



November 2019

# DEFENSE PROCUREMENT

## Ongoing DOD Fraud Risk Assessment Efforts Should Include Contractor Ownership

## Why GAO Did This Study

DOD generally accounts for about two-thirds of federal contracting activity. Some companies doing business with DOD may have an opaque ownership structure that conceals other entities or individuals who own, control, or financially benefit from the company. Opaque ownership could be used to facilitate fraud and other unlawful activity.

The House Armed Services Committee report on the National Defense Authorization Act for fiscal year 2018 included a provision for GAO to examine the risks posed by contractors with opaque ownership and DOD's processes for identifying ownership. This report identifies types of fraud and other risks that opaque contractor ownership poses to DOD in the procurement process and assesses whether DOD has taken steps to address those risks. GAO reviewed applicable laws and regulations and interviewed DOD officials, including procurement staff and criminal investigators. GAO researched cases from 2012–2018 where contractors may have concealed or failed to disclose ownership information. GAO compared DOD's efforts to leading practices in GAO's Fraud Risk Framework. This is a public version of a sensitive report that GAO issued in September 2019. Information that DOD deemed sensitive involving ongoing investigations and certain internal controls and vulnerabilities has been omitted.

## What GAO Recommends

GAO recommends that DOD assess risks related to contractor ownership as part of DOD's ongoing efforts to assess fraud risk. DOD should use this information to inform other types of risk assessments, including national security concerns. DOD concurred with GAO's recommendation.

View [GAO-20-106](#). For more information, contact Seto J. Bagdoyan at (202) 512-6722 or [bagdoyans@gao.gov](mailto:bagdoyans@gao.gov).

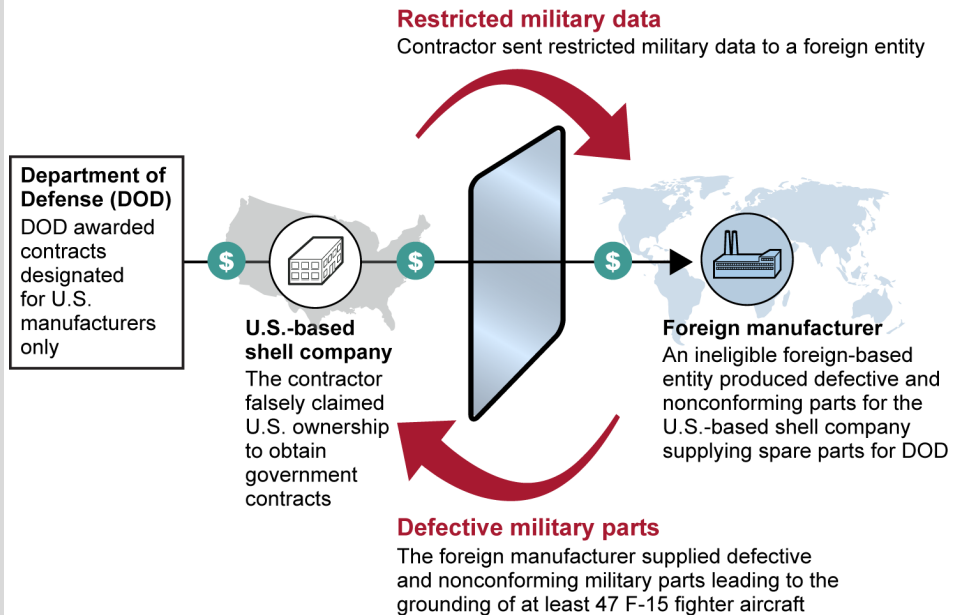
# DEFENSE PROCUREMENT

## Ongoing DOD Fraud Risk Assessment Efforts Should Include Contractor Ownership

### What GAO Found

The Department of Defense (DOD) faces several types of financial and nonfinancial fraud and national security risks posed by contractors with opaque ownership. These risks, identified through GAO's review of 32 adjudicated cases, include price inflation through multiple companies owned by the same entity to falsely create the appearance of competition, contractors receiving contracts they were not eligible to receive, and a foreign manufacturer receiving sensitive information or producing faulty equipment through a U.S.-based company. For example, one case involved an ineligible foreign manufacturer that illegally exported sensitive military data and provided defective and nonconforming parts that led to the grounding of at least 47 fighter aircraft, as illustrated below.

#### Ineligible Foreign Manufacturer Fraudulently Obtaining DOD Contracts



Source: GAO analysis of federal court records. | GAO-20-106

DOD has taken some steps that could address some risks related to contractor ownership in the procurement process but has not yet assessed these risks across the department. DOD, in coordination with other agencies, revised the Federal Acquisition Regulation in 2014 to require contractors to self-report some ownership information. DOD has taken steps to identify and use ownership information—for example, as part of its supply-chain risk analysis when acquiring critical components. DOD has also begun a department-wide fraud risk management program, but it has neither assessed risks of contractor ownership across the department nor identified risks posed by contractor ownership as a specific area for assessment. Assessing risks arising from contractor ownership would allow DOD to take a strategic approach to identifying and managing these risks, make informed decisions on how to best use its resources, and evaluate its existing control activities to ensure they effectively respond to these risks.

---

# Contents

---

---

Letter		1
	Background	5
	DOD Contractors with Opaque Ownership Can Pose a Range of Fraud and National Security Risks in the Procurement Process	13
	DOD Has Taken Steps That Could Address Some Risks Related to Contractor Ownership and Has Opportunities to Systematically Assess These Risks	29
	Conclusions	42
	Recommendation for Executive Action	43
	Agency Comments	43
Appendix I	Objectives, Scope, and Methodology	46
Appendix II	Summary of GAO Review of Cases Adjudicated or Settled from Calendar Years 2012 through 2018	50
Appendix III	GAO Contact and Staff Acknowledgments	61
Table		
	Table 1: Summary of GAO Review of 32 Court Cases of Department of Defense (DOD) Contractor Ownership-Related Fraud Adjudicated or Settled from Calendar Years 2012 through 2018	51
Figures		
	Figure 1: Illustrative Example of Contractor Ownership Opacity	6
	Figure 2: Federal Acquisition Regulation Offeror Ownership Requirement	8
	Figure 3: DOD Contractor Concealing Ownership to Fraudulently Inflate Prices	15
	Figure 4: Example of Potentially Related Offerors Bidding on the Same DOD Solicitation Who Shared the Same Addresses and Management Team	18

---

---

Figure 5: Example of Potentially Related Offerors Bidding on the Same DOD Solicitation, One of Whom Was Excluded from Doing Business with the Government	19
Figure 6: Example of Potentially Related Offerors Bidding on the Same DOD Solicitation Who Shared Information	21
Figure 7: Example of Two Offerors and a Subcontractor for a Third Offeror Who Shared Information Bidding on the Same DOD Solicitation	22
Figure 8: Service-Disabled Veteran–Owned Small-Business Fraud Scheme	25
Figure 9: Ineligible Foreign Manufacturer Fraudulently Obtaining DOD Contracts	26
Figure 10: GAO’s Fraud Risk Management Framework	41

---

### Abbreviations

DCMA	Defense Contract Management Agency
DIA	Defense Intelligence Agency
DLA	Defense Logistics Agency
DOD	Department of Defense
DOJ	Department of Justice
DSS	Defense Security Service
FAPIIS	Federal Awardee Performance and Integrity Information System
FAR	Federal Acquisition Regulation
FBO	Federal Business Opportunities
Fraud Risk Framework	A Framework for Managing Fraud Risks in Federal Programs
FRDAA	Fraud Reduction and Data Analytics Act of 2015
GSA	General Services Administration
OSD	Office of the Secretary of Defense
OUSD(C)	Office of the Under Secretary of Defense (Comptroller)
SAM	System for Award Management

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.



November 25, 2019

### Congressional Committees

The Department of Defense (DOD) is the largest contracting agency in the federal government, generally accounting for about two-thirds of all federal contracting activity. In fiscal year 2018, DOD obligated over \$350 billion in contracts for goods and services and awarded over 570,000 new contracts to approximately 38,000 contractors. DOD awards contracts to companies in the private sector to provide a wide variety of services for U.S. military forces. Of the thousands of contractors doing business with DOD, some companies are what are known as shell companies—that is, companies that exist but conduct either no business or minimal business. Shell companies can be used for legitimate purposes; for example, they may be formed to obtain financing before starting operations. However, companies sometimes use shell companies to form opaque ownership structures designed to disguise the beneficial owner—the natural person or persons who directly or indirectly own and control, or receive substantial economic benefit from, a company. These opaque ownership structures can be used to facilitate fraud and other unlawful activity in commerce, including contracts with DOD. For this report, we define opaque ownership as structures of business governance that may conceal or obfuscate entities or individuals who own, control, or benefit financially from a business.<sup>1</sup>

In the committee report on the National Defense Authorization Act for fiscal year 2018, the House Armed Services Committee expressed concerns that DOD contractors may disguise their identities and cost structures from procurement officers, in effect acting as hidden monopolies with unreasonable prices or establishing opaque ownership structures for benefits that are contrary to the government's interest.<sup>2</sup> The committee report included a provision that GAO examine DOD's processes to identify contractors' ownership structures and the risks posed to DOD by contractors with opaque ownership structures. This

---

<sup>1</sup>This report uses terminology to refer to companies or entities that have distinct meanings. An entity is a broad term that includes, among other things, corporations, limited liability companies, or other legal bodies that are created by filing with a Secretary of State or similar office. An entity becomes an offeror upon submitting a response to a government solicitation. An entity becomes a contractor upon award of a contract.

<sup>2</sup>H. Rep. No. 115-200, at 156 (2017).

---

report (1) identifies types of fraud and other risks, if any, that contractors with opaque ownership could pose to DOD in the procurement process and (2) assesses whether DOD has taken steps to address risks posed by contractor ownership in the procurement process.

This report is a public version of a sensitive report that we issued on September 12, 2019.<sup>3</sup> The sensitive report included the results of data analysis we conducted to identify offerors who might disguise their ownership to create the appearance of competition. DOD deemed some of the details from this analysis to be sensitive, which must be protected from public disclosure. This report also omits sensitive information about ongoing investigations, certain internal controls and vulnerabilities, and actions taken to address some of these vulnerabilities. Although the information provided in this report is more limited, it addresses the same overall objectives as the sensitive report and uses the same methodology.

To address our first objective, we researched information on closed cases investigated by the Defense Criminal Investigative Organizations or prosecuted by the Department of Justice (DOJ) from calendar years 2012 through 2018.<sup>4</sup> We also researched legal databases and news articles involving DOD contractors to identify federal court cases and agency decisions. We reviewed GAO bid-protest decisions to identify cases in which contractors may have failed to disclose foreign ownership or concealed beneficial-owner information to obtain contracts that they were not eligible to receive. For each of the 32 cases identified, we reviewed associated federal court filings or DOJ press releases. To identify additional types of risks that may not have been identified through our case-study research, we interviewed officials from the General Services Administration (GSA) and officials across DOD, including the Office of Inspector General, Defense Criminal Investigative Organizations, Defense Pricing and Contracting, Office of the Under Secretary of

---

<sup>3</sup>GAO, *Defense Procurement: Ongoing DOD Fraud Risk Assessment Efforts Should Include Contractor Ownership*, GAO-19-549SU (Washington, D.C.: Sept. 12, 2019).

<sup>4</sup>Defense Criminal Investigative Organizations refers to the Defense Criminal Investigative Service, the Army Criminal Investigation Command, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations, collectively. We chose this period to capture cases adjudicated or settled within 5 years of when we began our audit work. Given that it takes time for cases of alleged fraud to be adjudicated or settled, the fraudulent transactions that are described in these 32 cases may have actually occurred prior to 2012.

---

Defense (Comptroller) (OUSD[C]), Office of the Chief Information Officer, Defense Intelligence Agency (DIA), Defense Security Service (DSS), Defense Logistics Agency (DLA), Defense Contract Management Agency (DCMA), and Defense Contract Audit Agency, and relevant procurement policy officials from the Departments of the Army, Navy, and Air Force. We examined known risks identified through our case-study research and interviews with DOD officials; however, these risks are not necessarily representative of the extent or the types of presently undiscovered fraud or other risks that may exist across DOD.

We further examined the risk that contractors could be disguising their ownership to create the appearance of competition by analyzing bid response data on approximately 2,700 solicitations from GSA's Federal Business Opportunities website and offeror registration data from GSA's System for Award Management (SAM) for fiscal years 2015 through 2017. We selected this date range because fiscal year 2015 was the first year in which offerors were required to report ownership and 2017 was the most-recent complete year of data at the time of our analysis. To identify whether offerors were potentially related, we analyzed information to identify instances in which different offerors shared certain information.<sup>5</sup> Offerors sharing information does not definitively prove that the offerors are related or share ownership; however, it is an indicator that these offerors may not be independent of each other. The results of our analysis are limited to the approximately 2,700 solicitations we reviewed and are not generalizable to other DOD solicitations. To assess the reliability of these data, we performed electronic testing, reviewed related documents, and compared the data to published sources and source documentation maintained in the DOD contracting files. We also interviewed GSA officials responsible for these databases. We determined that the data were sufficiently reliable for the purposes of analyzing potential ownership relationships.

To address our second objective, we reviewed federal laws, the Federal Acquisition Regulation (FAR), DOD regulations, directives, instructions, policies, procedures, and training documents. We also reviewed OUSD(C) fraud assessment templates and preliminary results from the department's fraud risk management pilot program. We interviewed procurement policy officials from GSA, Defense Pricing and Contracting,

---

<sup>5</sup>Additional details discussing the methodology of our analysis and specific information shared by different offerors were deemed sensitive by DOD and have been omitted from this report.

---

DLA, and the Departments of the Army, Navy, and Air Force as well as officials from the Office of the Chief Information Officer, OUSD(C), DIA, DSS, DCMA, the Defense Contract Audit Agency, the Joint Staff Logistics Directorate, the Defense Industrial Policy office, members of DOD's Procurement Fraud Working Group, and the Naval Contracting Council to discuss how DOD has addressed risks. To assess these efforts, we compared these documents and the information from our interviews to federal internal control standards and the leading practices outlined in GAO's Framework for Managing Fraud Risks in Federal Programs (Fraud Risk Framework).<sup>6</sup> We contacted several government contractors' associations to gain members' perspectives on reporting beneficial ownership information and received feedback from 16 members of three government contractors' associations. The perspectives gained from our queries are not generalizable to all contractors. For more-detailed information on our scope and methodology, see appendix I.

The performance audit upon which this report is based was conducted from August 2017 to September 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with DOD from September 2019 to November 2019 to prepare this version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

---

<sup>6</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014); and *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 2015).

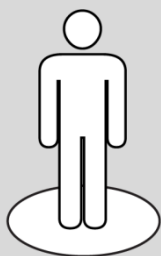


---

---

## Background

Entities seeking to do business with DOD may have opaque ownership structures that obscure ownership or control by other entities or individuals.



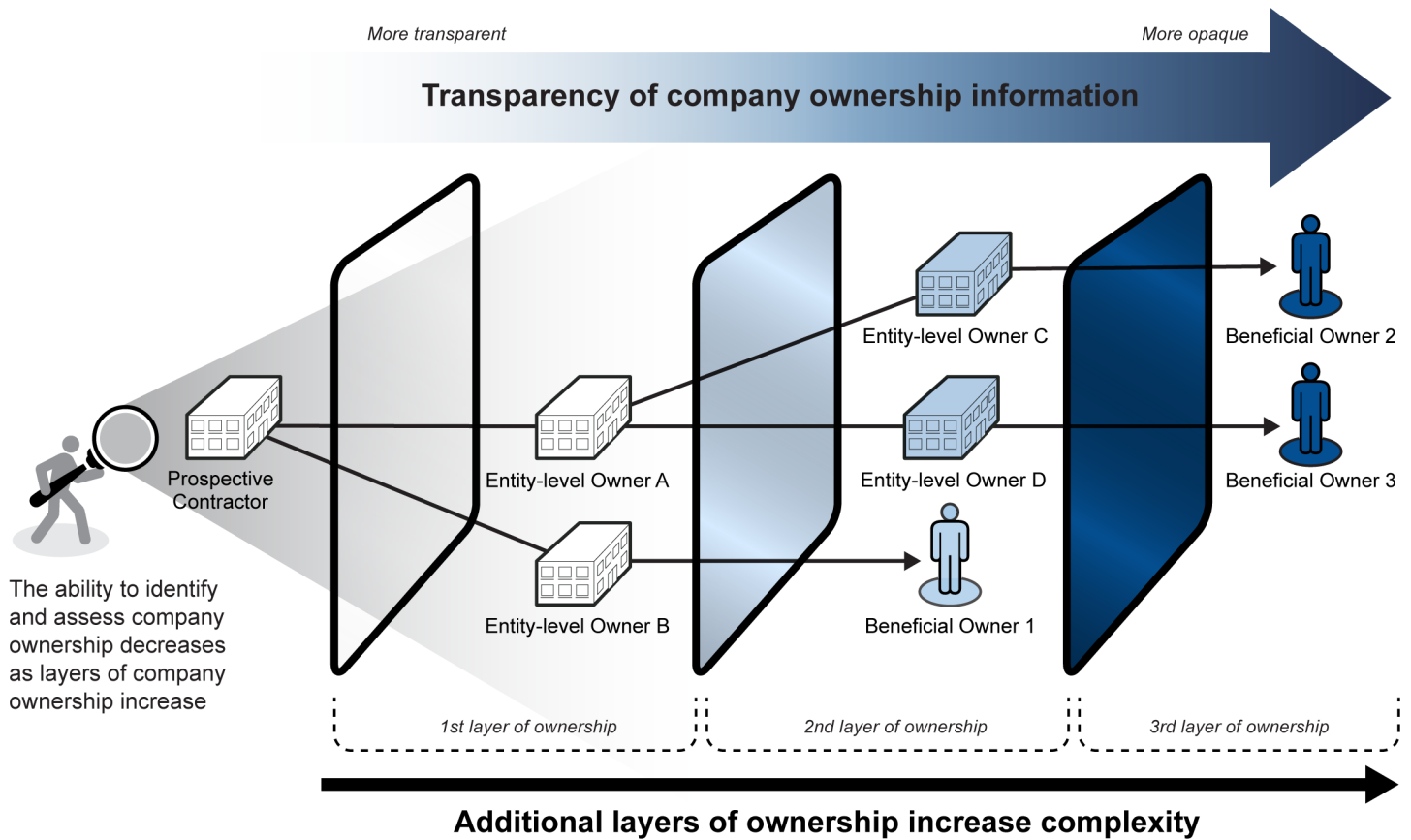
### **Beneficial Owner**



For the purposes of this report, we define a beneficial owner as the natural person or persons who directly or indirectly own and control, or receive substantial economic benefit from, a company.

Source: GAO. | GAO-20-106

As the number of layers of ownership increases, ownership information becomes more opaque, as shown in figure 1. This opacity can make it difficult for DOD to determine which entities and individuals ultimately own or control its contractors.

**Figure 1: Illustrative Example of Contractor Ownership Opacity**



- 
**Entity-level Owner**  
 An entity-level owner is a legal entity that owns another company and includes, among other things, corporations, limited liability companies, or other entities that are created by filing with a Secretary of State or similar office.
- 
**Beneficial Owner**  
 A beneficial owner is the natural person or persons who directly or indirectly own and control, or receive substantial economic benefit from, a company.

Source: GAO. | GAO-20-106

## Identifying Business Ownership Information

In the United States, no centralized information source or national registry maintains company ownership information. In 2014, the National Association of Secretaries of State found that most states collect minimal

---

ownership data.<sup>7</sup> The association reviewed key information collected by the 50 states and the District of Columbia during the entity-formation process and in annual or periodic reports. During both the entity-formation process and in annual or periodic reporting, the association found that very few states collect some form of entity ownership or control information from limited liability companies or corporations.

The Securities and Exchange Commission collects some ownership information on publicly traded companies. Any person or group of persons that acquires beneficial ownership of more than 5 percent of a publicly traded company's registered voting securities must register with the Securities and Exchange Commission. Institutional investment managers regularly disclose their holdings, and company officers, directors, and holders of more than 10 percent of a class of the company's registered equity securities must file a statement of ownership with the Securities and Exchange Commission.

---

## System for Award Management and Ownership Information

GSA's SAM is a federal government-wide database for vendor data that is used across all federal agencies. Any entity that wishes to do business with the government must register in SAM to be eligible to receive a contract award, except in specific circumstances outlined in the law and FAR.<sup>8</sup>

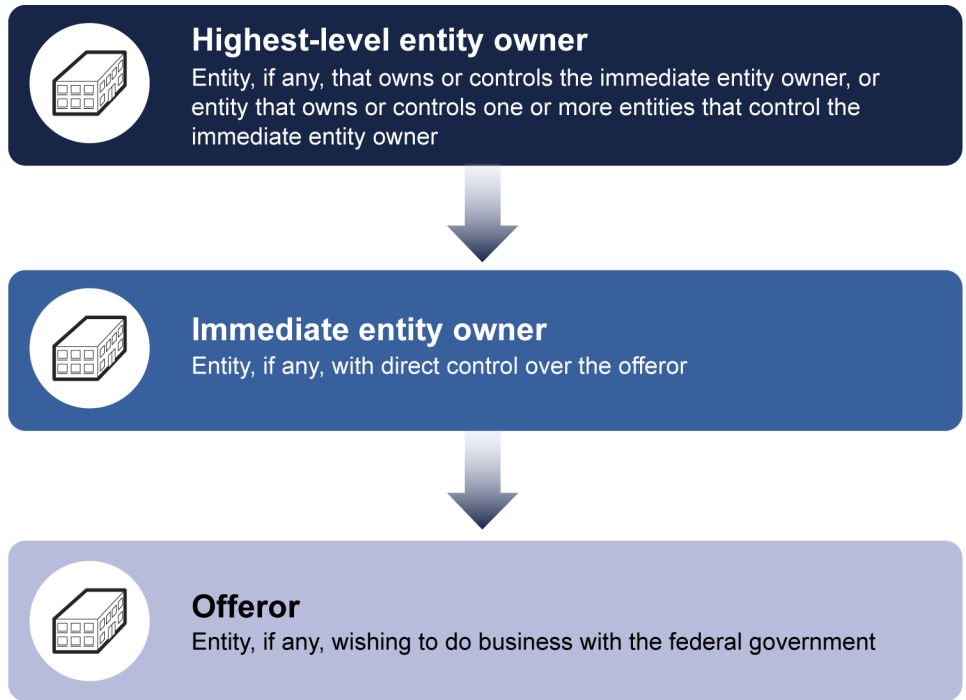
To increase procurement transparency and traceability, and broaden the government's ability to implement fraud-detection technologies, the FAR was amended to begin requiring entities that wish to do business with the federal government to provide additional ownership information through the annual registration process in SAM starting on November 1, 2014. The required ownership information includes the "immediate" and "highest" level ownership of an offeror, as shown in figure 2 below. The FAR includes a requirement for ownership to be provided at the entity level. There is no requirement for offerors to report their beneficial owners.

---

<sup>7</sup>Additionally, previous GAO work also found that most states do not require ownership information at the time a company is formed. GAO, *Company Formations: Minimal Ownership Information Is Collected and Available*, [GAO-06-376](#) (Washington, D.C.: Apr. 7, 2006).

<sup>8</sup>FAR § 4.1102.

**Figure 2: Federal Acquisition Regulation Offeror Ownership Requirement**



Source: Federal Acquisition Regulation. | GAO-20-106

### Evaluation of Prospective Contractors before Contract Award

The FAR contains several provisions governing the selection of an offeror. Provisions such as price and past performance of the offeror are generally applicable in determining which offeror should win a contract. Additional requirements may apply to certain types of procurements, such as the procurement of national security systems. We outline several of the relevant FAR provisions; however, this does not represent a comprehensive list of all steps required by the FAR in making contract-award decisions.

### Responsibility Determination

A prospective contractor must affirmatively demonstrate its responsibility, including, when necessary, the responsibility of its proposed subcontractors. Contracting officers must then determine the responsibility of prospective contractors, including whether prospective contractors can perform the terms of a contract. To be determined responsible, a prospective contractor must have adequate financial resources to perform the contract (or the ability to obtain them); be able to comply with the required delivery or performance schedule; have a

---

satisfactory performance, integrity, and ethics record; have the necessary organization, experience, accounting and operational controls, and facilities to carry out the contract (or the ability to obtain them); and be otherwise qualified and eligible to receive an award under applicable laws and regulations.<sup>9</sup>

Before awarding a contract over the simplified acquisition threshold (generally \$250,000 at the time of our review), a contracting officer must review the prospective contractor's performance and integrity information available in the Federal Awardee Performance and Integrity Information System (FAPIS).<sup>10</sup> FAPIS is a federal government-wide database designed to assist contracting officers with making a responsibility determination by providing integrity and performance information of covered federal agency contractors and grantees. FAPIS provides a prospective contractor "Report Card" that includes information pertaining to the prospective contractor's past performance (if applicable), such as any administrative agreements, contract terminations, nonresponsibility determinations, and exclusions, among other things. It also includes the ability to view the company relationship information, which details the ownership information that prospective contractors are required to report in SAM.<sup>11</sup> When making a responsibility determination, the contracting officer must consider all the information available through FAPIS with regard to the prospective contractor and any immediate owner, predecessor (an entity that the prospective contractor replaced by acquiring assets and carrying out affairs under a new name), or subsidiary identified for that prospective contractor in FAPIS.<sup>12</sup> The contracting officer must document in the contract file how the information in FAPIS was considered in any responsibility determination, as well as the action that was taken as a result of the information.<sup>13</sup>

DCMA can play a role in supporting contracting officials in making responsibility determinations. For example, DCMA officials stated that

---

<sup>9</sup>FAR §§ 9.103, 9.104-1.

<sup>10</sup>FAR § 9.104-6(a)(1).

<sup>11</sup>Company relationship information includes the immediate and highest-level ownership information reported in SAM. It does not provide information on other subsidiaries owned by the owner.

<sup>12</sup>FAR § 9.104-6(b)(1).

<sup>13</sup>FAR § 9.104-6(d).

---

they may provide information on a company's business systems, financial capabilities, and company history, and assess whether the prospective contractor is likely to stay in business for the duration of the contract. When assessing the capacity to perform a contract, DCMA officials stated they examine company assets as a whole, including any parent company, to make a determination. According to officials, DCMA's goal for identifying the organizational structure is to determine whether the company as a whole has the assets to perform the contract rather than to identify fraud or other risks that may be associated with that company. The level and type of support that DCMA provides to contracting officials depends on the particular needs of contracting officials for any given procurement. Some contracts require contractors to comply with cost-accounting standards and submit disclosures of their cost-accounting practice to show from which specific business units they receive allocations and to which specific business units they pass allocations; however, these disclosures are only required after a contract that is covered by cost-accounting standards is awarded.<sup>14</sup>

## Source Selection

Contract award decisions are based on evaluation factors and significant subfactors that are tailored to the procurement, at the discretion of procurement officials. At a minimum, these factors must include: price/cost, quality, and past performance.<sup>15</sup>

Federal law grants DOD additional authority to use public and nonpublic information to make source-selection decisions when acquiring national security systems.<sup>16</sup> DOD may exclude an offeror if necessary to protect national security by reducing supply-chain risk.<sup>17</sup> Under this authority,

---

<sup>14</sup>41 U.S.C. § 1501–1506 established the Cost Accounting Standards Board to prescribe, amend, and rescind cost-accounting standards to achieve uniformity and consistency in cost-accounting standards. These standards help the government determine cost allocation for contracts.

<sup>15</sup>FAR § 15.304(c). Past performance is evaluated for procurements that are expected to exceed the simplified acquisition threshold.

<sup>16</sup>10 U.S.C. 2339a. The term “national security system” generally means any information systems, including weapons systems, that involve activities related to national security, military security, or intelligence activities, among other things.

<sup>17</sup>Supply-chain risk means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

---

DOD does not have to disclose the reason an offeror was excluded, nor can the offeror protest DOD's decision.

Competition Generally  
Establishes Price  
Reasonableness

The FAR requires contracting officers to purchase supplies and services from responsible sources at fair and reasonable prices.<sup>18</sup> For negotiated contracts, price reasonableness is ordinarily established by adequate competition, such as when there are more than two responsible offerors competing independently.<sup>19</sup> For noncompetitive purchases with only one offeror, the contracting officer must obtain certified cost or pricing data, or data other than certified cost or pricing data, as necessary to establish a fair and reasonable price. Procurements with only one offeror may still be considered competitive if there was a reasonable expectation that two or more responsible and independent offerors would submit offers and the offeror submitted the offer with the expectation of competition.<sup>20</sup>

Never Contract with the Enemy

Section 841 of the 2015 National Defense Authorization Act grants DOD and other federal agencies the authority to limit contracts with entities that provide funds to a person or group that actively opposes U.S. or coalition forces involved in a contingency operation in which members of the armed forces are actively engaged in hostilities.<sup>21</sup> It also allows agencies to terminate for default, void, or restrict the award of a contract to any contractor that provides funds received under a federal contract directly or indirectly to entities actively opposing U.S. forces engaged in hostilities.

---

Fraud and Fraud Risk  
Definitions

Fraud and "fraud risk" are distinct concepts. Fraud involves obtaining something of value through willful misrepresentation and is challenging to detect because of its deceptive nature. 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. When fraud risks can be identified and mitigated, fraud may be less likely to occur.

---

<sup>18</sup>FAR § 15.402.

<sup>19</sup>FAR § 15.305. Negotiated procurements are either sole-source or competitive procurements and allow for negotiation between the government and offeror on the price of the contract.

<sup>20</sup>FAR § 15.403.

<sup>21</sup>Pub. L. No. 113-291, § 841 (2015), 10 U.S.C. § 2302 note.

---

---

## Fraud Risk Management Standards and Leading Practices

According to federal standards and leading practices, executive-branch agency managers are responsible for managing fraud risks and implementing practices for combating those risks. Federal internal control standards call for agency management officials to assess the internal and external risks their agencies face as they seek to achieve their objectives. The standards state that, as part of this overall assessment, management should consider the potential for fraud when identifying, analyzing, and responding to risks.<sup>22</sup> In July 2015, GAO issued its Fraud Risk Framework, which provides a comprehensive set of key components and leading practices that serve as a guide for agency managers to use when developing efforts to combat fraud in a strategic, risk-based way.<sup>23</sup> The Fraud Risk Framework consists of four components to effectively manage fraud risk: *Assess, Design and Implement, Evaluate and Adapt, and Commit*. The Assess component calls for federal managers to plan regular fraud risk assessments and to assess risks to determine a fraud risk profile. Identifying fraud risks is one of the steps included in the Fraud Risk Framework for assessing risks to determine a fraud risk profile. The fraud risk profile supports the development of a strategy to mitigate fraud risks.

The Fraud Reduction and Data Analytics Act of 2015 (FRDAA), enacted in June 2016, requires the Office of Management and Budget to establish guidelines for federal agencies to create controls to identify and assess fraud risks and to design and implement antifraud control activities.<sup>24</sup> The act further requires the Office of Management and Budget to incorporate the leading practices from the Fraud Risk Framework in the guidelines. In July 2016, the Office of Management and Budget published guidance about enterprise risk management and internal controls in federal executive departments and agencies.<sup>25</sup> Among other things, this guidance affirms that managers should adhere to the leading practices identified in the Fraud Risk Framework. The act also requires federal agencies to submit to Congress a progress report each year for 3 consecutive years on the implementation of the controls established under the Office of

---

<sup>22</sup>[GAO-14-704G](#).

<sup>23</sup>[GAO-15-593SP](#).

<sup>24</sup>Pub. L. No. 114-186, § 3, 130 Stat. 546 (2016).

<sup>25</sup>Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control*, Circular No. A-123 (Washington, D.C.: July 15, 2016).



---

Management and Budget guidelines, among other things. Recent GAO work examined federal agencies that are subject to FRDAA, including DOD, and found that 85 percent of those agencies have started planning and 78 percent have started implementing efforts to meet FRDAA requirements; however, the majority of these efforts were characterized as not being mature.<sup>26</sup> Maturity was determined by agency responses to a survey question that asked whether the agency's status of implementing FRDAA requirements was "not started," "started but not mature," or "mature." The report identified the number and percentage of agencies that fell into each of these status categories, but did not state the level of maturity for any individual agency.

---

## DOD Contractors with Opaque Ownership Can Pose a Range of Fraud and National Security Risks in the Procurement Process

Contractors with opaque ownership structures can pose a range of financial and nonfinancial fraud and national security risks to DOD by misrepresenting or concealing company ownership information to commit fraud against the government or to do harm to U.S. national security concerns.<sup>27</sup> We identified multiple types of fraud and national security risks by examining 32 cases for fraud involving DOD contractors that were adjudicated or settled from calendar years 2012 through 2018 and conducting interviews with knowledgeable DOD officials and criminal investigators. There may be additional risks and cases related to contractor ownership that are not identified below. Court cases we identified were investigated by DOD and other entities based on, for example, information from whistleblowers, defective parts received by DOD, lawsuits involving contractors, and U.S. government officials determining they were receiving false contractor information. As discussed later in this report, DOD has not systematically assessed risks posed by contractor ownership; therefore the magnitude and prevalence of the risks we identified are not known. Appendix II of this report contains a complete listing and additional details of the 32 cases we identified.

---

<sup>26</sup>GAO, *Fraud Risk Management: Office of Management and Budget Should Improve Guidelines and Work-Group Efforts to Support Agencies' Implementation of the Fraud Reduction and Data Analytics Act*, [GAO-19-34](#) (Washington, D.C.: Dec. 4, 2018).

<sup>27</sup>As described earlier, while shell companies can be used to form opaque ownership structures to disguise the beneficial owner of a company to facilitate fraud and other unlawful activity, they can also be used for legitimate business purposes.

---

---

**Contractors with Opaque Ownership Pose Financial Fraud Risks Including Price Inflation**

Contractors can use opaque ownership structures for illicit financial gain through a variety of methods, as described below.

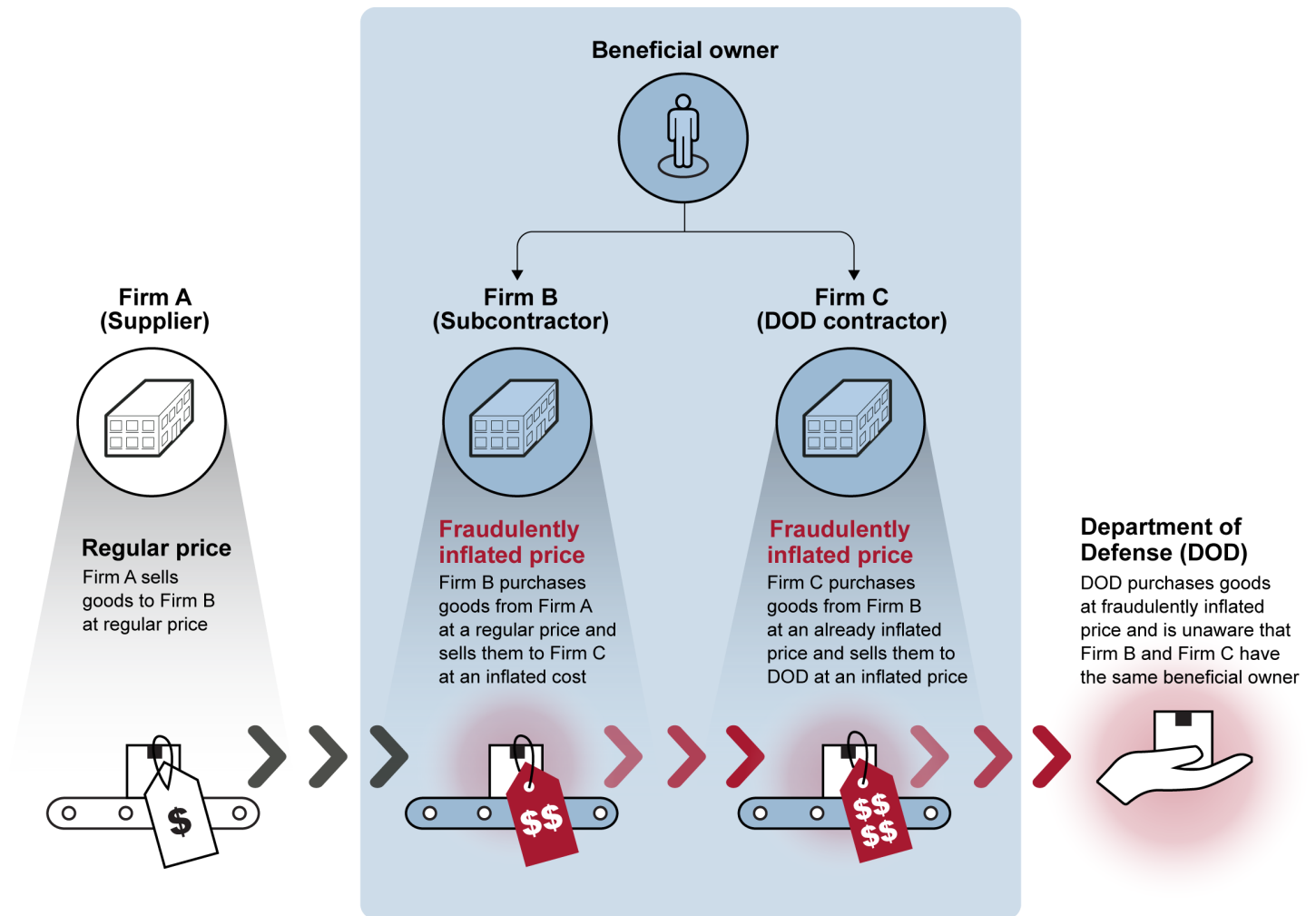
**Concealing relationship with subcontractor to inflate prices.**

Contractors can subcontract with companies they own or control to inflate prices for financial benefit. For example, in a 2014 federal court case we examined, a contractor and another company with common ownership pled guilty to major fraud against the United States. They agreed to pay \$434 million in criminal penalties and to settle a lawsuit in connection with concealing their relationship with a subcontractor that the contractor directed to fraudulently mark up costs on items that the contractor purchased and resold to DOD. Specifically, the contractor purchased goods from a company that its owners created, controlled, and used to make the fraudulent markups appear legitimate. Further highlighting the relationship between the company and the contractor, contractor personnel were also responsible for hiring individuals to work for the subcontractor.<sup>28</sup> The contractor billed the government an artificially high price for the goods from July 2005 through April 2009 and resulted in a loss to DOD of \$48 million. Figure 3 below illustrates this scheme to conceal ownership and fraudulently inflate prices.

---

<sup>28</sup>Additional details about this case were deemed sensitive by DOD and have been omitted from this report.

Figure 3: DOD Contractor Concealing Ownership to Fraudulently Inflate Prices



Source: GAO analysis of federal court records. | GAO-20-106

**Billing for work not performed.** Contractors or subcontractors can bill for work not performed by creating fictitious invoices that add costs to a contract. For example, in four court cases we examined, multiple DOD subcontractors were actually shell companies that did not have the inventory they purported to ultimately provide to the government or perform the work indicated in the contract requirements. According to documents filed in U.S. district court, some of these subcontractors hired other companies to perform work, but created additional invoices that added costs for work the subcontractors did not perform. These additional costs were then passed on to DOD.

---

**Disguising conflicts of interest.** Contractors or subcontractors can conceal conflicts of interest for financial benefits. We identified a case involving a DOD subcontractor that concealed ownership for illicit financial gain. According to court records, a DOD contractor employee and his spouse formed a company and concealed their interests by not listing their names but listing the names of family members on formation documents. This company became a subcontractor to the company that employed the DOD contractor. The contractor employee, in his official position, wrote letters justifying awards of purchase orders to the subcontractor he owned and approving recommendations that the awards be made to the subcontractor. The co-owner of the subcontractor concealed her involvement by signing contracts using a different name, knowing that the use of her real name could reveal the DOD contractor employee's ownership of the subcontractor and affect the awards.

**Creating the appearance of competition on a contract to inflate prices.** In our review of 32 cases, we also identified the potential risk of companies creating the appearance of competition by submitting bids from fictitious companies. Specifically, we identified one case that involved a DOD contractor whose executives admitted as part of their plea agreements to creating fictitious, inflated bids that were not from actual businesses to ensure that the contractor's own bid would be selected by DOD as the supposed lowest. In this instance, the contractor was required to obtain at least two competitive bids for certain services and items and provide the bids to DOD for selection. As part of their plea agreements, the individuals involved with the scheme also admitted that the scheme allowed the contractor to control and inflate the prices charged to DOD without any true, competitive bidding, as required. The contractor also fraudulently inflated invoices that were sent to DOD, and two individuals involved in the scheme admitted they were aware of losses to DOD of at least \$34.8 million. Court records state that the scheme took place from 2011 to 2013. In 2017, two contractor executives involved with this scheme were sentenced to prison for 70 and 46 months. Additionally, we identified additional cases involving this contractor and its owner bribing government officials in exchange for the approval of fraudulent invoices, steering contracts, and covering up the contractor's overcharging practices, which has led to at least 22 individuals pleading guilty. Additionally, DOD officials from Defense Pricing and Contracting and DLA identified the risk of different companies concealing common ownership to create the appearance of competition on a solicitation and attempt to inflate prices.

---

By analyzing a subset of DOD solicitation data, we further examined the risk that contractors could disguise their ownership to create the appearance of competition. We identified potential relationships among the offerors of solicitations that could indicate common ownership. Our analysis of responses to approximately 2,700 solicitations in the Federal Business Opportunities (FBO) website from fiscal years 2015 through 2017 found indications that at least 16 offerors were potentially related to at least one other offeror when bidding on the same solicitation.<sup>29</sup> This analysis shows indications that offerors may not always compete independently and the relationship among offerors is not always readily apparent to contracting officials or disclosed in SAM registration information. Specifically, we identified the following types of potential relationships among offerors.

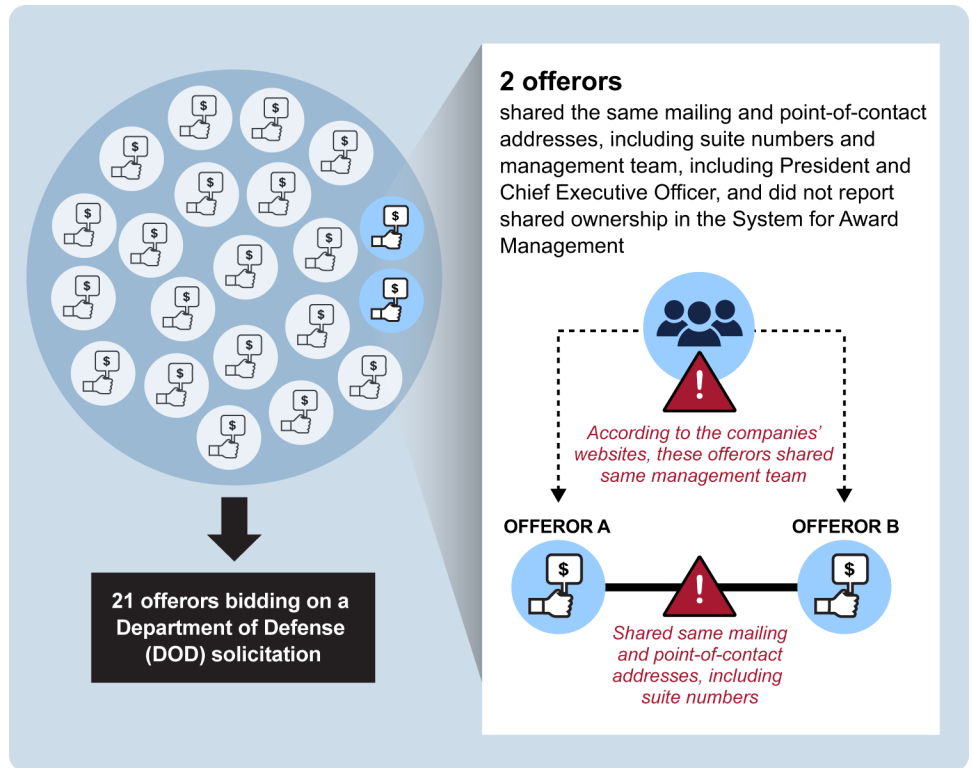
- **Offerors who shared the same management.** We identified two offerors who each submitted bids on the same three solicitations and also shared the same mailing address and point-of-contact address, including suite number. According to the companies' websites, the owner (who was also the President and Chief Executive Officer) for one offeror was the President and Chief Executive Officer of the other offeror. Further, both companies shared the same management team and neither company had reported any ownership information in SAM.<sup>30</sup> According to DOD contracting officials, no additional information was disclosed to the contracting office for these offerors, nor were they otherwise aware of the potential relationship. Figure 4 below shows an example from one solicitation.

---

<sup>29</sup>We analyzed solicitations having more than one response through the FBO bid module. The results of our analysis are limited to the approximately 2,700 solicitations we reviewed and are not generalizable to other DOD solicitations. Additional details for this analysis were deemed sensitive by DOD and have been omitted from this report.

<sup>30</sup>As previously noted, the "immediate owner" means an entity, other than the offeror, that has direct control of the offeror. Indicators of control include, but are not limited to, one or more of the following: ownership or interlocking management, identity of interests among family members, shared facilities and equipment, and the common use of employees. SAM is designed to capture the immediate and highest-level entity owner during the annual registration process. SAM does not collect, nor does the FAR require offerors to report, the beneficial owner—that is the natural person or persons who ultimately own or control a company, or benefit financially.

**Figure 4: Example of Potentially Related Offerors Bidding on the Same DOD Solicitation Who Shared the Same Addresses and Management Team**



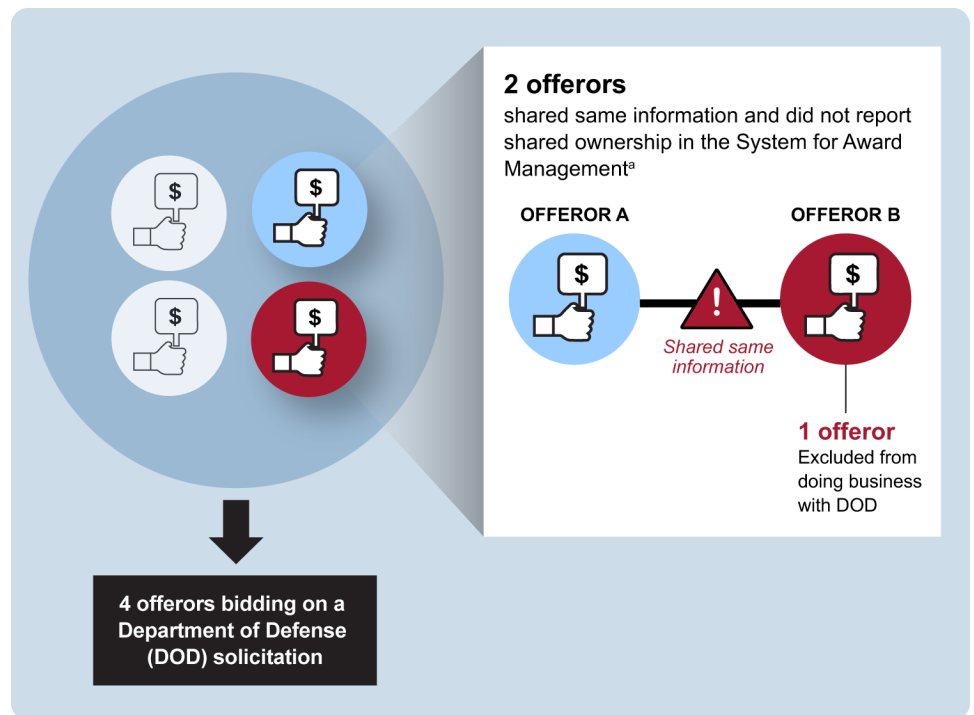
Source: GAO analysis of General Services Administration and DOD information. | GAO-20-106

- **Offerors who were potentially related to an entity excluded from doing business with the government.** We identified two offerors who were potentially related to a third offeror who was actively excluded from doing business with the government.<sup>31</sup> One of these

<sup>31</sup>Contractors debarred, suspended, or proposed for debarment are excluded from receiving contracts and are also excluded from conducting business with the government as agents or representatives of other contractors. Any offer received from an excluded entity cannot be evaluated for award. FAR § 9.405. Additional details discussing the methodology of our analysis and specific information shared by different offerors were deemed sensitive by DOD and have been omitted from this report.

offerors bid together with the excluded offeror on eight solicitations.<sup>32</sup> Figure 5 below shows an example of one solicitation.

**Figure 5: Example of Potentially Related Offerors Bidding on the Same DOD Solicitation, One of Whom Was Excluded from Doing Business with the Government**



Source: GAO analysis of General Services Administration and DOD information. | GAO-20-106

<sup>a</sup>Specific details about the type of information shared between the offerors were deemed sensitive by DOD and have been omitted from this report.

In addition, a third potentially related offeror was identified as sharing information with one of these offerors who later bid together on a ninth solicitation. For one of the nine solicitations, one of the offerors potentially related to the excluded company was awarded a contract.<sup>33</sup> According to DOD contracting officials, no additional

<sup>32</sup>Despite having an active exclusion from doing business with the government, this offeror continued to bid on solicitations. Additional details regarding the potential relationships identified in this analysis were deemed sensitive by DOD and have been omitted from this report.

<sup>33</sup>For the remaining eight solicitations, none of the potentially related offerors were awarded the contract.

---

information was disclosed to the contracting office for these offerors, nor were they otherwise aware of the potential relationship.

- **Offerors who shared other information.** We identified 11 offerors who shared other information with at least one other offeror when bidding on the same solicitation.<sup>34</sup> In some instances, these potentially related offerors bid on multiple solicitations. For example, we found two potentially related offerors bid together on three separate solicitations in our FBO data. We further examined these 11 potentially related offerors' SAM registration information to determine whether they reported shared ownership in SAM, and found one instance in which two of the potentially related offerors self-reported their relationship that one offeror owned the other; the remaining nine offerors did not report any type of shared ownership information in SAM. According to DOD contracting officials, none of the nine offerors disclosed a relationship with another offeror nor was the contracting officer otherwise aware of the potential relationship. While sharing certain information does not definitively confirm they are owned by the same entity, it is an indicator that these offerors are related.

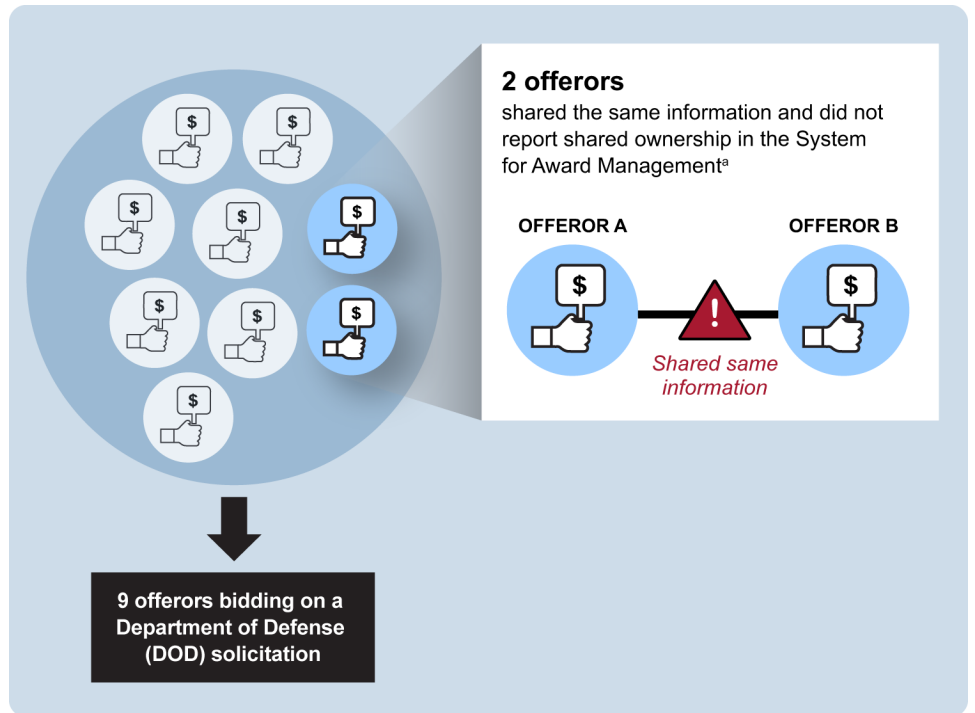
Figure 6 below highlights an example in which two offerors bidding on the same solicitation shared information and did not report shared ownership in SAM.

---

<sup>34</sup>These offerors bid on a combined total of six distinct solicitations. In one instance, multiple groups of potentially related offerors bid on the same solicitation. Specific details about the type of information shared between the offerors were deemed sensitive by DOD and have been omitted from this report.



**Figure 6: Example of Potentially Related Offerors Bidding on the Same DOD Solicitation Who Shared Information**

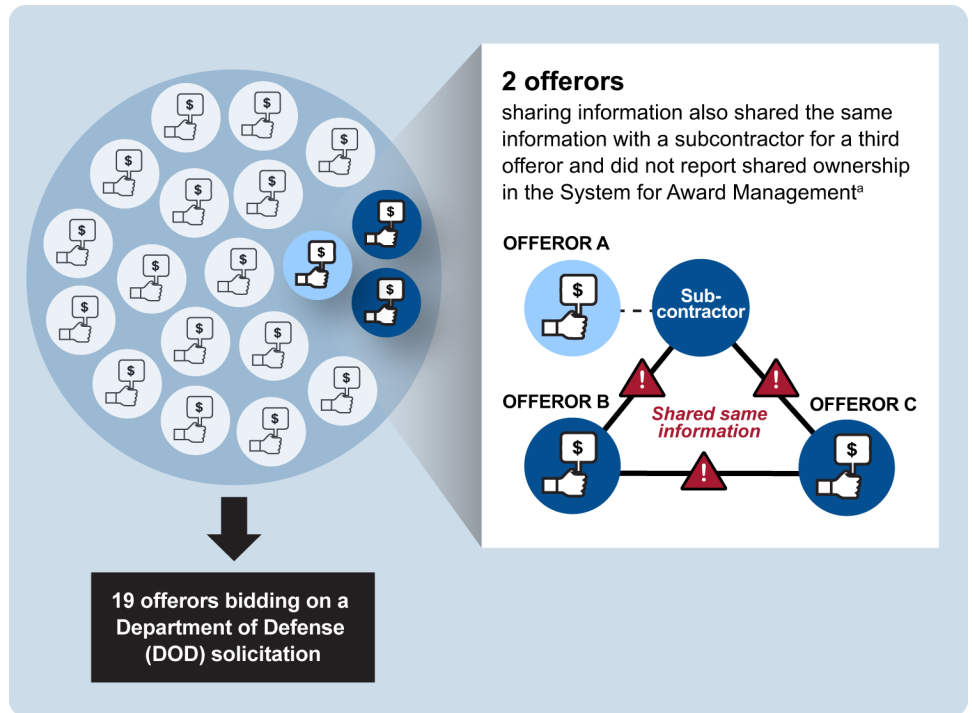


Source: GAO analysis of General Services Administration and DOD information. | GAO-20-106

<sup>a</sup>Specific details about the type of information shared between the offerors were deemed sensitive by DOD and have been omitted from this report.

Additionally, we identified an instance in which this type of information was also shared between two offerors and a subcontractor for a third offeror, as shown in figure 7 below.

**Figure 7: Example of Two Offerors and a Subcontractor for a Third Offeror Who Shared Information Bidding on the Same DOD Solicitation**



Source: GAO analysis of General Services Administration and DOD information. | GAO-20-106

<sup>a</sup>Specific details about the type of information shared between the offerors were deemed sensitive by DOD and have been omitted from this report.

The potentially related offerors we identified did not appear to affect the overall competition on these contracts because other, seemingly unrelated offerors also submitted bids. As a result, it is unlikely that they would have affected the price paid by the government in these contracts. However, these potentially related offerors represent a risk that offerors may not always be competing independently and these types of relationships may not always be readily apparent to contracting officers, which is important when evaluating the sufficiency of competition on a solicitation and the independence of its offerors. Further, contractors may not always be forthcoming in reporting their ownership information in SAM, which can affect other areas of the procurement process, including any procedures that rely on the accuracy of this information.

---

---

Contractors with Opaque  
Ownership Pose  
Nonfinancial Fraud Risks  
Including Circumventing  
Set-Aside Eligibility  
Requirements

Contractors can pose nonfinancial fraud risks to DOD by concealing their ownership structure to bid on and obtain contracts that they are not eligible to receive. These nonfinancial risks may not pose a direct financial cost to DOD, but they can allow ineligible companies to contract with DOD while potentially denying eligible companies from contracting with DOD. As discussed below, these risks can also lead to additional vulnerabilities. In our review of 32 cases, we identified DOD contractors that concealed their ownership information to obtain contracts set aside for particular types of businesses, to obtain contracts only intended for domestic companies, and to circumvent debarment by the government.

**Set-Aside Contract Eligibility.** Contractors with opaque ownership structures can pose the risk that government contracts set aside for small businesses are awarded to ineligible companies.<sup>35</sup> Ineligible contractors could take advantage of Small Business Administration set-aside programs that allow small businesses that are owned by service-disabled veterans, women, minorities, or economically and socially disadvantaged individuals to receive government contracts specifically set aside for these types of businesses. Of the 32 cases we reviewed, we identified 20 cases in which DOD contractors or DOD contractor employees were found guilty, pled guilty, or settled with the government for representing themselves as eligible to receive set-aside contracts. These contractors falsified self-reported information and made false certifications to the government to claim eligibility by using eligible individuals as figurehead owners. In these cases, the figurehead owners did not actually maintain the level of beneficial ownership or control of the contractor required by federal regulations, or the contractors simply used the names of eligible individuals when communicating with the government to bid on and win contracts.

---

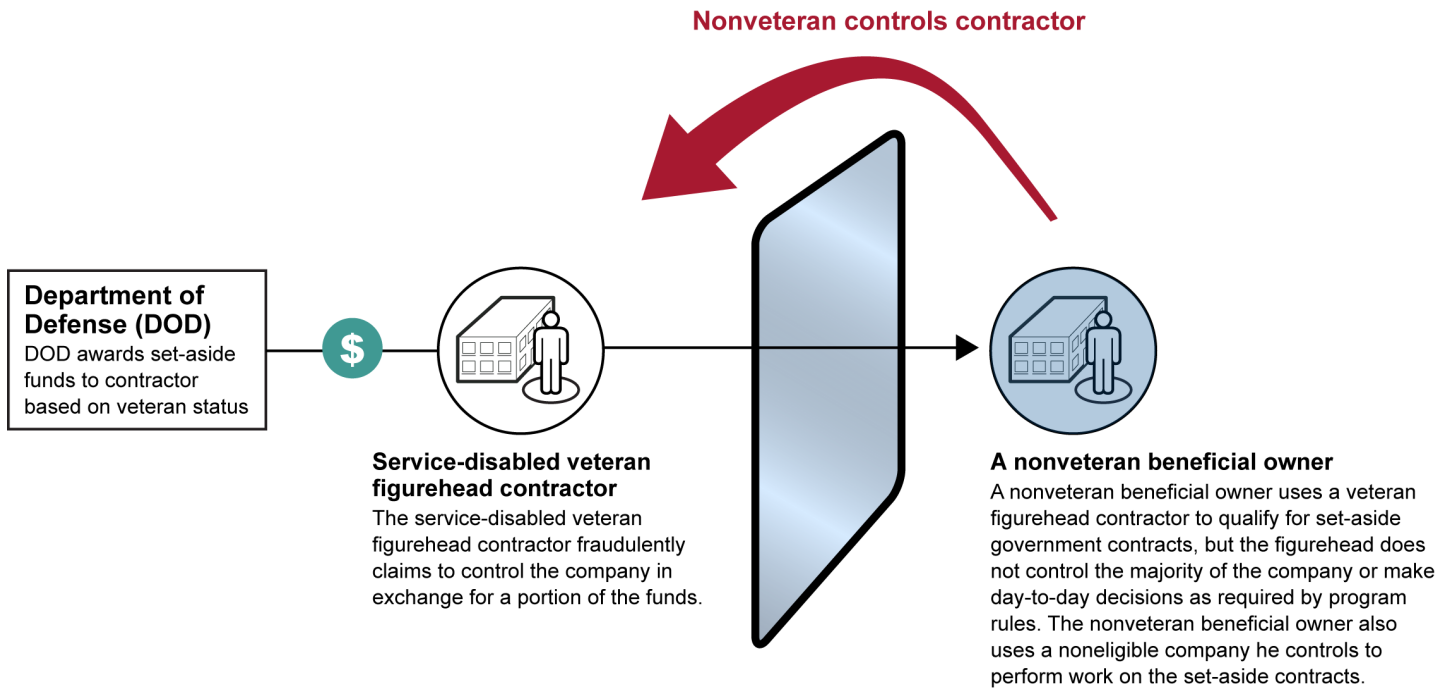
<sup>35</sup>Awards to set-aside companies include those participating in the Small Business Administration programs for 8(a) set-aside companies, Women-Owned Small Businesses, and Service-Disabled Veteran-Owned Small Businesses. 8(a) set-aside companies must, among other things, be at least 51 percent owned and controlled by U.S. citizens who are economically and socially disadvantaged as defined in regulation. Women-Owned Small Businesses must be at least 51 percent owned and controlled by U.S. citizens who are women and who manage day-to-day operations and make long-term decisions, among other qualifications. Service-Disabled Veteran-Owned Small Businesses must be at least 51 percent owned and controlled by service-disabled veterans who manage day-to-day operations and make long-term decisions, among other qualifications. The Small Business Administration is responsible for administering these programs.

---

For example, we identified one case that involved two DOD contractors participating in a single scheme to misrepresent their common ownership and obtain over \$200 million in awards that they were not eligible to receive. One of the contractors that fraudulently obtained set-aside contracts claimed it was owned by a service-disabled veteran; however, that veteran had virtually no involvement with the contractor. The other contractor claimed to be owned by an economically disadvantaged individual who worked full-time for another entity and did not control the contractor. These contractors were not eligible to receive the set-aside contracts because they were not at least 51 percent controlled by the eligible individuals and the eligible individuals did not make long-term decisions for the companies. Rather, the contractors were controlled by an ineligible individual who owned and controlled a separate company that actually performed work on the set-aside contracts.

To obtain government contracts set aside for companies owned by economically and socially disadvantaged individuals, the qualifying individuals must also control the majority of the company and make day-to-day decisions. Figure 8 below, which is based on an actual case, illustrates how ineligible contractors can obtain and receive government funds on contracts intended for Service-Disabled Veteran–Owned Small Businesses.

**Figure 8: Service-Disabled Veteran–Owned Small-Business Fraud Scheme**



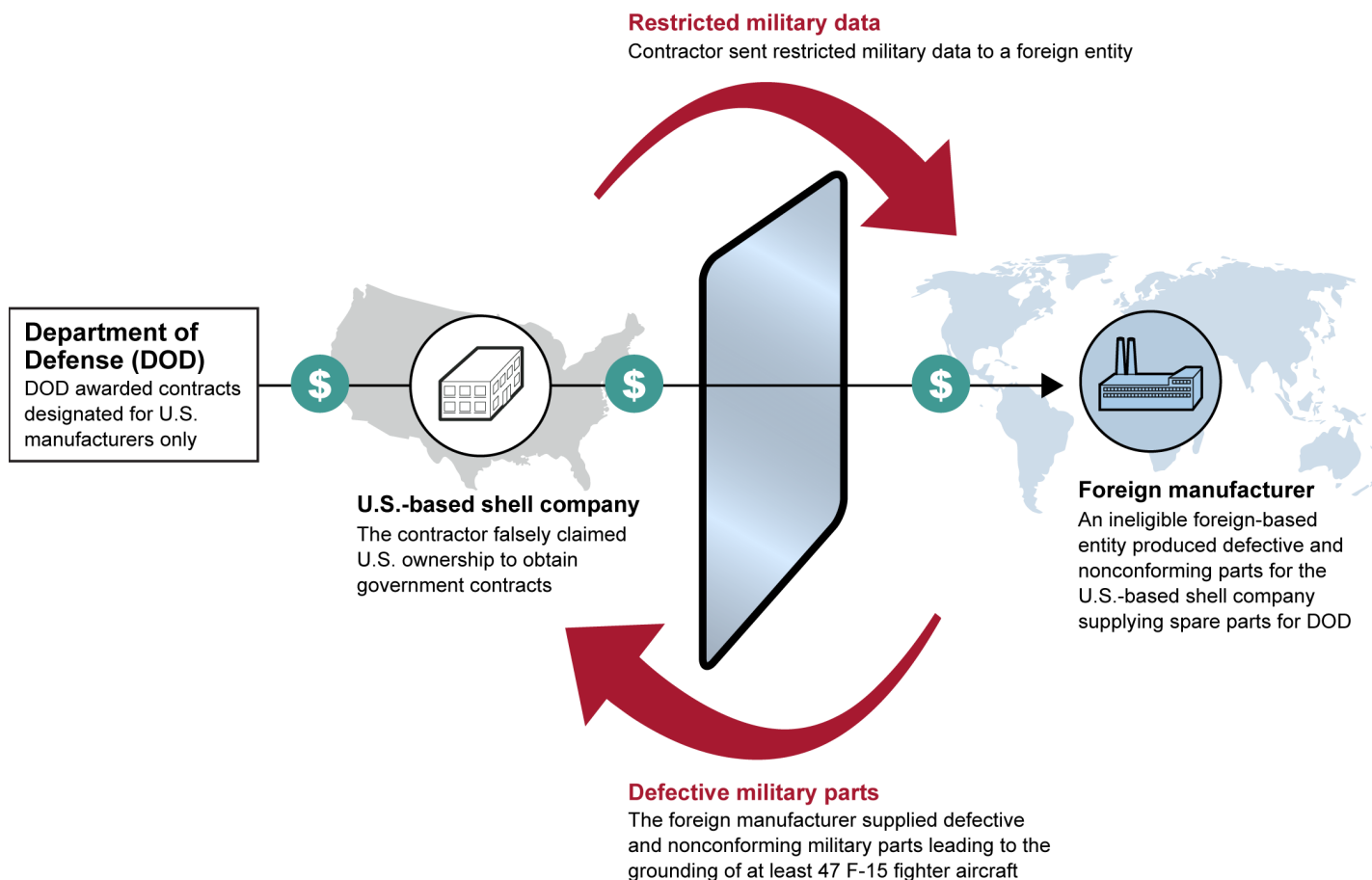
Source: GAO analysis of federal court records. | GAO-20-106

**Domestic Contractor Eligibility.** Contractors with opaque ownership structures can also pose the risk of circumventing eligibility requirements for contracts that are only designated for domestic companies, which can lead to other vulnerabilities that affect warfighter readiness. Of the 32 cases we reviewed, we identified four cases in which individuals created domestic shell companies for foreign manufacturers and bid on contracts designated for domestic companies. In three of the four cases, the individuals behind the shell companies also had ownership interests in the foreign manufacturing companies. Foreign manufacturers received payments from the contracts, despite the contracts only allowing domestic manufacturers to be eligible, and one such manufacturer ultimately supplied DOD with defective and nonconforming parts that led to the grounding of at least 47 fighter aircraft.<sup>36</sup> In multiple instances, another ineligible contractor supplied parts that were unusable due to design flaws and nonconformities. Three of these companies also exported military

<sup>36</sup>Supplies are nonconforming when they are defective in material or workmanship or are otherwise not in conformity with contract requirements.

technical drawings and blueprints to foreign countries in violation of the Arms Export Control Act.<sup>37</sup> Figure 9 below, which is based on an actual case, illustrates a contractor acting as a shell company and misrepresenting foreign manufacturing.

**Figure 9: Ineligible Foreign Manufacturer Fraudulently Obtaining DOD Contracts**



Source: GAO analysis of federal court records. | GAO-20-106

**Circumventing Debarment.** Individuals that have been debarred, or prohibited from conducting business with the federal government, can circumvent their debarment by concealing their ownership in new companies that were created for the sole purpose of continuing to

<sup>37</sup>22 U.S.C. §§ 2751–2799.

---

conduct business with the government. Of the 32 cases we reviewed, we identified one conviction of an individual who was debarred from 2013 to 2016 for supplying defective parts to DOD. This individual created three shell companies and concealed his beneficial ownership and control of these companies by omitting his name from communication with DOD and using fictitious names and names of family members as company officials. These three shell companies continued to provide defective and nonconforming parts to DOD, and the debarred individual received approximately \$2.8 million in payments from DOD from May 2013 to June 2016.

---

### Contractors with Opaque Ownership Structures Pose National Security Risks Including Supply-Chain Infiltration

DOD officials we spoke with and published DOD research have identified the risk of contractors disguising company ownership as an enabler to do harm to national security interests. Contractors fraudulently misrepresenting themselves to DOD could actually be operated by adversaries seeking to act against the government's interests. Foreign-owned contractors can conceal ownership information when registering in SAM, which allows contractors to self-attest ownership information. For example, in addition to the 32 cases we identified through our review, we also identified a bid protest filed with GAO challenging a contract award made to a foreign-owned DOD contractor in fiscal year 2018 that prohibited the participation of foreign firms or domestic companies under foreign ownership, control, or influence. This contractor did not disclose its foreign ownership or control in SAM or to DOD, as required by the FAR and the solicitation. As a result of the bid protest, DOD subsequently terminated the contract later in fiscal year 2018 after confirming the foreign ownership with the contractor.

DIA and DLA officials stated that adversarial foreign governments or other malicious entities, such as companies attempting to access sensitive government information, could access sensitive systems to conduct sabotage or surveillance. These entities could infiltrate DOD's supply chain to introduce components, such as circuit-board chips and routers modified to fail, facilitate state or company espionage, or compromise the integrity of DOD's information-technology systems. According to CIO officials, adversarial entities could also potentially gain access to sensitive information through their relationship with DOD contractors. For example, DIA officials identified the possibility of foreign or adversarial entities exploiting companies in DOD's supply chain with financial difficulties, and according to CIO officials, DOD may not always have visibility over foreign entities acquiring a domestic contractor.

---

In 2017, the Office of the Director of National Intelligence released a management background paper discussing supply-chain risks, which stated that the multiple layers and networks of suppliers in this chain can allow foreign adversaries the ability to access the supply chain at multiple points. For example, according to the background paper, a hostile foreign intelligence entity could potentially conceal its presence in government supply chains by operating through multiple front organizations, companies, hackers, and organized crime, making it extremely difficult to discover and counter its actions. The paper also states that adversaries may be able to penetrate the supply chain to access sensitive research and development programs, steal intellectual property and personally identifiable information, insert malware into critical components, and mask foreign ownership, control, or influence of key providers of components and services. Furthermore, in April 2018, the U.S.-China Economic and Security Review Commission issued a report identifying a supply-chain threat to U.S. national security that stems from products produced, manufactured, or assembled by entities that are owned, directed, or subsidized by national governments or entities known to pose a supply-chain or intelligence threat to the United States.<sup>38</sup>

DOD officials have also identified an additional risk of contracting with companies that have opaque ownership structures. For example, a 2017 Defense Contract Audit Agency report to Congress described the risk of individuals receiving government contracts or gaining access to government installations who would harm deployed troops. Officials we spoke with from the Joint Staff Logistics Directorate also acknowledged the risk that government funds could be provided to contractors owned by a person or entity that is actively opposing U.S. or coalition forces involved in a contingency operation in which service members are actively engaged in hostilities. These adversaries can potentially use opaque ownership structures to disguise their ownership and contract with the government in areas involved in contingency operations, such as Iraq or Afghanistan, to fund their operations or gain access to military bases.

---

<sup>38</sup>The U.S.-China Economic and Security Review Commission was created by Congress in October 2000 with the legislative mandate to monitor, investigate, and submit to Congress an annual report on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China, and to provide recommendations, where appropriate, to Congress for legislative and administrative action.



---

---

## DOD Has Taken Steps That Could Address Some Risks Related to Contractor Ownership and Has Opportunities to Systematically Assess These Risks

DOD has taken steps that could address some fraud and other risks related to contractor ownership in the procurement process. It has not yet conducted a department-wide assessment of these risks or identified them as a risk area for assessment in its development of a fraud risk management program in accordance with federal internal control standards and leading practices, however. As mentioned previously, DOD and other federal agencies revised the FAR in 2014 to collect some contractor ownership information. DOD has also begun to consider contractor ownership to address national security risks, including identifying and using contractor ownership information as part of its supply-chain risk analysis in the procurement of national security systems and critical components, avoiding contracting with the enemy, and determining whether contractor facilities can be cleared to access classified materials. Although DOD has taken these actions, it faces a number of challenges in identifying and verifying contractor ownership. To assist the department and its components in identifying and assessing fraud risks, DOD has also begun a department-wide fraud risk management program. As it develops a fraud risk assessment across the department, DOD has opportunities to systematically assess risks related to contractor ownership as part of this larger effort. This fraud risk assessment, if used to inform the development of a risk-based antifraud strategy, could enhance the effectiveness of managing fraud risks for DOD, including those related to contractor ownership.

---

---

## DOD Has Taken Steps That Could Address Some Fraud and Other Risks Related to Contractor Ownership

DOD and Others Revised the FAR to Collect Ownership Information to Improve Their Review of Contractor Past Performance before Awarding New Contracts

DOD, GSA, and the National Aeronautics and Space Administration amended the FAR in May 2014 to require prospective contractors to self-report their immediate and highest-level entity owner, but not their beneficial owner, as part of contractors' annual registration process in SAM.<sup>39</sup> The agencies added the requirement to support the implementation of business tools to help track contractor performance issues across corporations as well as to improve supply-chain transparency and integrity efforts, among other reasons. According to DOD procurement policy officials, the intent is that the ownership information would be made available in FAPIIS for contracting officers to help identify past-performance issues across corporations to aid with responsibility determinations.<sup>40</sup>

The FAR requires contracting officers to consider all relevant information available in FAPIIS when making responsibility determinations, but, according to DOD procurement policy officials, there is no requirement to document whether and how ownership information is considered. According to DOD procurement policy officials, contracting officers' general focus in the responsibility determination process is largely centered on whether the contractor is financially solvent, has the ability to carry out the contract, and has satisfactory past performance. DOD procurement policy officials said that they did not want to be too prescriptive in directing contracting officers on the use of this information, and therefore have not developed policies or procedures or provided training on how to specifically use the ownership information collected.

---

<sup>39</sup>This amendment applies to entities registering in SAM, beginning November 1, 2014. Contractors are required to register annually, or upon any change of registration information.

<sup>40</sup>Contracting officers are generally required to check FAPIIS for procurements over the simplified acquisition threshold (generally, \$250,000 at the time of our review). Contracting officers must consider all information available in FAPIIS, which includes ownership information, as part of a prospective contractor's past-performance review when making responsibility determinations.

---

According to these officials, DOD has not historically considered contractor ownership structures in the responsibility determination process, nor has the agency been aware of the extent to which such structures could pose a range of risks. As discussed below, conducting a department-wide assessment of risks posed by contractor ownership—an action that DOD has not yet taken—would be a key first step for the department before developing such policies and procedures.

Within DOD, DLA has taken steps that could address some risks posed by contractor ownership.<sup>41</sup> First, according to procurement officials, DLA provides its contracting officials with a “contractor responsibility matrix,” which outlines mandatory, recommended, and optional steps to take when making a responsibility determination for procurements both below and above the simplified acquisition threshold. Among the steps included, DLA requires contracting officials to review contractors’ attestations to ownership or control by a foreign government to determine whether the prospective contractor is qualified and eligible to receive an award. It also recommends contracting officials obtain responsibility information from other sources, including an internet search of the company’s reviews, and its owners and principals. This step is listed as optional for existing contractors.

Further, DLA’s contracting officers are required to review the Defense Contractor Review List to identify any past-performance information. The Defense Contractor Review List is an internal tool used by DLA that is designed to monitor fraud, waste, and abuse for commercial entities and military unique items. The system is designed to allow DLA to identify and communicate information on its contractors, such as performance ability, delinquency information, suspension and debarment information, and various types of notes that may be relevant to contract performance or procurement decisions. DLA officials told us the Defense Contractor Review List can be used to communicate information or risks about contractor ownership.

The Defense Logistics Acquisition Directive requires DLA contracting officers to review any Special Attention Reason Codes in the Defense

---

<sup>41</sup>DLA is DOD’s combat logistics support agency, providing worldwide logistics support to the military services as well as several civilian agencies and foreign countries. According to its website, DLA supplies 86 percent of the military’s spare parts and nearly 100 percent of fuel and troop support consumables, among other products, to military and other federal agencies.

---

Contractor Review List and comply with its associated Special Attention Treatment Codes when making responsibility determinations. The Special Attention Reason Codes describe the basis for being on the list and the Special Attention Treatment Codes provide recommended actions to contracting officers for mitigating risk. According to DLA officials, contractor ownership information is generally not identified in the Defense Contractor Review List. Nevertheless, ownership information may be included in the documentation if, for example, the contracting officer identifies that two or more companies appear to be related or in cases in which there may be suspected collusion.

DOD Has Taken Steps to Use Contractor Ownership Information to Address Other Risks Such as National Security Concerns

DOD has taken steps in other areas to use contractor ownership information to address risks in specific types of procurements, including those involving national security systems. For example, DOD has taken steps to address national security concerns related to contractor ownership, including conducting threat assessments to identify risks related to supply chains for critical components and national security systems. DOD has also taken steps to identify contractor ownership information to avoid contracting with the enemy, and to address foreign ownership, control, and influence in contracts involving classified information.<sup>42</sup> DOD has outlined policies and procedures in some, but not all, of these areas. As discussed below, conducting a department-wide assessment of risks posed by contractor ownership—an action that DOD has not yet taken—would be a key first step for the department before fully developing such policies and procedures.

- **Steps taken to use ownership information to address supply chain risks.** DOD has taken some steps to identify and consider contractor ownership to address supply-chain risks. For example, DIA considers contractor ownership information when conducting threat assessments as part of its supply-chain risk analysis for procurement of national security systems and critical components, according to DIA officials. Specifically, DOD is able to use public and nonpublic intelligence information to exclude sources that present risks of an adversarial foreign government or other malicious entities infiltrating DOD's supply chain and stealing information or compromising

---

<sup>42</sup>According to DOD procurement and industrial policy officials, contractor ownership information is also identified during investigations conducted by the Committee on Foreign Investment in the United States when reviewing certain foreign investment transactions to determine the effect on U.S. national security. However, information gathered in the investigation process is restricted and cannot be shared for other purposes, such as to inform the contracting process, according to these officials.

---

government systems. DIA officials told us that, as part of this supplier-related threat assessment, they identify and consider ownership information along the supply chain, including beneficial-ownership information.

The guidelines in Intelligence Community Standard 731-02 state that a supply-chain threat assessment for a procurement item determined to be mission-critical should at a minimum include information on the contractor's parent company, ultimate parent company, and subsidiaries. However, the guidance does not specify whether this ownership and related company information is to be independently verified or whether it relies on the contractor self-attestations in SAM. According to the guidance, supply-chain threat assessments should also include, at a minimum, information on the contractor's key management personnel, such as members of the board of directors, officers, general partners, and senior management officials. The guidance does not mention, however, identifying beneficial owners or those who do not have direct control over a contractor but derive substantial economic benefit from it.

- **Steps taken to use ownership information to address legal provisions against contracting with the enemy.** Officials from the Joint Staff Logistics Directorate responsible for DOD's vendor vetting program told us that contractor ownership information, including beneficial ownership, may be identified as part of the intelligence information gathered on vendors by combatant commands to ensure that money is not flowing to contractors owned by a person or entity that is actively opposing U.S. or coalition forces involved in a contingency operation in which service members are actively engaged in hostilities.<sup>43</sup> According to these officials, DOD has not established department-wide policies or procedures to implement reviews of contractor ownership during the process of vetting vendors, but it is something the department is currently developing. These officials stated that a vendor threat-mitigation working group discusses how to close gaps in information sharing among the intelligence,

---

<sup>43</sup>The vendor vetting program was established in response to provisions in the fiscal year 2015 National Defense Authorization Act prohibiting DOD from providing funds to contractors owned by a person or entity that is actively opposing U.S. or coalition forces involved in a contingency operation. "Contingency operation" generally means a military operation in which members of the armed forces are or may become involved in military actions, operations, or hostilities against an enemy of the United States or against an opposing military force.

---

procurement, and operations communities.<sup>44</sup> Officials also noted some challenges. Although contracting officers are responsible for determining the responsibility of vendors and whether vendors can perform the terms of a contract, the information that may be available to contracting officers and the actions that they can take are not always clear. For example, the officials we spoke with mentioned concerns that contracting officers are not always able to access or act on intelligence information. GAO recently completed a review of this program in a classified report.<sup>45</sup>

- **Steps taken to address ownership risks in contracts involving classified information.** DOD has taken steps to address risks posed by contractor ownership as part of the Facilities Clearance Process. DOD uses the Facilities Clearance Process to determine whether a contractor is eligible to access classified information. DOD has developed written policies and procedures for how contractor ownership, including foreign ownership, control, and influence, is to be investigated and addressed. As part of this process, Defense Security Service (DSS) guidance instructs its officers to identify key management personnel and to assess the risks they pose for possible foreign ownership, control, or influence. DSS guidelines indicate that key management personnel include company officers, directors, and members of a limited liability company, among others. Some key management personnel, such as members of a limited liability company, may also be the owners. According to DSS officials, beneficial owners who benefit financially but do not partake in active management may be identified as key management personnel as part of the clearance process, depending on various factors including the percentage of ownership. As an example, DSS officials stated that an individual who owns 50 percent of a company would not be able to purport that he or she does not control the company. According to the DSS guidance, if foreign ownership, control, or influence is found, mitigation agreements can be put into place to reduce the risk.

---

<sup>44</sup>We have previously reported that DOD formed the vendor threat-mitigation working group in October 2016. GAO, *Operational Contract Support: Actions Needed to Enhance Capabilities in the Pacific Region*, [GAO-17-428](#) (Washington, D.C.: June 23, 2017).

<sup>45</sup>GAO, *Operational Contract Support: Actions Needed to Strengthen DOD Vendor Vetting Efforts*, [GAO-19-37C](#) (Washington, D.C.: Dec. 20, 2018).

---

---

## DOD Has Encountered Challenges in Identifying and Verifying Contractor Ownership

DOD officials identified a number of challenges in identifying and verifying contractor ownership, especially if the contractor is actively seeking to misrepresent its ownership. For example, verifying contractor ownership can be challenging because state governments determine the type of information collected during company formation and, as discussed earlier, most states collect minimal ownership information as part of this process. As described earlier, there is no centralized information source or registry on company ownership information in the United States. As a result, contracting officers could face challenges in time-consuming efforts to verify contractor ownership. Further, DOD procurement policy officials stated that workload and resource constraints limit the extent to which they can verify contractor ownership.

The nature of ownership information submitted during the SAM registration process also presents challenges to any verification efforts conducted by contracting officers. The ownership information submitted in SAM is self-reported by the prospective contractor, and therefore relies on the contractor to honestly report such information. DOD officials told us that, for most procurements, with the exception of those involving classified work or other national security concerns, this information is not verified. A related limitation involving SAM ownership information is that contractors must provide information on the immediate and highest-level entity owners and are not required to report beneficial-ownership information, that is, on the natural person or persons who own or control, or benefit financially from, the company. Lastly, while the SAM ownership requirement provides some transparency at the prime-contractor level, it does not provide transparency at the subcontracting levels below the prime contractor. Subcontractors are not required to register in SAM and, therefore, are not required to report their ownership.<sup>46</sup> Consequently, DOD generally does not have insight into the ownership of its subcontractors. DOD procurement policy officials noted that this poses particular challenges in identifying fraud and other risks to the supply chain. For example, the contractor itself may not pose a risk; but that does not guarantee that the contractor's suppliers do not pose fraud or other risks. DOD procurement policy officials told us that it would be helpful to require subcontractors to register in SAM and report their ownership. This requirement would be an additional burden on

---

<sup>46</sup>Some subcontractors serve as the prime contractor on other contracts, and would be required to report in SAM in that capacity.

---

contractors, however, and would need to be balanced with the potential benefit of being able to identify problem actors.<sup>47</sup>

Another challenge involves the use of publicly available ownership information, including commercially available data services, by contracting officers to help identify contractor ownership. Depending on how a company is structured, there may be no publicly available ownership information. Furthermore, DOD procurement policy officials told us that public information, including ownership information, could be inaccurate or outdated and potentially expose the department to bid protests from the contractor. Therefore, any external or supplemental information used that was not part of the contractor's submission would need to be vetted by the contractor before using it. These officials said that DOD would need to come up with an efficient process to inform the prospective contractor of the additional information and provide due process to allow it the opportunity to refute any information obtained. Additionally, DOD procurement policy officials noted that another difficulty with using a commercial tool to determine ownership is the volume of contracts processed by contracting officials, which amounted to over 570,000 new contracts in fiscal year 2018.

For sensitive procurements in which DOD has the authority to use both public and nonpublic information (for example, those involving national security systems or classified work), DSS officials stated that the process of identifying and verifying ownership is lengthy, particularly with complex ownership. In some instances, it has taken DSS 1 to 2 years to resolve issues that have arisen when clearing contractors' facilities for access to classified materials. In addition, DSS officials mentioned that the many different types of business structures, including new structures that DSS comes across, create challenges for identifying ownership. According to DIA officials, it is significantly easier to identify the beneficial owner of publicly traded companies than privately owned companies. DSS officials also mentioned that it is difficult and resource-intensive to monitor changes to contractor ownership, particularly given that they monitor 13,000 facilities.

---

<sup>47</sup>The Federal Funding Accountability and Transparency Act of 2006 (Pub. L. No. 109-282, § 2) required the Office of Management and Budget to develop a pilot program to determine how to collect and implement a reporting program for subcontractors, among other things, and conduct an assessment of the reporting burdens placed on contractors and subcontractors. As part of these efforts, according to GSA officials, a separate requirement for subcontractors to register in SAM was explored but was ultimately rejected because it was viewed as too burdensome for subcontractors.



---

According to DOD procurement policy officials, DOD would need to determine which contracts require additional research into contractor ownership and which office would be responsible for conducting the research. Officials noted that DOD does not currently have the resources in place to focus on these kinds of activities because contracting officers are already operating in a constrained environment with limited resources, lacking the time, resources, or training they need to conduct in-depth reviews or analysis of the ownership aspects of a particular company. According to these officials, DOD should dedicate staff and funds to resolve this problem, including bringing in people with data-analysis and data-mining skillsets to learn from private-sector companies and organizations that already conduct vendor ownership-related risk assessments and data analytics.

DOD procurement policy officials identified that another strategy to address opaque ownership structures would be to require contractors to report additional ownership information, such as beneficial-ownership information, when registering to do business with the federal government in SAM. However, the officials also noted that, previously, both public-sector organizations and private companies have resisted requirements to provide additional ownership information, due in part to the difficulty in defining ownership. Additionally, regulatory trends within government contracting have generally focused on easing the burden to do business with the government. New requirements to provide additional information may be viewed as an additional burden.

A selected group of companies that contracted with DOD in the last 5 years provided us with mixed views on the potential burden of providing additional ownership information.<sup>48</sup> Most small-business contractors we contacted told us that an additional beneficial-ownership reporting requirement would pose little to no further burden on them. In contrast, both of the large, publicly traded companies that similarly contracted with DOD expressed concerns about the complexity and difficulty of reporting their beneficial ownership. One large company noted that beneficial ownership would need to be more narrowly defined for it to determine the resulting regulatory burden.

---

<sup>48</sup>To connect with contractors, we contacted several contractors' associations to gain the perspectives of their members. The results of our discussion are descriptive of only the 16 members who contracted with DOD belonging to three contractors' associations from whom we received a response. These results are not generalizable to all contractors.

---

---

## DOD Has Opportunities to Systematically Assess Risks Related to Contractor Ownership as It Develops a Fraud Risk Assessment across the Department

### DOD Has Begun to Develop a Department-Wide Fraud Risk Assessment

DOD has taken steps to conduct a department-wide fraud risk management program designed to identify and assess fraud risks. According to DOD's Fraud Risk Management Pilot Program Instructions, in 2017 DOD began efforts to design, implement, and operate an internal control system that addresses fraud risks and to comply with requirements established by FRDAA.<sup>49</sup> As mentioned earlier, FRDAA created requirements for agencies to establish financial and administrative controls for managing fraud risks. FRDAA also requires agencies to report their progress identifying risks and vulnerabilities to fraud affecting payroll, beneficiary payments, grants, purchase and travel cards, and large contracts. As part of this implementation process, and to test the development of its fraud risk management program, DOD conducted a fraud risk management pilot program in 2018 by selecting four components to identify fraud risks, assess controls they have in place to mitigate these risks, and develop mitigation plans, as appropriate.<sup>50</sup> According to DOD, the pilot program was designed to assist DOD and its components in the development of a department-wide fraud risk management program by identifying and assessing fraud risks in a manner that is aligned with the leading practices within GAO's Fraud Risk Framework.<sup>51</sup>

---

<sup>49</sup>Pub. L. No. 114-186, 130 Stat. 546 (June 30, 2016).

<sup>50</sup>DOD selected the Defense Finance and Accounting Service, Department of the Navy, U.S. Special Operations Command, and Washington Headquarters Services for its fraud risk management pilot program. DOD requested that these components identify fraud risks with respect to payroll, beneficiary payments, grants, large contracts, asset safeguards, information technologies and services, commissaries, and purchase, travel, and fleet cards; and assess whether there are controls in place that will mitigate these fraud risks.

<sup>51</sup>[GAO-15-593SP](#).

---

To prepare for this pilot program, in 2017, the Office of the Under Secretary of Defense (Comptroller) (OUSD[C]) conducted a survey requesting that 66 DOD components determine the extent and maturity of control activities currently in place related to the prevention, detection, and response to fraud. The survey asked components to provide, among other things, information on any antifraud programs, key fraud risks identified, and processes for identifying, responding to, and monitoring risks. The responses from the 41 responding components were scored to determine their fraud program maturity. According to DOD's Fraud Risk Management Pilot Program Instructions, the results of this survey were also used to identify potential vulnerabilities from the FRDAA requirements and guide the development of DOD's pilot program. DOD officials told us that before the recent development of their fraud risk management pilot program, the department did not have a process for assessing fraud risks department-wide.<sup>52</sup>

Also, as part of the pilot program, OUSD(C) and the components identified seven fraud schemes that affect large contracts, five of which we discuss above as having the potential to involve risks posed by contractor ownership. Specifically, the pilot program identified fraud schemes involving service-disabled veteran-owned businesses, inflated prices charged by contractors for the services rendered, bid submission with the same two or three offerors on multiple contract opportunities, inclusion of one or more contractors as a subcontractor on the bid rigger's proposal, and counterfeit parts.<sup>53</sup> As discussed previously in this report, opaque ownership structures can play a role in carrying out these types of fraud schemes. DOD completed the pilot program in 2018, and in March 2019 began expanding the fraud risk management program department-wide by requesting that DOD components identify fraud risk and controls in place to mitigate these risks by July 2019. As with the pilot program, the components were requested to identify and assess fraud risks to meet requirements established by FRDAA and allow DOD to identify fraud risks and vulnerabilities facing the department.

---

<sup>52</sup>DOD currently plans for its fraud risk management program to be implemented department-wide in fiscal year 2019. GAO is conducting ongoing work examining DOD's fraud risk management efforts regarding contract fraud that will discuss how DOD manages contractor fraud risk.

<sup>53</sup>According to DOD officials, the schemes identified were adopted from DOD Office of Inspector General fraud-detection resources for auditors and by conducting a review of DOD Office of Inspector General reports.

---

## DOD Has Not Systematically Assessed Risks Related to Contractor Ownership

While DOD has taken some steps to identify and potentially address fraud and other risks posed by contractor ownership, it has not conducted a department-wide assessment of these risks or selected them as a risk area for assessment in its development of a fraud risk management program. DOD procurement policy officials told us that contractor ownership and financing structures have not historically been considered by the department. DOD procurement policy officials expressed the need for a strategic assessment of contractor ownership risks at the Office of the Secretary of Defense (OSD) level to deal with the wide range of potential threats that exist. Still, getting support at the senior OSD level to consider the risks posed by contractor ownership and dedicate resources to mitigating these risks is a challenge, according to these officials. The challenge exists because senior DOD officials may not be aware of the potential magnitude or frequency of risks posed by contractor ownership issues, including the extent to which risks cross multiple areas throughout the department. Additionally, DOD procurement policy officials told us that contracting officers do not have anyone within the department to contact for assistance in determining ownership during the procurement process and there is no dedicated entity within the department that deals with contractor ownership issues.

Federal internal control standards call for agency management officials to assess the internal and external risks their entities face as they seek to achieve their objectives. The standards state that as part of this overall assessment, management should consider the potential for fraud when identifying, analyzing, and responding to risks, including changes to risks, and consider factors such as absent or ineffective controls that provide an opportunity to commit fraud.<sup>54</sup> In a complementary fashion, the Assess component of GAO's Fraud Risk Framework calls for federal managers to plan regular fraud risk assessments and to identify and assess risks to determine a fraud risk profile, as described in figure 10 below.<sup>55</sup> According to the Fraud Risk Framework, a fraud risk profile documents the findings from a fraud risk assessment and can help agencies decide how to allocate resources to respond to residual fraud risks.

---

<sup>54</sup>[GAO-14-704G](#).

<sup>55</sup>[GAO-15-593SP](#).

**Figure 10: GAO's Fraud Risk Management Framework**



Source: GAO. | GAO-20-106

The Assess component also indicates that relevant stakeholders, including those with responsibilities for specific control activities and with knowledge of emerging fraud risks, should be involved in the assessment process. This could include a variety of internal and external stakeholders, such as general counsel, contractors, or other external entities with knowledge about emerging fraud risks or responsibilities for specific control activities. For example, the DOD Office of Inspector General and its work on emerging risks involving contractor ownership may inform the fraud risk assessment process and help managers to identify fraud risks.<sup>56</sup> Additionally, an assessment of ownership risks could include relevant DOD officials responsible for assessing and responding to national security risks, such as those responsible for assessing supply-

<sup>56</sup>Specific details regarding work performed by the DOD Office of Inspector General involving contractor ownership were deemed sensitive by DOD and have been omitted from this report.

---

chain risks in national security system procurements, vetting vendors to ensure DOD avoids contracting with the enemy, and determining whether contractor facilities can be cleared to access classified materials. Including relevant stakeholders would allow DOD to leverage the knowledge and experience of such officials and more comprehensively identify risks related to contractor ownership. Further, it would allow DOD to better understand the extent to which risks cross multiple areas throughout the department.

At a fundamental level, assessing risks arising from contractor ownership would allow DOD to take a strategic, risk-based approach to identifying and managing these risks. In addition, a risk assessment would help DOD better understand the magnitude and prevalence of these risks, including the effects these risks have from both a fraud and national security perspective, and whether certain types of procurements are more vulnerable to contractor ownership risks. Further, conducting a department-wide assessment of risks posed by contractor ownership would assist the department in its evaluation of whether its existing control activities are sufficient and designed to effectively respond to these risks or whether additional control activities are needed. For example, it would allow DOD to better determine how contractor ownership information should be used and verified, and whether additional ownership information should be collected. In accordance with leading practices, DOD would then be positioned to design and implement specific control activities to prevent and detect contract ownership-related fraud and make informed decisions on how best to use its resources.

---

## Conclusions

DOD is the largest contracting agency in the federal government in terms of contract dollars obligated and number of contracts awarded. The scope and scale of this activity makes DOD procurement inherently susceptible to fraud. Our various analyses and discussions with procurement officials from across the department identified risks posed by contractors with opaque ownership that involve various types of procurements. DOD has taken some steps that could address some risks posed by contractor ownership in the procurement process. It has the opportunity to include these risks as part of its department-wide fraud risk assessment at a strategic level. Assessing risks related to contractor ownership, as a fundamental first step, would help DOD better determine whether certain types of procurements are more vulnerable to this type of risk. Further, it would help DOD determine whether additional policies and procedures are needed to articulate how officials should use and verify the ownership

---

information it collects, or to require additional ownership information. We recognize that collecting additional ownership information, including beneficial-ownership information, could pose compliance burdens for contractors; and regulatory trends have generally focused on easing the burden to do business. Additionally, verifying contractor ownership can be challenging and time-consuming. Nevertheless, having a thorough assessment of contractor-ownership risks will better position DOD to make informed decisions on how best to use its resources and help ensure that the department's fraud risk management program is organized and targeted to manage risks in a prioritized manner. Lastly, involving relevant stakeholders with knowledge of emerging risks could help inform other types of risk assessments across the department, including national security concerns. Doing so will contribute to the effective implementation of leading fraud risk management practices when considering the existing and emerging risks to the department.

---

## Recommendation for Executive Action

The Office of the Undersecretary of Defense (Comptroller) (OUSDC) should include an assessment of risks related to contractor ownership as part of its ongoing efforts to plan and conduct a department-wide fraud risk assessment. As part of this assessment, consistent with leading practices, DOD should involve relevant stakeholders with knowledge of emerging risks and use this information to help inform other types of risk assessments across the department, including for national security concerns. (Recommendation 1)

---

## Agency Comments

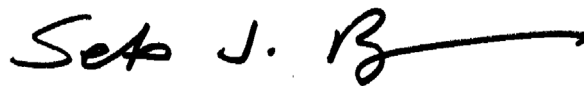
We provided a draft of the sensitive version of this report to DOD and GSA for comment. In commenting on a draft of the sensitive version of this report, DOD concurred with our recommendation and provided additional written comments outlining current and planned efforts in response to our recommendation. These written comments were deemed sensitive by DOD and have been omitted from this report. In an email, GSA stated that it did not have any comments. DOD also provided technical comments, which we incorporated as appropriate.

---

---

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, the Administrator of GSA, and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

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

A handwritten signature in black ink that reads "Seto J. Bagdoyan". The signature is written in a cursive style with a long horizontal stroke extending to the right.

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



---

*List of Committees*

The Honorable James M. Inhofe  
Chairman  
The Honorable Jack Reed  
Ranking Member  
Committee on Armed Services  
United States Senate

The Honorable Richard C. Shelby  
Chairman  
The Honorable Richard J. Durbin  
Ranking Member  
Subcommittee on Defense  
Committee on Appropriations  
United States Senate

The Honorable Adam Smith  
Chairman  
The Honorable Mac Thornberry  
Ranking Member  
Committee on Armed Services  
House of Representatives

The Honorable Pete J. Visclosky  
Chairman  
The Honorable Ken Calvert  
Ranking Member  
Subcommittee on Defense  
Committee on Appropriations  
House of Representatives

---

# Appendix I: Objectives, Scope, and Methodology

---

This report is a public version of a sensitive report that we issued on September 12, 2019, with the objectives to (1) identify types of fraud and other risks, if any, that contractors with opaque ownership could pose to the Department of Defense (DOD) in the procurement process and (2) assess whether DOD has taken steps to address risks posed by contractor ownership in the procurement process.<sup>1</sup> The sensitive report included the results of data analysis we conducted to identify offerors who might disguise their ownership to create the appearance of competition. DOD deemed some of the details from this analysis to be sensitive, which must be protected from public disclosure. This report also omits sensitive information about ongoing investigations, certain internal controls and vulnerabilities, and actions taken to address some of these vulnerabilities. Although the information provided in this report is more limited, it addresses the same overall objectives as the sensitive report and uses the same methodology.

To address our first objective, we researched information on closed cases investigated by the Defense Criminal Investigative Organizations or prosecuted by the Department of Justice (DOJ) from calendar years 2012 through 2018.<sup>2</sup> These cases were identified by researching press releases from the websites of the DOJ Office of Public Affairs, Offices of the U.S. Attorney, DOD Office of Inspector General, and Defense Criminal Investigative Organizations. We also researched legal databases and news articles involving DOD contractors to identify federal court cases and federal agency decisions. We reviewed GAO bid-protest decisions to identify cases in which a contractor may have failed to disclose foreign ownership or concealed beneficial-owner information to obtain contracts that they were not eligible to receive. We interviewed investigators from the Defense Criminal Investigative Organizations and DOD contracting offices to supplement our research. For each case identified, we reviewed the associated federal court filings or DOJ press

---

<sup>1</sup>GAO, *Defense Procurement: Ongoing DOD Fraud Risk Assessment Efforts Should Include Contractor Ownership*, GAO-19-549SU (Washington, D.C.: Sept. 12, 2019).

<sup>2</sup>Defense Criminal Investigative Organizations refer to the Defense Criminal Investigative Service, the Army Criminal Investigation Command, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations, collectively. We chose this period to capture cases adjudicated or settled within 5 years of when we began our audit work. Given that it takes time for cases of alleged fraud to be adjudicated or settled, the fraudulent transactions that are described in these 32 cases may have actually occurred prior to 2012.

releases to determine the outcome of the case and how contractor ownership was used or concealed to carry out the offense.

To identify additional types of risks that may not have been identified through our case-study research, we interviewed officials from the General Services Administration (GSA) and officials from across DOD, including the Office of Inspector General, Defense Criminal Investigative Organizations, Defense Pricing and Contracting, the Office of the Under Secretary of Defense (Comptroller) (OUSD[C]), the Office of the Chief Information Officer, Defense Intelligence Agency (DIA), Defense Security Service (DSS), Defense Logistics Agency (DLA), Defense Contract Management Agency (DCMA), and Defense Contract Audit Agency, and relevant procurement policy officials from the Departments of the Army, Navy, and Air Force. We examined known risks identified through our case-study research and interviews with DOD officials; however, these risks are not necessarily representative of the extent or the types of these risks. There may be additional fraud or other risks and cases related to contractor ownership that are presently undiscovered fraud and are not identified in our report.

Additionally, we further examined the risk that contractors could be disguising their ownership to create the appearance of competition on a contract to inflate prices by analyzing bid response data from GSA's Federal Business Opportunities (FBO) website and registration data in GSA's System for Award Management (SAM). Specifically, we analyzed responses to approximately 2,700 solicitations submitted for fiscal years 2015 through 2017 to identify indications of potentially related offerors bidding on the same solicitation.<sup>3</sup> We selected this date range because fiscal year 2015 was the first year in which the Federal Acquisition Regulation (FAR) required offerors to report their ownership and fiscal year 2017 was the most-recent complete year of data at the time of our analysis. To identify whether offerors were potentially related, we analyzed information to identify instances in which different offerors

---

<sup>3</sup>Specifically, we analyzed solicitations having more than one response through FBO's bid module. According to DOD officials, there is no DOD system that comprehensively captures data on the identities of its offerors. Information containing the identities of the offerors of DOD solicitations is often maintained in individual contract files, and not in a machine-readable format. The FBO system has an optional bid module that contracting offices can elect to use that allows offerors to respond to solicitations directly through the website and thus captures the identities of offerors for a limited number of solicitations.

shared certain information.<sup>4</sup> Offerors sharing information does not definitively prove that the offerors are related or share ownership; however, it is an indicator that these offerors may not be independent of each other. For offerors we identified as potentially related, we researched company websites and third-party data sources to determine whether we could find other indicators of a relationship. Further, we provided a list of the potentially related offerors we identified to the relevant DOD contracting office to determine whether the offeror disclosed any relationships to other offerors or whether the contracting officer was otherwise aware of the relationship with another offeror. The results of our analysis are limited to the approximately 2,700 solicitations we reviewed and are not generalizable to other DOD solicitations.

To assess the reliability of the data used in our analysis, we performed electronic testing to determine the validity of specific data elements in the FBO bid module and other datasets. We also reviewed documentation related to these databases, compared the data to published sources and source documentation maintained in the DOD contracting files, and interviewed GSA officials responsible for these databases. We determined that the data were sufficiently reliable for the purposes of analyzing potential ownership relationships.

To address our second objective, we reviewed federal laws, the FAR, DOD regulations, directives, instructions, policies, procedures, and training documents. We also reviewed OUSD(C) fraud assessment templates and preliminary results from DOD's fraud risk management pilot program. We interviewed procurement policy officials from GSA, Defense Pricing and Contracting, DLA, and the Departments of the Army, Navy, and Air Force as well as officials from the Office of the Chief Information Officer, OUSD(C), DIA, DSS, DCMA, the Defense Contract Audit Agency, the Joint Staff Logistics Directorate, the Defense Industrial Policy office, members of DOD's Procurement Fraud Working Group, and the Naval Contracting Council to discuss how DOD has addressed risks. We also interviewed officials from the Defense Acquisition University to determine how, if at all, DOD trained contracting officials to consider risks posed by contractor ownership. To assess these efforts, we compared these documents and the information from our interviews to federal internal control standards and the leading practices outlined in GAO's

---

<sup>4</sup>Additional details discussing the methodology of our analysis and specific information shared by different offerors were deemed sensitive by DOD and have been omitted from this report.

---

Framework for Managing Fraud Risks in Federal Programs.<sup>5</sup> To gain the perspectives of contractors on whether a requirement to report beneficial-ownership information when doing business with DOD would impose a burden on companies, we researched and contacted several government contractors' associations to gain the perspectives of their members. The contractors' associations we contacted included associations for large, medium, and small businesses working in a variety of industries doing business with the government. We received responses to our inquiries from three associations. To gain their members' perspectives, officials from the three associations forwarded our inquiries to their members and we received responses from 16 members. These 16 members were from a range of business sizes and industries. The perspectives gained from our queries are limited to the contractors from whom we received a response and are not generalizable to all contractors.

We conducted this performance audit from August 2017 to September 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with DOD from September 2019 to November 2019 to prepare this version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

---

<sup>5</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014); and *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 2015).

---

# Appendix II: Summary of GAO Review of Cases Adjudicated or Settled from Calendar Years 2012 through 2018

---

The table below summarizes the information we reviewed involving Department of Defense (DOD) contractors or subcontractors that provided false information about ownership or corporate structure to allegedly commit fraud. We identified cases involving contractors that posed financial and nonfinancial risks to DOD (see app. I for additional details on the methodology used). Financial risks we identified involved DOD contractors using opaque ownership structures to fraudulently inflate prices on DOD contracts. We also identified subcontractors that misrepresented ownership or shared common ownership with a contractor for the purpose of obtaining awards or overcharging the government. Nonfinancial risks we identified involved contractors bidding on and obtaining contracts that they were not eligible to receive, including contracts set aside for small businesses owned by service-disabled veterans or socially and economically disadvantaged individuals. We also identified cases involving ineligible foreign manufacturers creating domestic shell companies to obtain government contracts. As discussed in our report, DOD has not assessed risks posed by contractor ownership; therefore the magnitude and prevalence of these risks are not known. There may be additional risks and cases related to contractor ownership that are not identified below.

The 32 cases below were adjudicated or settled from calendar years 2012 through 2018. As shown in the table below, we used public court records and Department of Justice and DOD press releases to identify the type of fraud and calendar years in which the cases were adjudicated or settled, a summary of how the contractor's ownership was disguised or obfuscated to carry out the fraud schemes, dollar amount awarded or received to the extent available in each case, and the government agencies affected by the fraud.

**Appendix II: Summary of GAO Review of  
Cases Adjudicated or Settled from Calendar  
Years 2012 through 2018**

**Table 1: Summary of GAO Review of 32 Court Cases of Department of Defense (DOD) Contractor Ownership–Related Fraud Adjudicated or Settled from Calendar Years 2012 through 2018**

<b>Case number: type of fraud (year adjudicated or settled)</b>	<b>Summary of fraud scheme</b>	<b>Amount awarded or received<sup>a</sup> (dollars)</b>	<b>Affected government agencies</b>
Case 1: Circumventing debarment (2017)	<p>A DOD contractor and its owner were debarred from doing any business with the United States from 2013 through 2016 for supplying defective and nonconforming aircraft parts to DOD.</p> <p>The debarred company’s owner created three shell companies to circumvent debarment and to continue contracting with DOD between 2013 and 2016. He concealed his involvement in the contractors by using the names of relatives and fictitious individuals as the responsible individuals at these companies.</p> <p>Defective aircraft parts continued to be provided to DOD by the shell companies.</p>	2.8 million received	DOD
Case 2: Concealing relationship to foreign manufacturer (2017)	<p>An individual established a shell company in the United States to bid on DOD contracts that required parts to be manufactured in the United States. This contractor fraudulently received 346 government contracts from 2010 until 2015.</p> <p>The contractor falsely stated to DOD that the contractor was a U.S.-based manufacturer in order to be eligible for the awards while a foreign company manufactured the parts.</p> <p>The contractor’s owner was able to access and download thousands of technical drawings, including those subject to U.S. export control regulations that require a license from the State Department while not in the United States, by falsely stating he was a U.S. citizen.</p> <p>In multiple instances, parts supplied by the contractor were unusable due to design flaws and nonconformities.</p>	7.3 million awarded	DOD
Case 3: Concealing relationship with foreign manufacturer (2016)	<p>Two shell companies misrepresented domestic manufacturing to bid for DOD contracts that the companies were not eligible to receive from 2010 to 2012.</p> <p>The shell companies provided spare parts manufactured in a foreign production facility co-owned by the contractor’s owner. The companies exported drawings of military technology and sensitive military data to an individual in a foreign country without the proper license or approval.</p> <p>There were quality-control issues with the parts that were ultimately provided to DOD that led to the grounding of 47 fighter aircraft.</p>	Not stated in court documents	DOD

**Appendix II: Summary of GAO Review of  
Cases Adjudicated or Settled from Calendar  
Years 2012 through 2018**

<b>Case number: type of fraud (year adjudicated or settled)</b>	<b>Summary of fraud scheme</b>	<b>Amount awarded or received<sup>a</sup> (dollars)</b>	<b>Affected government agencies</b>
Case 4: Concealing relationship with foreign manufacturer (2015)	<p>A shell company was created in the United States for the purpose of contracting with the government and obtaining DOD contracts that foreign-based manufacturers were not permitted to receive. This shell company received payments from DOD from June 2011 to September 2013.</p> <p>The contractor's owner was a foreign citizen who was also president of a foreign manufacturing company. The foreign company was used to manufacture replacement aircraft parts and other defense items against the terms of the contract.</p> <p>Despite claiming to be a domestic company, contract payments were wired to a foreign bank account, the majority of which were transferred to the bank account of the foreign manufacturing company.</p> <p>The contractor's owner used an alias to receive access to military critical technical data that he was not eligible to access as a foreign citizen.</p>	Over 635,000 received	DOD
Case 5: Concealing relationship with foreign manufacturer (2015)	<p>Two shell companies were created in the United States for the purpose of contracting with the government and obtaining DOD contracts that foreign-based manufacturers were not permitted to receive. The shell companies received payment from the government from 2009 to 2014.</p> <p>An owner of the shell companies used an alias when submitting bids for contracts and when corresponding with the government.</p> <p>Parts supplied to the government were nonconforming and were unable to be used.</p>	1.3 million received	DOD
Case 6: Concealing company ownership for illicit financial gain (2018)	<p>A Navy officer used his relationship with Navy prime contractors to instruct them to subcontract with and steer funds to three shell companies.</p> <p>The Navy officer registered one of the shell companies, along with two other individuals, and approached other individuals to set up the other two companies. These three shell subcontractors operated in 2014 and 2015 and did not provide the prime contractor or the Navy with any goods or services.</p> <p>As part of the scheme, the individuals distributed funds among themselves for personal gain rather than provide the Navy with any value.</p>	2.7 million received	DOD



**Appendix II: Summary of GAO Review of  
Cases Adjudicated or Settled from Calendar  
Years 2012 through 2018**

<b>Case number: type of fraud (year adjudicated or settled)</b>	<b>Summary of fraud scheme</b>	<b>Amount awarded or received<sup>a</sup> (dollars)</b>	<b>Affected government agencies</b>
Case 7: Concealing company ownership for illicit financial gain (2017)	<p>Members of a contractor's management engaged in a scheme to ensure that their company's bids would be selected by DOD as the supposed low bidder.</p> <p>The contractor's management submitted fraudulent bids that were either entirely fictitious, contained falsified prices supposedly from actual businesses, or fraudulently stated that the business shown on the letterhead could not provide the items or services requested.</p> <p>Individuals involved with the scheme admitted that submitting the fraudulent bids allowed the company to control and inflate the prices charged to DOD without any true, competitive bidding, as required.</p> <p>This contractor was also involved with bribing government officials in exchange for the approval of fraudulent invoices, steering contracts, and covering up the contractor's overcharging practices that has led to at least 22 individuals pleading guilty.</p>	Not stated in court documents. 34.8 million estimated loss to the government	DOD
Case 8: Concealing company ownership for illicit financial gain (2016)	<p>A whistleblower alleged that a contractor used shell companies to fraudulently bill the government for unlawful profits and work it did not perform in 2004 and 2005.</p> <p>The government alleged in court that this company created two shell affiliates, to which it subcontracted work related to a U.S. Army contract. One of the shell companies had no employees to perform the services under the contract.</p> <p>These shell companies further subcontracted the work to other companies, and later billed the contractor for the cost of this work, plus additional, undisclosed profits.</p>	Not stated in court documents	DOD
Case 9: Concealing company ownership for illicit financial gain (2015)	<p>An employee of a DOD subcontractor formed two shell companies for the purpose of profiting from government contracts.</p> <p>The employee used his position as a project manager on a construction project for a government contract to instruct two of his employer's vendors to subcontract with the companies he created and owned. This individual did not disclose that he was associated with the company and informed the vendors that it was not necessary to reference his companies in paperwork submitted to his employer.</p> <p>No materials or services were ever provided to the vendor by the two shell companies.</p>	Approximately 600,000 awarded	DOD

**Appendix II: Summary of GAO Review of  
Cases Adjudicated or Settled from Calendar  
Years 2012 through 2018**

<b>Case number: type of fraud (year adjudicated or settled)</b>	<b>Summary of fraud scheme</b>	<b>Amount awarded or received<sup>a</sup> (dollars)</b>	<b>Affected government agencies</b>
Case 10: Concealing company ownership for illicit financial gain (2014)	<p>An employee of a DOD contractor and his wife formed a company and concealed their names on company formation documents. Instead, these individuals listed the names of family members as company managers. The company was formed with the purpose of doing business with a DOD contractor.</p> <p>The contractor employee, in his official position, wrote letters justifying awards of purchase orders for parts to his own company without competitive quotes and, in instances in which there had been competitive quotes, approving recommendations that the awards be made to his company.</p> <p>The co-owner of the subcontractor signed contracts as the subcontractor's agent using her maiden name knowing that the use of her married name could reveal the DOD contractor employee's involvement in the company and affect the awards.</p>	At least 9.7 million awarded	DOD
Case 11: Concealing company ownership for illicit financial gain (2014)	<p>The contractor purchased goods from a company that its owners created and controlled, and instructed the company to fraudulently mark up prices on items that were resold to DOD from 2005 to 2009.</p> <p>The contractor and its owners made efforts to conceal its relationship with its subcontractor to appear to make the fraudulent markups appear legitimate.</p> <p>Contractor personnel were responsible for hiring individuals to work for the subcontractor, and subcontractor employees were paid from a bank account controlled by the prime contractor and its owners.</p> <p>In 2014, the contractor pled guilty to major fraud against the United States and agreed to pay \$434 million in criminal penalties.</p>	48 million received	DOD
Case 12: Concealing company ownership for illicit financial gain (2013)	<p>Two employees of a government prime contractor created a sham company to act as an additional subcontractor between prime contractors and subcontractors.</p> <p>The true nature of the ownership and control of the sham subcontractor was concealed by omitting facts and purportedly transferring ownership of the company to another individual that did not actually control the company.</p> <p>The sham subcontractor added no value to the government and carried no inventory, but still submitted invoices for payment, causing prime contractors to overcharge DOD by including these fraudulent charges in the prime contractor invoices.</p>	Approximately 33.5 million awarded	DOD

**Appendix II: Summary of GAO Review of  
Cases Adjudicated or Settled from Calendar  
Years 2012 through 2018**

<b>Case number: type of fraud (year adjudicated or settled)</b>	<b>Summary of fraud scheme</b>	<b>Amount awarded or received<sup>a</sup> (dollars)</b>	<b>Affected government agencies</b>
Case 13: Set-aside contracting fraud (2018)	<p>A contractor falsely represented itself as a service-disabled veteran-owned small business and obtained 20 government construction contracts from 2005 to 2013. The contractor was a front company for another company owned by a nonveteran that performed the work on the contract.</p> <p>Federal regulations require that to be eligible as a service-disabled veteran-owned small business to receive government set-aside contracts, the small businesses must be at least 51 percent owned and controlled by an eligible service-disabled veteran and service-disabled veterans must control the daily operation and long-term decision-making of the company.</p> <p>The contractor falsely certified that the disabled veteran was involved in the daily operations of the contractor.</p>	13.8 million awarded	DOD, Department of Veterans Affairs
Case 14: Set-aside contracting fraud (2018)	<p>A joint venture was created between a company owned by a service-disabled veteran and a nonveteran to appear qualified to receive contracts set aside for service-disabled veteran-owned businesses. The joint venture fraudulently obtained contracts from 2010 to 2015.</p> <p>Federal regulations require that an eligible joint venture be managed by a service-disabled veteran-owned small business and at least 40 percent of the joint venture's work must be performed by the eligible service-disabled veteran-owned small business.</p> <p>The service-disabled veteran status was used to bid on contracts while the nonveteran-owned small business performed the work and retained 98 percent of every payment from the government. The nonveteran also owned and controlled the day-to-day operations of the joint venture while the service-disabled veteran worked full-time for another entity.</p>	11 million awarded	DOD, Department of Veterans Affairs
Case 15: Set-aside contracting fraud (2018)	<p>An individual formed a company and listed a service-disabled veteran as the majority owner and president even though he was physically incapable of managing the company due to illness.</p> <p>The company was registered as a service-disabled veteran-owned small business for the purpose of bidding on contracts set aside for this type of company, despite the service-disabled veteran not managing the company's day-to-day activities.</p> <p>The company was managed and controlled by a nonveteran who continued to claim the veteran was the majority owner even after his death and forged his signature in documents submitted to the government. Another company, ineligible for set-aside contracts and owned by the nonveteran, performed all of the work on 11 contracts fraudulently obtained from calendar years 2009 to 2013.</p>	11.6 million awarded	DOD

**Appendix II: Summary of GAO Review of  
Cases Adjudicated or Settled from Calendar  
Years 2012 through 2018**

<b>Case number: type of fraud (year adjudicated or settled)</b>	<b>Summary of fraud scheme</b>	<b>Amount awarded or received<sup>a</sup> (dollars)</b>	<b>Affected government agencies</b>
Case 16: Set-aside contracting fraud (2018)	<p>The contractor self-certified that it met the small-business size requirements for eligibility to receive small-business innovation and research funding between 2008 and 2015 and was awarded multiple small-business innovation and research contracts by the Air Force, Army, and Navy.</p> <p>The small-business innovation and research program is designed to stimulate technological innovation by funding small businesses to engage in federal research and development efforts. According to a Department of Justice press release discussing this case, a contractor must not be majority owned by another company to be considered a small business for the purpose of small-business innovation and research awards.</p> <p>The contractor was not eligible for the small-business innovation and research contracts it was awarded because it was a majority-owned subsidiary of another company at the time it was awarded and performed on small-business innovation and research contracts.</p> <p>The contractor paid \$12.1 million to the government to resolve these allegations.</p>	Not stated in court documents	DOD
Case 17: Set-aside contracting fraud (2018)	<p>An eligible contractor bid on and obtained small business set-aside contracts while having an agreement with two separate companies that performed the majority of the work against the set-aside contracting program rules. The eligible contractor was paid a kickback by the companies performing the work as part of this agreement.</p> <p>The contractor paid \$7.8 million to the government to resolve these allegations.</p>	Not stated in court documents	DOD
Case 18: Set-aside contracting fraud (2018)	<p>Two contractors fraudulently claimed they were owned and controlled by eligible individuals in order to win government contracts set aside for a particular type of business.</p> <p>One contractor claimed it was owned by a service-disabled veteran who essentially had no involvement in the company. The other contractor claimed to be owned by an economically disadvantaged individual that worked full-time for another entity and did not control the contractor.</p> <p>A third company not eligible for government set-aside contracts performed the majority of the work awarded to the service-disabled veteran– and economically disadvantaged–owned firms.</p>	Over 200 million received	DOD, Department of Veterans Affairs

**Appendix II: Summary of GAO Review of  
Cases Adjudicated or Settled from Calendar  
Years 2012 through 2018**

<b>Case number: type of fraud (year adjudicated or settled)</b>	<b>Summary of fraud scheme</b>	<b>Amount awarded or received<sup>a</sup> (dollars)</b>	<b>Affected government agencies</b>
Case 19: Set-aside contracting fraud (2018)	<p>An ineligible individual sought to form a service-disabled veteran–owned small business to seek contracts set aside for this type of business and sought a disabled veteran to form the company with him.</p> <p>The contractor’s owner made false statements to DOD, the General Services Administration, and the Small Business Administration from 2008 to 2015 stating that the contractor qualified as a service-disabled veteran–owned small business when he knew that it did not.</p> <p>The disabled veteran acted as a figurehead who was paid for allowing his name to be used by the business, worked full-time for another company in a different state from the contractor, and according to a witness was rarely in the office and did not approve any business decisions.</p>	32.5 million awarded	DOD
Case 20: Set-aside contracting fraud (2017)	<p>Three contractors reached a settlement agreement with the government to resolve the allegations below.</p> <p>The contractor was a shell company that did not perform work on contracts awarded to it and did not qualify for the service-disabled veteran–owned small business contracts that it received from 2008 to 2011.</p> <p>It was alleged in a civil complaint that the contractor was not managed or controlled by a service-disabled veteran and did not have any employees or capacity to perform at least the 15 percent of the contract work required by law.</p> <p>The contracting company was created for the purpose of bidding and obtaining government contracts that were set aside for service-disabled veteran–owned small businesses while two other ineligible companies performed the work. The headquarters listed as belonging to the contractor was actually the corporate office of another company.</p>	Approximately 21 million awarded	DOD, Department of Veterans Affairs
Case 21: Set-aside contracting fraud (2017)	<p>The contractor was a shell company with no full-time employees and was used to bid on and receive a contract under the Small Business Administration’s 8(a) program intended for businesses owned by minority or disadvantaged individuals from 2011 to 2014.</p> <p>A company that was ineligible for 8(a) contracts, because its revenue was too high, reached an agreement with the contractor to perform substantially all of the work. The contractor’s owner submitted false statements to the Small Business Administration when answering questions regarding the work to be performed by the company.</p> <p>According to the criminal complaint in this case, the terms of the contract required the eligible 8(a) contractor to perform 35 percent of the work on the contract and not subcontract any of the requirements without prior written approval.</p>	Over 1.1 million awarded	DOD

**Appendix II: Summary of GAO Review of  
Cases Adjudicated or Settled from Calendar  
Years 2012 through 2018**

<b>Case number: type of fraud (year adjudicated or settled)</b>	<b>Summary of fraud scheme</b>	<b>Amount awarded or received<sup>a</sup> (dollars)</b>	<b>Affected government agencies</b>
Case 22: Set-aside contracting fraud (2016)	<p>An individual utilized two shell companies to receive 27 government set-aside contracts for small disadvantaged businesses that his company was not eligible to receive from 2008 to 2013.</p> <p>Two contractors were certified to participate in the Small Business Administration's 8(a) program for disadvantaged businesses. The contractors partnered with an ineligible company and allowed it to have access to its contracts.</p> <p>Even though it was not eligible to receive set-aside contracts, the company performed all the work on the contracts awarded to the two shell companies.</p>	Over 70.2 million awarded	DOD, General Services Administration, Department of the Interior, Department of Homeland Security
Case 23: Set-aside contracting fraud (2016)	<p>A contractor acquired government contracts between 2006 and 2010 by falsely representing to federal contracting officers that the company was owned and operated by service-disabled veterans.</p> <p>When the contractor was formed in 2006, a disabled veteran was recruited to act as the company's straw owner for the sole purpose of obtaining federal contracts set aside under the service-disabled veteran-owned small-business program. A second disabled veteran was added to serve as the figurehead owner of the contractor after the initial veteran's health deteriorated.</p>	Over 113 million awarded	DOD, Department of Veterans Affairs, General Services Administration
Case 24: Set-aside contracting fraud (2016)	<p>An individual utilized the stolen name and Social Security number of a service-disabled veteran to create a fraudulent service-disabled veteran-owned small business for the purpose of obtaining government contracts set aside for small businesses that are majority-owned and controlled by a service-disabled veteran.</p> <p>This individual first used the stolen information to obtain certification as a service-disabled veteran-owned small business in October 2009 and fraudulently obtained 14 government contracts and received funds from the government from 2013 to 2015.</p>	2.7 million awarded	DOD, Department of Veterans Affairs
Case 25: Set-aside contracting fraud (2016)	<p>A company and its employees created a shell company for the purpose of obtaining contracts set aside for service-disabled veterans from 2009 to 2012.</p> <p>A service-disabled veteran was hired as a figurehead to allow the shell company to bid on and obtain set-aside contracts from the government while allowing the other company to perform the work on the contracts.</p> <p>The veteran did not have any significant management over the company, and instead was responsible for overseeing tools and plowing snow for the company that improperly performed the work on the contracts.</p>	Approximately 14.4 million awarded	DOD, Department of Veterans Affairs

**Appendix II: Summary of GAO Review of  
Cases Adjudicated or Settled from Calendar  
Years 2012 through 2018**

<b>Case number: type of fraud (year adjudicated or settled)</b>	<b>Summary of fraud scheme</b>	<b>Amount awarded or received<sup>a</sup> (dollars)</b>	<b>Affected government agencies</b>
Case 26: Set-aside contracting fraud (2015)	<p>Two contractors falsely represented to the government that they were two separate and distinct entities, but operated from the same location and comingled employees and assets.</p> <p>The contractors used aliases and false identities to communicate with DOD and also fabricated the companies' performance history by using fictitious references.</p> <p>The companies also made false representations to the government regarding ownership and eligibility for service-disabled veteran-owned small-business contracts in order to receive contracts they were not eligible to receive from 2007 to 2013.</p>	Over 30 million awarded	DOD
Case 27: Set-aside contracting fraud (2015)	<p>Two companies used legitimate disadvantaged businesses as shell companies to obtain government set-aside contracts between 2008 and 2014 by using the disadvantaged businesses names when bidding for contracts.</p> <p>Noneligible companies actually performed the work covered by the contracts, and paid the owners of the bidding companies a percentage of the contract value.</p>	Over 2.6 million awarded	DOD, Department of the Interior
Case 28: Set-aside contracting fraud (2015)	<p>The contractor was a front company that used a service-disabled veteran as a figurehead to obtain contracts set aside for service-disabled veteran-owned small businesses. This contractor fraudulently received 45 government contracts from calendar years 2007 to 2010.</p> <p>When making bids for government contracts, the service-disabled veteran represented himself as the president of the company, but a nonveteran actually controlled the company and listed himself as the president and 100 percent owner in other company documents not submitted to the government.</p>	23.4 million awarded	DOD, Department of Veterans Affairs
Case 29: Set-aside contracting fraud (2014)	<p>An ineligible company bid on and was awarded contracts that had been set aside for service-disabled veteran-owned small businesses from 2007 to 2009.</p> <p>The company claimed that a service-disabled veteran was the majority owner, but the veteran had no affiliation or involvement in the company and was really the receptionist at another company controlled by the founder of the ineligible company.</p> <p>The veteran's signature was forged on letters submitted to the government.</p> <p>This company did not pay some of its 31 veteran employees a total of approximately \$100,000 in wages that were required under the terms of the contract.</p>	1.9 million awarded	DOD, Departments of Homeland Security and Veterans Affairs

**Appendix II: Summary of GAO Review of  
Cases Adjudicated or Settled from Calendar  
Years 2012 through 2018**

<b>Case number: type of fraud (year adjudicated or settled)</b>	<b>Summary of fraud scheme</b>	<b>Amount awarded or received<sup>a</sup> (dollars)</b>	<b>Affected government agencies</b>
Case 30: Set-aside contracting fraud (2014)	<p>The contractor used a figurehead owner to obtain Small Business Administration 8(a) contracting preferences by falsely claiming that a minority individual was the majority owner. A noneligible individual actually exercised complete and undisclosed control over the contractor's operations, including the day-to-day management and long-term decision-making.</p> <p>The contractor was awarded contracts that it was not entitled to receive from 1999 to 2013 based on the fraudulent 8(a) application and annual updates to the Small Business Administration stating that the company was controlled by a socially and economically disadvantaged individual.</p>	52.9 million awarded	DOD, Department of Commerce, Department of the Interior, Social Security Administration, General Services Administration
Case 31: Set-aside contracting fraud (2013)	<p>The contractor used a figurehead owner to fraudulently obtain Small Business Administration 8(a) contracting preferences by falsely claiming that this individual, with a history of social disadvantage, formed and founded the company and was the only member of its management.</p> <p>The contractor also used its funds to bribe a U.S. government official who agreed to help the company win contracts.</p>	31.8 million received	DOD, National Aeronautics and Space Administration, General Services Administration, Department of Homeland Security, U.S. Nuclear Regulatory Commission, Department of the Interior, National Oceanic and Atmospheric Administration, Department of Health and Human Services
Case 32: Set-aside contracting fraud (2012)	<p>A DOD contractor became ineligible to receive contracts set aside for small businesses after receiving a \$50 million contract. To continue bidding on such contracts, the owner and Vice President of the contractor formed a new company and recruited a sham owner to appear as its owner on legal documents.</p> <p>The owner and Vice President always maintained true ownership and control over the new company and were the only signatories on the new company's bank accounts.</p> <p>In 2007, the new company fraudulently bid on and was awarded a 5-year \$100 million small-business set-aside contract. The company received payment from DOD for the contract until 2011 with its owners profiting approximately \$10.9 million.</p> <p>The true owners of the company repeatedly lied to the government, submitted material misrepresentations, and omitted critical facts about their true ownership and control over both companies.</p>	100 million awarded	DOD

Source: GAO analysis of federal court records and DOD and Department of Justice information. | GAO-20-106

<sup>a</sup>The amount included was the amount available in the court documents or Department of Justice press release for each case. This amount represents the amount awarded or the amount received due to false misrepresentations, as noted throughout.



---

# Appendix III: GAO Contact and Staff Acknowledgments

---

---

## GAO Contact

Seto J. Bagdoyan at 202-512-6722 or [bagdoyans@gao.gov](mailto:bagdoyans@gao.gov)

---

## Staff Acknowledgments

In addition to the contact named above, the following staff members made key contributions to this report: Tonita Gillich (Assistant Director); Tracy Abdo (Analyst-in-Charge); Marissa Esthimer; Colin Fallon; Mollie Lemon; Maria McMullen; Madeline Messick; Dustin Milne; Lauren Ostrander; Daniel Purdy; Daniel Silva; Sabrina Streagle; and Shana Wallace. Others who contributed to this report include Steven Campbell, Suellen Foth, and Pamela Snedden.

---

## 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 GAO's website (<https://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <https://www.gao.gov> and select "E-mail Updates."

---

## Order by Phone

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

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

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

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).  
Subscribe to our [RSS Feeds](#) or [E-mail 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/fraudnet/fraudnet.htm>

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

---

## Congressional Relations

Orice Williams Brown, Managing Director, [WilliamsO@gao.gov](mailto:WilliamsO@gao.gov), (202) 512-4400,  
U.S. Government Accountability Office, 441 G Street NW, Room 7125,  
Washington, DC 20548

---

## Public Affairs

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

---

## Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, [spel@gao.gov](mailto:spel@gao.gov), (202) 512-4707  
U.S. Government Accountability Office, 441 G Street NW, Room 7814,  
Washington, DC 20548



Please Print on Recycled Paper.