

¹⁸GAO-21-309.

¹⁹GAO-21-309.

2023 that not all components' fraud risk assessments aligned with leading practices, such as identifying inherent procurement fraud risks and determining fraud risk tolerance.²⁰

DOD also does not comprehensively compile a fraud risk profile in alignment with the second component of the Fraud Risk Framework.²¹ The Comptroller consolidates the risks reported in the components' fraud risk assessments and uses this information to update the department-wide fraud risk profile. Because the components' fraud risk assessments may lack information on certain types of fraud risk, the Comptroller cannot ensure that the department's documented fraud risk profile is complete or accurate. In addition, the Comptroller does not obtain and analyze relevant information on adjudicated procurement fraud cases from the DOD Office of Inspector General and the Secretaries of the Navy, Air Force, and Army, as we recommended in 2024.²²

Without obtaining and analyzing such information, DOD may not fully assess its fraud risks or design and implement data-analytics activities to prevent or detect these risks. In response to our 2024 recommendation, DOD established a Confirmed Fraud Working Group consisting of members of the military criminal investigative organizations and the Risk Management Internal Control Program. According to DOD officials, the Confirmed Fraud Working Group will work to collect and analyze adjudicated confirmed fraud cases to identify root causes, lessons learned, and other relevant information by November 2025.

²⁰According to *Standards for Internal Control in the Federal Government*, a risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. In the context of fraud risk management, if the objective is to mitigate fraud risks—in general, to have a very low level of fraud—the risk tolerance reflects managers' willingness to accept a higher level of fraud risks, and it may vary, depending on the circumstances of the program.

²¹A fraud risk profile is a documented analysis that identifies internal and external fraud risks, their perceived likelihood and impact, managers' risk tolerance, and the prioritization of risks. It is an essential piece of an overall antifraud strategy and can inform the specific control activities that managers design and implement.

²²[GAO-24-105358](#).

DOD Issued an Antifraud Strategy but Does Not Fully Include Control Activities That Align with Leading Practices

Fraud Risk Framework Component

Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.



Source: GAO. | GAO-25-108500

The third component of the Fraud Risk Framework—design and implement—calls for managers to design and implement a strategy with specific control activities to mitigate assessed fraud risks and to collaborate to help ensure effective implementation. DOD issued an inaugural fraud risk management strategy in July 2020 and an updated version in August 2023.²³ When discussing the strategy update prior to its issuance, the Comptroller noted the importance of ensuring that the strategy provides long-term guidance and clarity about DOD’s fraud risk management efforts.

DOD’s current antifraud strategy includes some control practices that have been designed and implemented to prevent, detect, and respond to fraud, such as the creation of the Fraud Reduction Task Force. However, we found it has not established data analytics as a method for preventing, detecting, and responding to fraud. As a leading practice under the Fraud Risk Framework’s third component, and as our analytical work has shown, data-analytics activities are an important part of an effective antifraud strategy.²⁴ 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. These activities can also help inform DOD’s decision-making and mitigate assessed fraud risks.

In February 2024, we found that DOD’s fraud risk management strategy generally refers to data-analytics goals, roles, responsibilities, and activities.²⁵ However, it does not fully leverage data analytics in accordance with leading practices in the Fraud Risk Framework, as we recommended. For example, DOD’s strategy does not fully discuss designing and implementing system edit checks, data matching, and data mining; combining data across programs to facilitate analytics; or pursuing access to

²³Department of Defense, *Fraud Risk Management Strategy and Guidance*, (August 2023).

²⁴[GAO-24-105358](#).

²⁵[GAO-24-105358](#).

necessary external data. Further, it does not identify which entity has the authority to ensure that fraud-related data-analytics activities are implemented, as we recommended.

Our analysis of alleged and adjudicated DOD procurement fraud cases demonstrated how information from investigative case data could help inform DOD's fraud risk management consistent with leading practices in the Fraud Risk Framework. Despite this potential, DOD's antifraud strategy does not include plans for obtaining and analyzing the information that can be gleaned from such data.²⁶ Until DOD obtains information on relevant adjudicated procurement fraud cases, DOD's ability to conduct DOD fraud-related data analytics to inform its risk management efforts will be limited.

In 2024, DOD indicated that it planned to publish a revised fraud risk management strategy to address several of our open recommendations, including establishing data analytics as a method for preventing, detecting, and responding to fraud. However, it has delayed implementing its updated strategy five times over 7 months. Officials stated that recent leadership transitions have delayed finalizing the strategy's publication and that they now expect to finish revising it to address all relevant recommendations by July 2025. Until DOD leadership commits to developing and implementing a comprehensive antifraud strategy that effectively aligns with leading practices, the department remains at substantial risk of fraud against its programs. We found that DOD could save a significant amount—one hundred million dollars or more—by implementing our fraud risk management recommendations related to using data analytics to prevent, detect, and respond to fraud.²⁷

Given the significant fraud exposure and requirements for managing fraud risk, DOD leadership should enhance the department's fraud risk management efforts throughout its many programs and operations. This includes fully implementing counter-fraud activities to better understand the totality of its fraud risk exposure and implementing controls to readily prevent, detect, and respond to fraud.

Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions you may have.

GAO Contacts and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Seto J. Bagdoyan, Director, Forensic Audits and Investigative Service at BagdoyanS@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Heather Dunahoo (Assistant Director), Samantha Sloate (Analyst in Charge), Jasmina Clyburn, Colin Fallon, and Joseph Rini.

²⁶We 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 about relevant adjudicated procurement fraud case data.

²⁷GAO, *Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve an Additional One Hundred Billion Dollars or More in Future Financial Benefits*, [GAO-25-107604](https://www.gao.gov/products/GAO-25-107604) (Washington, D.C.: May 13, 2025).

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.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on [X](#), [LinkedIn](#), [Instagram](#), and [YouTube](#).

Subscribe to our [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

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

A. Nicole Clowers, Managing Director, CongRel@gao.gov

General Inquiries

<https://www.gao.gov/about/contact-us>