United States Government Accountability Office

Report to the Honorable Gary C. Peters, U.S. Senate

January 2021

DEPARTMENT OF ENERGY CONTRACTING

Improvements Needed to Ensure DOE Assesses Its Full Range of Contracting Fraud Risks

A Century of Non-Partisan Fact-Based Work

GAO-21-44

GAO@100
Highlights

Highlights of GAO-21-44, a report to the Honorable Gary C. Peters, U.S. Senate

January 2021

DEPARTMENT OF ENERGY CONTRACTING

Improvements Needed to Ensure DOE Assesses Its Full Range of Contracting Fraud Risks

Why GAO Did This Study

DOE relies primarily on contractors to carry out its missions at its laboratories and other facilities, spending approximately 80 percent of its total obligations on contracts. GAO and DOE's Inspector General have reported on incidents of fraud by DOE contractors and identified multiple contracting fraud risks.

GAO was asked to examine DOE's processes to manage contracting fraud risks. This report examines, for DOE, (1) types of contracting fraud schemes and their financial and nonfinancial impacts, (2) steps taken to commit to combating contracting fraud risks and the extent to which these risks have been assessed, and (3) steps taken to design and implement an antifraud strategy and to evaluate and adapt its approach.

GAO reviewed relevant laws and guidance; reviewed agency media releases, Agency Financial Reports, and DOE Inspector General reports to Congress from 2013 through 2019; and reviewed documents and interviewed officials from 42 DOE field and site offices, contractors, and subcontractors, representing a range of sites and programs.

What GAO Recommends

GAO is making two recommendations, including for DOE to expand its fraud risk assessment methodology to ensure all fraud risks facing DOE programs are fully assessed and documented in accordance with leading practices. DOE concurred with GAO's recommendations.

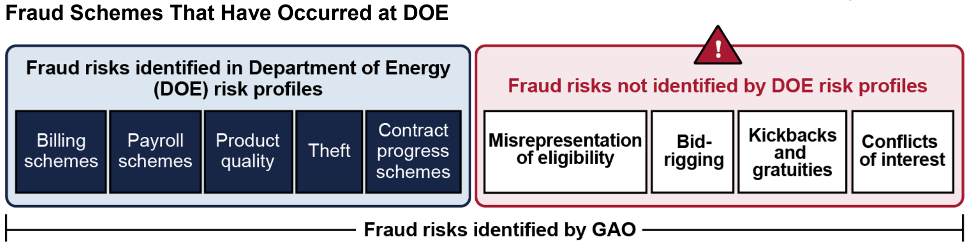
View GAO-21-44. For more information, contact Rebecca Shea at (202) 512-6722 shear@gao.gov or Allison B. Bawden at (202) 512-3841, bawdena@gao.gov

What GAO Found

GAO identified nine categories of contracting fraud schemes that occurred at the Department of Energy (DOE), including billing schemes, conflicts of interest, and payroll schemes. For example, a subcontractor employee at a site created fraudulent invoices for goods never received, resulting in a loss of over $6 million. In another scheme, a contractor engaged in years of widespread time card fraud, submitting inflated claims for compensation. The contractor agreed to pay $18.5 million to settle the case. DOE reported that it identified nearly $15 million in improper payments due to confirmed fraud in fiscal year 2019. However, due to the difficulty in detecting fraud, agencies—including DOE—incur financial losses related to fraud that are never identified or are settled without admission to fraud and are not counted as such. Fraud can also have nonfinancial impacts, such as fraudsters obtaining a competitive advantage and preventing legitimate businesses from obtaining contracts.

DOE has taken some steps and is planning others to demonstrate a commitment to combat fraud and assess its contracting fraud risks, consistent with the leading practices in GAO's Fraud Risk Framework. However, GAO found that DOE has not assessed the full range of contracting fraud risks it faces. Specifically, GAO found DOE's methods for gathering information about its fraud risks captures selected fraud risks—rather than all fraud risks—facing DOE programs. As shown in the figure, DOE's risk profiles for fiscal years 2018 and 2019 did not capture four of nine fraud schemes that occurred at DOE. For example, one entity did not include any fraud risks in its risk profiles, yet GAO identified six types of fraud schemes that occurred at the entity's site. DOE plans to expand its risk assessment process, but officials expect the new process will continue to rely on a methodology that gathers information on selected fraud risks. The Fraud Risk Framework states that entities identify specific tools, methods, and sources for gathering information about fraud risks. Without expanding its methodology to capture, assess, and document all fraud risks facing its programs, DOE risks remaining vulnerable to these types of fraud.

Fraud Risks Identified in Fiscal Years 2018 and 2019 Risk Profiles Compared with Types of Fraud Schemes That Have Occurred at DOE



Source: GAO analysis of DOE information. | GAO-21-44

DOE is planning to develop an antifraud strategy in fiscal year 2022 and has taken some steps to evaluate and adapt to fraud risks, consistent with leading practices in GAO's Fraud Risk Framework. Part of DOE's effort to manage fraud risks includes adapting controls to address emerging fraud risks. Additionally, DOE is planning to expand its use of data analytics to detect contracting fraud, beginning in fiscal year 2022.

Contents

Figures

Abbreviations

AFR	Agency Financial Reports
DEAR	Department of Energy Acquisition Regulation
DOE	Department of Energy
EA	Entity Assessment
FAR	Federal Acquisition Regulation
FMA	Financial Management Assessment
M&O	management and operating
NNSA	National Nuclear Security Administration
OCFO	Office of the Chief Financial Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget

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

January 13, 2021

The Honorable Gary C. Peters
United States Senate

Dear Senator Peters:

The Department of Energy (DOE)—including the National Nuclear Security Administration (NNSA)—relies primarily on contractors to carry out its diverse missions. For example, in fiscal year 2019, DOE spent approximately 80 percent of its $41 billion in total obligations, primarily on contracts to manage and operate its scientific laboratories, engineering and production facilities, and environmental restoration sites, or to construct facilities. GAO and the DOE Office of Inspector General (OIG) have reported on incidents of fraudulent activity by DOE contractors and subcontractors and identified multiple contracting fraud risks.[1] GAO first designated aspects of DOE's contract management as a high-risk area for the government in 1990 because DOE's record of inadequate management and oversight of contractors left the department vulnerable to fraud, waste, abuse, and mismanagement. Since at least fiscal year 2010, the DOE OIG has also identified contract management as a significant challenge at DOE, and DOE's approach to managing these fraud risks continues to be a concern.[2]

[1]Fraud and "fraud risk" are distinct concepts. Fraud—obtaining something of value through willful misrepresentation—is a determination to be made through the judicial or other adjudicative system. 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. Although the occurrence of fraud indicates there is a fraud risk, a fraud risk can exist even if actual fraud has not yet been identified or occurred.

[2]Each year, the DOE OIG identifies management challenges at the department. In its fiscal year 2018 identification of management challenges, DOE's OIG added subcontract management as a component of its previously identified management challenges for DOE contract oversight, in part because the OIG's investigative work and referrals to the OIG hotline identified continued vulnerabilities from inadequate oversight of subcontracts. Department of Energy, Office of Inspector General, *Management Challenges at the Department of Energy – Fiscal Year 2018*, DOE-OIG-18-09 (Washington, D.C.: Nov. 27, 2017).

In March 2017, we reviewed DOE's approach to managing its risk of fraud and the extent to which that approach incorporated leading practices.[3] We found that DOE did not use leading practices for managing the department's risk of fraud because it considered its risk of fraud to be low. We found that by not implementing leading practices, DOE was missing an opportunity to organize and focus its resources in a way that would allow it to mitigate the likelihood and impact of fraud. We made six recommendations regarding how DOE could implement leading practices to manage the risk of fraud and other improper payments.[4] DOE generally concurred with five of our recommendations but did not concur with the sixth. DOE has started to take some actions to implement the recommendations from our March 2017 report.

You requested that we review DOE's processes for managing its risk related to contracting fraud. This report examines (1) the types of contracting fraud schemes that have been identified at DOE, and the financial and nonfinancial impacts of those schemes; (2) the steps DOE has taken to commit to combating its contracting fraud risks, and the extent to which DOE has assessed those risks; and (3) the steps DOE has taken to design and implement an antifraud strategy and to evaluate and adapt its approach to address contracting fraud risks as they are identified.

To determine the types of contractor fraud schemes that have been identified at DOE and the financial and nonfinancial impacts of those schemes, we obtained publicly available information on incidents and reports of contracting fraud at DOE. Specifically, we obtained information on contracting fraud at DOE by reviewing information on cases that were made public in DOE OIG and Department of Justice media releases and DOE OIG audit reports in calendar years 2013 through 2019.[5] We also

[3]GAO, *Department of Energy: Use of Leading Practices Could Help Manage the Risk of Fraud and Other Improper Payments,* GAO-17-235 (Washington, D.C.: Mar. 30, 2017).

[4]Fraud is distinct from improper payments, as improper payments are any payments that should not have been made or that were made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements. Improper payments include any payment to an ineligible recipient or ineligible service, duplicate payments, payments for services not received, and any payment for an incorrect amount. However, not all improper payments are fraud.

[5]The process for pursuing a fraud case can be lengthy and, thus, some of the schemes we identified occurred before 2013 but were identified in our sources during the 2013 through 2019 time frame that our review covered.

reviewed DOE's Agency Financial Reports (AFR) from fiscal years 2018 and 2019 and DOE OIG semiannual reports to Congress from fiscal years 2013 through 2019 to identify financial and nonfinancial fraud impacts.[6] We conducted a broader literature search of contracting fraud risks and organized the identified DOE schemes in general categories of contracting fraud risks described in the literature. Sources include the Association of Government Accountants, Association of Certified Fraud Examiners, and multiple OIGs.[7]

To determine the extent to which DOE has taken steps to commit to combating its contracting fraud risks, to assess those risks, to design and implement an antifraud strategy, and to evaluate and adapt its approach, we compared documentary and testimonial evidence obtained during our review with selected leading practices from GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework).[8] We reviewed related fraud risk management documentation and interviewed officials from DOE's Office of the Chief Financial Officer (OCFO) and a nonprobability sample of DOE field and site offices, contractors, and subcontractors. We selected this sample to represent a variety of contract sizes, contract types, award types, locations, program offices, contractors with fraud risks present in DOE OIG and Department of Justice media releases, and fraud risks identified by DOE. In total, we conducted 42 semistructured interviews with 12 DOE field and site offices, 12 management and operating (M&O) contractors, 10 non-M&O contractors, and eight subcontractors.[9] In addition, we interviewed

[6]We limited our review of the AFR to fiscal years 2018 and 2019 because DOE did not report improper payments identified for recapture by category—including fraud-related categories such as confirmed fraud and settlements—prior to fiscal year 2018.

[7]We reviewed documents from the OIGs from the Departments of Defense, Transportation, Health and Human Services, and Housing and Urban Development. These OIGs had publicly available information that related to contracting fraud risks.

[8]GAO, *A Framework for Managing Fraud Risks in Federal Programs,* GAO-15-593SP (Washington, D.C.: July 2015). For this review, we selected leading practices that were most relevant for our review. Specifically, we selected leading practices that aligned with themes that had been identified in previous GAO audits related to fraud risk management as well as themes identified during the course of our interviews.

[9]M&O contracts are agreements under which the government contracts for the operation, maintenance, or support, on its behalf, of a government-owned or government-controlled research, development, special production, or testing establishment wholly or principally devoted to one or more of the major programs of the contracting federal agency.

officials from the DOE OIG. For more details about the selection process and the interview methodology, see appendix I.

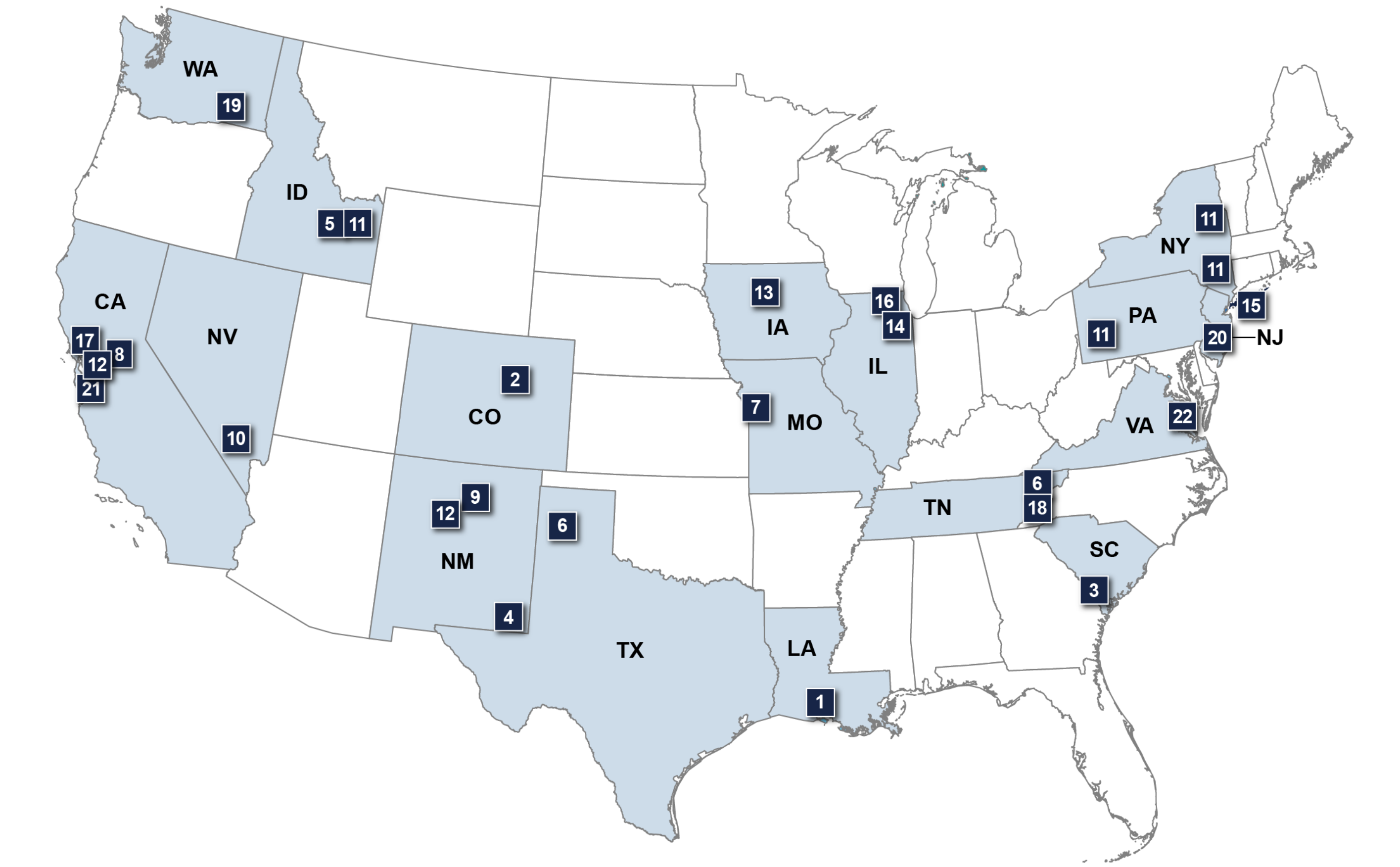
We conducted this performance audit from April 2019 to January 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

DOE Contracting Environment and Organization

DOE relies on contracts to accomplish most of its work. In fiscal year 2019, DOE had 22 M&O contracts at sites across the country (see fig. 1). In addition, DOE uses non-M&O contracts to provide other goods or services not related to managing and operating government-owned facilities. DOE is organized into program offices that oversee the agency's numerous programs. These program offices primarily oversee mission-related activities and are responsible for integrating the activities across the multiple sites performing work. Three DOE program offices—NNSA, the Office of Science, and the Office of Environmental Management—award about 75 percent of DOE's obligations. DOE field offices provide oversight to two or more site offices. Site offices are co-located with the M&Os and oversee the day-to-day activities of the contractors as well as mission support functions, such as safety.

Figure 1: Department of Energy Management and Operating Contract Sites, by Program Office



Program office/operating contract sites name

Fossil energy
1. Strategic Petroleum Reserve Office

Energy efficiency and renewable energy
2. National Renewable Energy Laboratory

Environmental management
3. Savannah River Site
4. Waste Isolation Pilot Plant

Nuclear energy
5. Idaho National Laboratory

National Nuclear Security Administration (NNSA)
6. Pantex Plant/ Y-12 National Security Complex
7. Kansas City National Security Campus
8. Lawrence Livermore National Laboratory
9. Los Alamos National Laboratory
10. Nevada National Security Site
11. Naval Nuclear Laboratory
12. Sandia National Laboratories

Science
13. Ames Laboratory
14. Argonne National Laboratory
15. Brookhaven National Laboratory
16. Fermi National Accelerator Center
17. Lawrence Berkeley National Laboratory
18. Oak Ridge National Laboratory
19. Pacific Northwest National Laboratory
20. Princeton Plasma Physics Laboratory
21. SLAC National Accelerator Laboratory
22. Thomas Jefferson National Accelerator Facility

Sources: Department of Energy; Map Resources (map). | GAO-21-44

Note: Sites in this figure with the same number operate under the same contract.

DOE's oversight of contractors is subject to the Federal Acquisition Regulation (FAR), the Department of Energy Acquisition Regulation (DEAR),[10] and other internal DOE directives. Specifically, DOE's 15 field Chief Financial Officers, in cooperation with DOE contracting officers, are responsible for overseeing contractor and other activities in the field, and they assist the OCFO. The OCFO is responsible for directing, managing, and providing policy guidance and oversight of DOE financial management personnel, activities, and operations.

Government-wide Requirements for Managing Fraud Risk

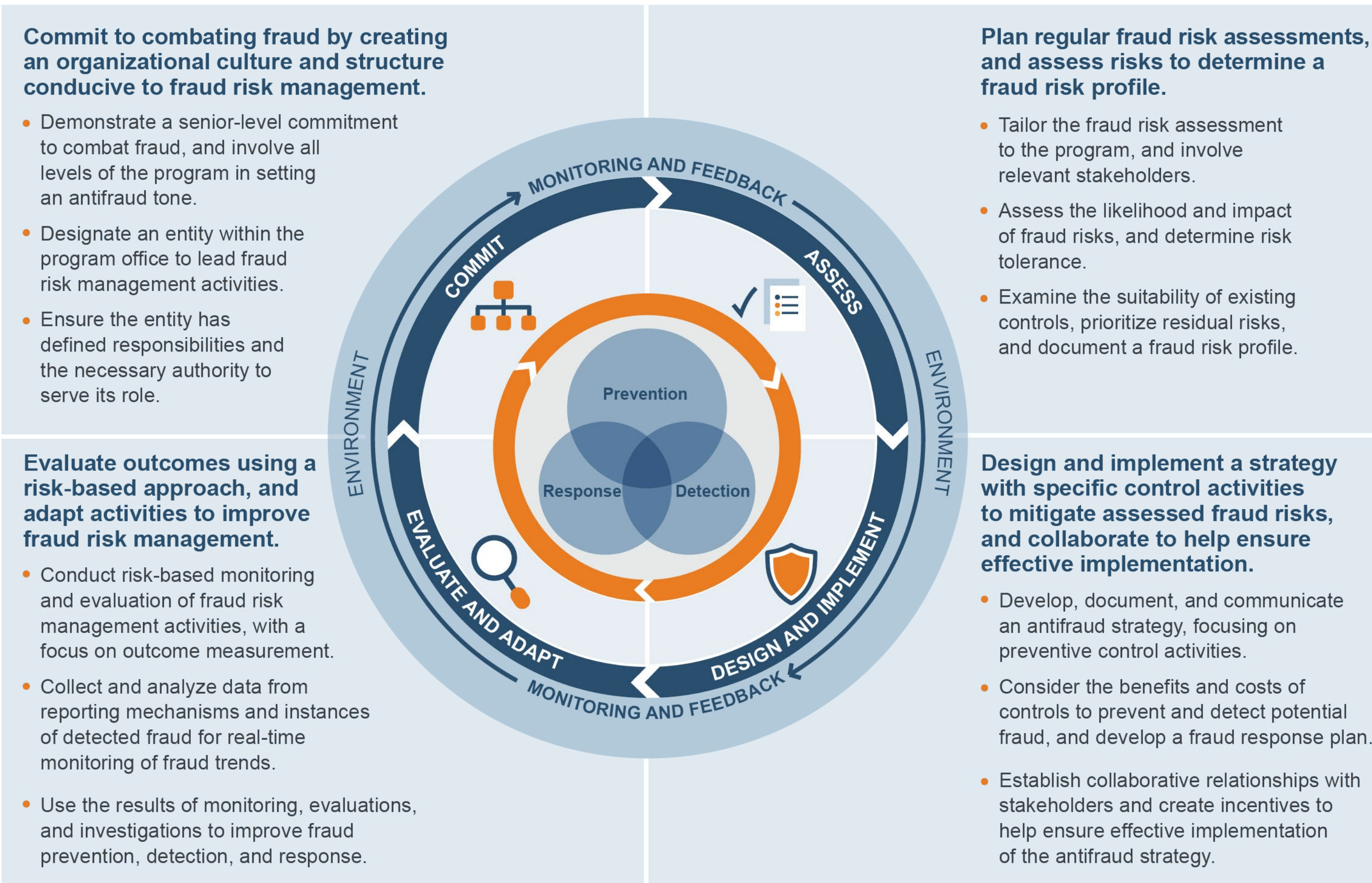
Executive branch agency managers are responsible for managing fraud risks and implementing practices for combating those risks. Federal internal control standards state that as part of an overall risk assessment, management should consider the potential for fraud when identifying, analyzing, and responding to risks.[11] To help federal program managers combat fraud and preserve integrity in government agencies and programs, in 2015 GAO published the Fraud Risk Framework, which provides a comprehensive set of leading practices for agency managers to develop or enhance efforts to combat fraud in a strategic, risk-based manner.[12] (See fig. 2.) The Fraud Risk Framework encompasses control activities to prevent, detect, and respond to fraud, with an emphasis on prevention, as well as structures and environmental factors that influence or help managers achieve their objective to mitigate fraud risks. In addition, the Framework highlights the importance of monitoring and incorporating feedback, which are ongoing practices that apply to all four of the components of the framework.

[10]While the FAR sets forth regulatory requirements for the acquisition process, the DEAR supplements it by providing additional internal agency regulations, including designations and delegations of authority, assignments of responsibilities, work-flow procedures, and internal reporting requirements. 48 C.F.R. § 1.301(a)(2).

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

[12]GAO-15-593SP.

Figure 2: The Four Components of the Fraud Risk Management Framework and Selected Leading Practices



Source: GAO. | GAO-21-44

The Fraud Reduction and Data Analytics Act of 2015, enacted in June 2016, required the Office of Management and Budget (OMB) to establish guidelines for federal agencies to create controls to identify and assess fraud risks and to design and implement antifraud control activities. In its Circular A-123 guidelines, OMB has directed agencies to adhere to the Fraud Risk Framework's leading practices as part of their efforts to effectively design, implement, and operate an internal control system that addresses fraud risks.[13] Although the Fraud Reduction and Data Analytics Act of 2015 was repealed in March 2020, the Payment Integrity

[13]Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control*, OMB Circular A-123 (Washington, D.C.: July 15, 2016).

Information Act of 2019 requires these guidelines to remain in effect, subject to modification by OMB as necessary, and in consultation with GAO.[14] Further, OMB guidance requires agencies to report annually on improper payments made as a result of confirmed fraud.[15]

Documents Prepared as Part of DOE's Broader Risk Assessment Process

As part of its internal control activities, DOE conducts annual assessments of financial and nonfinancial risk based on the requirements of OMB Circular A-123. DOE requires all reporting entities—typically DOE's headquarters offices, field and site offices, and M&O contractors—to annually assess risk. (See app. II for a list of reporting entities.) Fraud risks are considered as part of these efforts but are not the primary focus of these broader risk assessments. The results of these broader risk assessments are summarized in three key documents—(1) risk profiles, (2) financial management assessments, and (3) entity assessments.[16]

- Risk Profiles: OMB Circular A-123 requires each agency to prepare an annual prioritized and ranked risk profile. OCFO manages the annual development of the overall DOE risk profile in a bottom-up process, using a risk profile template completed by each reporting entity (see fig. 3).[17] Specifically, M&O contractors are to identify their most significant risks and provide a risk profile to the cognizant field office. Field offices then use input from the M&O contractors to identify their most significant risks and provide a risk profile to the cognizant program office. Program offices use input from the field offices and M&O contractors to identify their most significant risks and provide a risk profile to the cognizant Under Secretary. The OCFO consolidates information from the Under Secretaries and other headquarters offices that do not report to an Under Secretary into a

[14]Pub. L. No. 116-117, § 2(a), 134 Stat. 113, 131 - 132 (2020), codified at 31 U.S.C. § 3357.

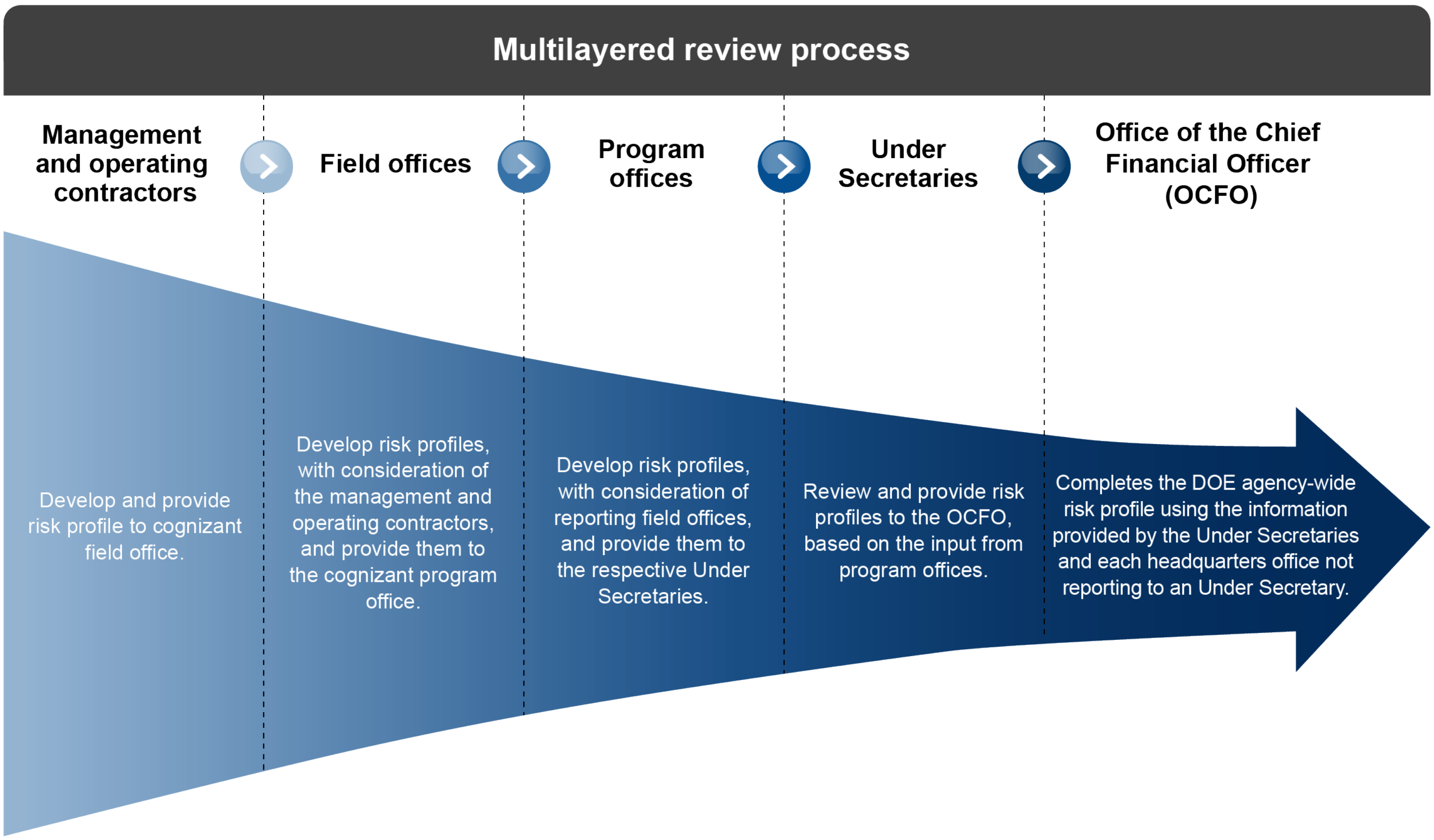
[15]OMB M-18-20 states that transactions that management determines to be anomalous or indicative of potential fraud and subsequently referred to the agency's Inspector General or the Department of Justice should not be identified or otherwise categorized as fraud—one type of improper payment—until the appropriate judicial or adjudicative process makes that determination.

[16]Reporting entities may perform additional tasks to identify and assess fraud risks as part of their internal control process. Reporting entities can identify fraud risk in other places, such as the entity risk register or audit reviews; however, this information is not provided as part of the risk assessment process, including to the OCFO.

[17]Throughout this report, we refer to the M&O contractors, field offices, and offices within headquarters that are required to produce risk profiles as "reporting entities."

single DOE risk profile that functions as DOE's annual agency-wide assessment of risk.

Figure 3: The Department of Energy's (DOE) Risk Profile Development and Review Process



Source: GAO analysis of DOE information. | GAO-21-44

- Financial Management Assessment (FMA): The FMA is completed by each reporting entity annually. The FMA documents the evaluation of relevant financial business processes, subprocesses, and risks facing each reporting entity as well as the key controls for each process that are relied upon to mitigate the risks. Controls that mitigate a financial risk on a risk profile must be tested and documented in the FMA.
- Entity Assessment (EA): The EA is also completed by each reporting entity annually. The EA is a structured self-evaluation with the goal of providing reasonable assurance that internal control systems are designed and implemented and operating effectively and to verify that risks are mitigated and validate that the agency's mission objectives are accomplished effectively, efficiently, and in compliance with laws

and regulations. The EA is where controls that mitigate a nonfinancial risk on a risk profile must be tested and documented.[18]

Various Types of Contracting Fraud Schemes Have Been Identified at DOE, Resulting in Financial and Nonfinancial Impacts

We identified contracting fraud schemes that occurred at DOE that fell into nine categories: bid-rigging, billing schemes, conflicts of interest, contract progress schemes, kickbacks and gratuities, misrepresentation of eligibility, payroll schemes, product quality, and theft. The cases we identified through our review of Department of Justice media releases and DOE OIG reports represent a portion of contracting fraud at DOE, as not all fraud schemes are identified, investigated, or adjudicated as fraud, and some DOE fraud cases may not have been made publicly available in the sources we reviewed.[19] Also, the process for pursuing a fraud case can be lengthy and, thus, some of the schemes we identified occurred before 2013, but were identified in our sources during the 2013 through 2019 timeframe that our review covered.

Table 1 provides descriptions and examples for these categories of fraud schemes. In some cases, the DOE contracting fraud cases that we reviewed involved more than one type of scheme. Although many of the examples in table 1 involved non-M&O contractors, these schemes could apply to M&O contractors and subcontractors as well. Further, while some types of fraud schemes were less common than others in the publicly available case information that we reviewed, they represent inherent fraud risks associated with contracting.[20]

[18]For example, one reporting entity identified contractor safety policies and standards as potentially inadequate and ineffective, which could lead to safety issues or misrepresentation of the quality of work. The reporting entity noted that they have on-site field monitoring and approved quality assurance programs to help reduce that risk.

[19]The contracting fraud schemes identified through our review of fraud cases in media releases and DOE OIG semiannual reports to Congress represent only those cases that had been investigated and charged as fraud in some manner (e.g., indictment, plea, settlement, conviction).

[20]According to federal internal control standards, inherent risk is the risk to an entity in the absence of management's response to the risk (see GAO-14-704G, 7.03).

Table 1: Types and Examples of Reported Contracting Fraud Schemes That Have Occurred at the Department of Energy

Category	Description of fraud scheme	Number of cases identified	Examples
Bid-rigging	Agency officials or contractors bidding on a contract conspire to influence the purchase of goods or services to avoid competitive bidding controls. Bid-rigging typically involves contractors agreeing to artificially increase the prices of goods or services offered in bids to the government or bidding in such a way to ensure a specific contractor wins the contract.	2	In July 2013, firms conspired to submit noncompetitive bids on a construction contract for the Lawrence Berkeley National Laboratory in California to ensure that a specific developer was awarded the contract. Several contractors submitted sham bids to ensure that the $5.7 million bid from the developer would win the contract.
Billing schemes	Contractors obtaining payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.	26	An employee of a subcontractor at the Savannah River site in South Carolina created fraudulent invoices for payment of what appeared to be goods needed, but no goods were ever received. This scheme took place over several years starting in 2009, and resulted in a loss of over $6 million.
Conflicts of interest	Agency officials or government contractors inappropriately awarding business to vendors in which they have an unreported direct or indirect interest, potentially resulting in higher contract costs or purchases of goods or services not needed. Conflicts of interest can arise at the individual or organizational level. Organizational conflict of interest can occur when a contractor has a preexisting relationship with a potential subcontractor or vendor that results in inappropriate award of subcontracts at higher cost to the government.	7	According to the DOE Office of Inspector General (OIG), a contractor employee at Lawrence Livermore National Laboratory in California purchased equipment from a company in which the employee had a financial interest. DOE was reimbursed over $200,000 from the contractor’s management fee as a result of the fraud investigation.
Contract progress schemes	Contractors inappropriately obtaining payments by purposefully misrepresenting the extent of project completion.	2	According to the DOE OIG, an investigation determined that the management and operating contractor at the Savannah River site inaccurately represented work completion percentages. The contractor agreed to pay $3 million to the National Nuclear Security Administration in the settlement.

Category	Description of fraud scheme	Number of cases identified	Examples
Kickbacks and gratuities	Contractors making undisclosed payments to agency officials or other government contractors, or giving something of value to reward a business decision.	6	According to the DOE OIG, an investigation determined that a Hanford site contractor employee received at least $41,000 in kickback payments to influence, assist, and reward the employee for securing a $232 million subcontract to an affiliate company. The subcontract was executed in 2011. The DOE OIG reported that the Department of Justice entered into a $124,440 settlement agreement with the employee.
Misrepresentation of eligibility	Contractors purposefully reporting incorrect information in a bid proposal to falsely claim eligibility to perform the work, such as status as a small business.	3	In 2010 and 2012, a DOE contractor at the Hanford site in Washington claimed that it was subcontracting to small, disadvantaged businesses when these businesses were allegedly being used as a pass-through, and the work was actually performed by a different subcontractor that was not a small, disadvantaged business. The awards were for multi-million-dollar subcontracts, and the government recovered over $5.5 million from the defendants. As a result of this type of scheme, legitimate small, disadvantaged businesses may not have had the opportunity to fairly compete for and perform work on subcontracts.
Payroll schemes	Contractors obtaining payment through submission of false claims for compensation, such as misrepresenting employee labor in order to charge for more work hours and increase profit.	15	Between 1999 and 2008, a contractor at the Hanford site in Washington engaged in years of widespread time card fraud, wherein the contractor condoned workers overstating hours worked and submitted inflated claims for compensation. The contractor agreed to pay $18.5 million in settlement to relieve its criminal and civil liability.

Category	Description of fraud scheme	Number of cases identified	Examples
Product quality	Contractors purposefully conducting work in a way that results in the delivery of goods of a lesser quality than required by the contract.	10	According to the DOE OIG, an investigation determined that DOE subcontractor employees at the Portsmouth site in Ohio altered testing records of portable radiation detection devices—wearable devices that can detect elevated levels of radiation—so they appeared to be calibrated when, in fact, they were not. Multiple prime contractor and subcontractor employees were terminated as a result of the investigation.
Theft	Contractors stealing or misappropriating government resources, such as cash or other assets.	27	According to the DOE OIG, an investigation determined that a former contractor employee stole approximately $58,000 worth of optical devices, toner cartridges, and computer accessories from Lawrence Livermore National Laboratory and subsequently sold them online. As a result, the former contractor employee was debarred from government contracting for a period of 3 years, was ordered to pay restitution to DOE, and was permanently banned from Lawrence Livermore National Laboratory after pleading guilty.

Sources: Department of Energy (DOE) Office of Inspector General (OIG) audit reports and semi-annual reports to Congress, and DOE OIG and Department of Justice media releases from calendar year 2013 through 2019. | GAO-21-44

Notes: The cases we reviewed include incidents and reports of contracting fraud at DOE from publicly available sources. Some of these incidents resulted in official adjudication as fraud through a settlement, plea, or conviction. However, others were settled without an admission of guilt by the contractor. We included all these cases in our review because they all represent contractor fraud risk at DOE. Additionally, the process for pursuing a fraud case can be lengthy and, thus, some of the schemes we identified occurred before 2013 but were identified in our sources during the 2013 through 2019 timeframe that our review covered.

Contracting fraud schemes impact DOE financially through the loss of appropriated funds, which means those funds are not available for their intended purposes. DOE reports some information on the financial impacts of fraud, including contracting fraud, as part of annual financial reporting requirements for improper payments.[21] For example, in the most recent data available at the time of our review, DOE reported that it had identified about $6.66 million in improper payments related to confirmed

[21]DOE reports the payments in the year they were identified and does not provide information on the year that the payments were made. Also, DOE reports its improper payments 1 year in arrears, so, for example, DOE reported improper payments identified in fiscal year 2018 in its fiscal year 2019 AFR.

fraud in fiscal year 2018 and about $14.83 million in fiscal year 2019, as shown in table 2. While the financial impact of contracting fraud is not reported separately from other fraud in the AFR, agency sources indicate that contracting fraud cases can be a significant portion of fraud-related improper payments.

Table 2: Improper Payments From Confirmed Fraud Identified in Fiscal Years 2018 and 2019 and Reported in the Department of Energy's Agency Financial Reports

Dollars in millions

	Reporting year	
	Fiscal year 2018	**Fiscal year 2019**
Confirmed fraud	6.66	14.83

Source: Department of Energy (DOE) agency financial reports. | GAO-21-44

Note: DOE reports fraud-related improper payments in the year that they are identified, not the year that they occurred. Additionally, DOE reports its improper payments 1 year in arrears; for example, DOE reported improper payments identified in fiscal year 2018 in its fiscal year 2019 Agency Financial Report. The data above list the improper payments in the year they were identified, rather than the year the Agency Financial Report was issued. DOE does not report fraud-related improper payments to contractors separately from improper payments associated with other fraud cases, such as those involving grantees or federal employees.

The amounts that DOE reports in fraud-related improper payments in its AFR do not represent the total financial impact of contracting fraud at the agency. Specifically:

- **Agencies report information if the case is adjudicated as fraud.** In accordance with Appendix C of OMB Circular A-123, payments are to be categorized as fraud after the appropriate judicial or adjudicative process makes the determination of fraud. We found in June 2020 that DOE has made improper payments with characteristics of fraud that were not designated as such because they were not adjudicated as fraud.[22] For example, DOE incurred a loss of $500 million from a loan guarantee in which the DOE OIG found the company made false claims and omissions in its application and eventually declared bankruptcy. This amount was not reported as fraud, in accordance with OMB guidance, because the payment was not determined to be related to fraud through a court case or other legal process. Additionally, in August 2020, two contractors agreed to pay about $58 million in a settlement regarding overbilling at the Hanford site.

[22]GAO, *Improper Payments: Improvements Needed to Ensure Reliability and Accuracy in DOE's Risk Assessments and Reporting,* GAO-20-442 (Washington, D.C.: June 17, 2020).

Because the agreement did not include a determination of fraud, DOE is not required to report this amount as confirmed fraud in its AFR.[23]

- **DOE reports settlement and restitution amounts.** DOE policy requires reporting the settlement or restitution amounts as improper payments related to fraud, as opposed to the total financial impact of the fraud. As a result, improper payments related to fraud may not represent the total financial impacts of fraud. For example, a former contractor employee was ordered to pay $40,000 in restitution after pleading guilty to one count of theft of government property. The investigation determined that the former contractor employee stole at least 42,000 pounds of copper from Lawrence Livermore National Laboratory and sold it to a scrap metal company in exchange for nearly $118,000 over a 3-year period. In accordance with agency policy, DOE would report the restitution amount—$40,000—as an improper payment, which is about one-third of the total financial impact of the fraud. Furthermore, the reported amounts would not capture indirect costs to the agency associated with fraud, such as those associated with schedule delays, lost productivity, and the agency resources used to replace the products or services.
- **Difficulty in detecting fraud.** Due to the difficulty in detecting fraud, agencies—including DOE—incur financial losses related to fraud that are never identified. Some fraud schemes are never uncovered, and others do not result in criminal charges or other legal action and, therefore, the financial impact of these cases are not included in DOE's reporting on improper payments related to fraud. We have previously reported that challenges in determining the amount of undetected fraud can make it difficult to create accurate fraud estimates.[24] This would include determining the total financial impact of fraud.

In addition to the financial impacts described above, our review of fraud cases and DOE OIG reports identified nonfinancial impacts related to

[23]Certain settlement amounts related to cases with characteristics of contract fraud may be reported as improper payments in the AFR, as DOE reports settlements as a result of litigation. For example, DOE reported $60.6 million of improper payments identified through a fiscal year 2017 settlement with a contractor that was related to potential fraud, and this was reported as a settlement as a result of litigation. DOE reported improper payments related to settlements as a result of litigation totaling $68.67 million in fiscal year 2017 and $5.02 million in fiscal year 2018. While settlements as a result of litigation may include improper payments related to cases with characteristics of fraud, it may also include improper payment amounts from settlements that are not related to fraud.

[24]GAO-15-593SP.

contracting fraud at DOE. For example, fraud can affect government outcomes, agency reputation, the broader industry of the contractor, the environment, and communities and individuals. The International Public Sector Fraud Forum, an organization of countries that shares leading practices in fraud management, has identified nonfinancial impacts of fraud that are pertinent to DOE contract fraud risks, including the following:[25]

- **Government outcomes impacts:** Fraud against public bodies compromises the government's ability to deliver services and achieve intended outcomes. Money and resources are diverted away from the intended targets, and the services delivered can be substandard or unsafe. This can lead to program failure. For example, a contractor allegedly submitted falsified testing data for parts supplied to the Bonneville Power Administration, located in the Pacific Northwest. An investigation determined the company used fraudulent data in certifying that the tests had taken place and manipulated test results that would pass onsite witness inspections. From 2000 to 2018, the company failed to conduct required design and production tests before the parts were shipped to the Bonneville Power Administration but made false representations that the required testing had been completed. As a result, the parts may have been substandard and failed to meet requirements.
- **Reputational impact:** Fraud against government programs can result in an erosion of trust in government and industries and lead to a loss of international and economic reputation of countries. For example, a DOE employee accepted cash and other benefits from various companies while providing them access to federal funding and contracts between 2004 and 2014. The DOE official, a program manager at a DOE facility in Germantown, Maryland, accepted at least $469,000 in kickbacks. This type of fraudulent behavior may affect DOE's reputation by creating doubt about whether DOE employees at other sites may be doing something similar.
- **Industry impact:** Fraud against public bodies can result in distorted markets where fraudsters obtain a competitive advantage and drive legitimate business out. For example, in its April 2019-September

[25]International Public Sector Fraud Forum, *Guide to Understanding the Total Impact of Fraud* (February 2020). The International Public Sector Fraud Forum consists of representatives from organizations in the governments of Australia, Canada, New Zealand, the United Kingdom, and the United States. The collective aim of the Forum is to come together to share best and leading practice in fraud management and control across public borders.

2019 semiannual report, the DOE OIG reported that a contractor established fictitious small businesses and sought to obtain small business set-aside contracts, valued in excess of $100 million, from a broad range of federal agencies, including DOE. Contracts awarded to companies that are not eligible for such awards mean that there are fewer contracts available for legitimate small businesses, and these small businesses then have fewer opportunities to benefit from the programs aimed at providing a more level playing field in government contracting. Furthermore, this may result in DOE overstating the extent that it achieved small business contracting goals.

- **Environmental impact:** Fraud may also have an impact on the environment. Environmental damage can be immediate and direct, such as increasing levels of pollution. These impacts can be medium to long term or, in some cases irreversible. For example, a DOE prime contractor at the Paducah Gaseous Diffusion Plant in McCracken County, Kentucky, allegedly improperly dumped contaminated waste into storage areas and knowingly hid this from DOE and environmental regulators. A settlement was reached between DOE and the contractor in 2016 on a lawsuit that was originally filed in 1999.
- **Human impact:** While the direct financial loss is borne by public bodies, behind every story of fraud, there are real individuals, families and communities whose lives have been impacted. These human impacts can often occur through the provision of substandard services or products that may jeopardize the safety of workers and communities. For example, in 2016, several DOE contractors agreed to pay $125 million to resolve allegations that they charged DOE for deficient nuclear quality materials, services, and testing that was provided at the Waste Treatment Plant at DOE's Hanford site near Richland, Washington. The contractors were paid to design and build the Waste Treatment Plant, a facility to treat dangerous radioactive wastes that are currently stored at the site. In this case, the contractors may have put the safety of citizens at risk by failing to meet important nuclear quality standards required by the contract.

DOE Has Taken Steps to Combat and Assess Its Contracting Fraud Risks but Has Not Assessed the Full Range of Contracting Fraud Risks the Agency Faces

DOE has taken some steps and is planning others that demonstrate a commitment to combat fraud and assess its contracting fraud risks, consistent with the leading practices in the Fraud Risk Framework. However, we found that DOE has not assessed the full range of contracting fraud risks it faces. Specifically, we found that DOE has not developed a comprehensive assessment of its fraud risks and that reporting entities did not consistently obtain information on fraud risks of the contractors they oversee when developing their risk profiles. Without conducting a comprehensive assessment of its fraud risks, DOE will remain vulnerable to these fraud risks and could be missing important trends in fraud risks across its programs.

DOE Has Taken Steps That Demonstrate a Commitment to Combating Contracting Fraud Risks and Has Planned Additional Steps

DOE has taken steps that demonstrate its commitment to combating contracting fraud risks, consistent with leading practices in the Fraud Risk Framework, and has planned additional steps related to this component of the Framework. According to GAO's Fraud Risk Framework, managers who effectively manage fraud risks demonstrate a senior-level commitment to integrity and combating fraud.[26] Various actions can help managers meet these leading practices. For example, managers can establish a code of conduct that sets expectations for ethical behavior to demonstrate a senior-level commitment.

DOE has taken steps to demonstrate a senior-level commitment to integrity and combating fraud. It has done so, for example, by requiring contractors to establish a code of business ethics and conduct for their employees and to display fraud hotline posters at contract work sites, a practice that is designed to require contractors to participate in fraud prevention and detection efforts.[27] DOE includes these requirements in contract clauses with its contractors, and DOE contractors in turn include these requirements in contract clauses with their subcontractors. DOE has similar requirements for its own employees that work at headquarters, field, and site offices.

[26] GAO-15-593SP.

[27] In addition to these activities, part 3 of the FAR prescribes policies and procedures for avoiding improper business practices and personal conflicts of interest and for dealing with their apparent or actual occurrence. See 48 C.F.R. § 3.1004. Specific required language can be found at 48 C.F.R. §§ 52.203-13 and 52.203-14.

Designating an entity to design and oversee fraud risk management activities is also a leading practice for fraud risk management. In March 2017, we found that DOE had not created a structure with a dedicated entity to design and oversee fraud risk management activities, and we recommended that it do so.[28] During this review, DOE indicated that, since March 2017, OCFO has taken on the responsibilities of the dedicated antifraud entity within DOE. As the dedicated entity, OCFO coordinates the annual agency-wide risk assessment, issues annual internal controls guidance, and offers annual training to DOE employees and contractors on fraud awareness and on how to assess risk for completing the annual risk profile.[29]

In December 2020, DOE provided us with a finalized charter indicating that it expanded the responsibilities of the agency's Department Internal Control and Assessment Review Council to include performing duties as the Senior Risk Management Council to oversee the fraud risk management process and take on other roles of the designated entity, with support from OCFO. Further, DOE plans for these entities to collaborate with other entities within DOE to serve as the designated entities to lead fraud risk management activities for the department. While DOE has taken steps toward meeting the leading practices for creating a structure with a dedicated entity to design and oversee fraud risk management activities, as we recommended in March 2017, this new entity is still in the early phases of carrying out its new role. Thus, we will continue to monitor DOE's progress in this area.

DOE Has Taken Steps to Assess Some of its Fraud Risks but Has Not Assessed the Full Range of Contracting Fraud Risks It Faces

DOE has taken steps to assess some of its fraud risks, consistent with the Fraud Risk Framework; however, DOE has not assessed the full range of its contracting fraud risks. The Fraud Risk Framework states that effective fraud risk managers: (1) plan regular fraud risk assessments that are tailored to the program, and (2) identify and assess risks to determine the program's fraud risk profile. A fraud risk profile is an essential piece of an overall antifraud strategy that informs the design and implementation of specific fraud control activities.

DOE has taken some steps to conduct risk assessments that include a consideration of fraud risks. As previously discussed, DOE conducts an annual agency-wide assessment of risk, including top fraud risks, and

[28]GAO-17-235.

[29]According to agency officials, beginning in fiscal year 2021, DOE will conduct the fraud risk awareness training on a semiannual basis.

documents an agency-wide risk profile that ranks and prioritizes risks based on their likelihood and impact. Reporting entities, including DOE field and site offices and M&O contractors, identify and assess risks by completing their own risk profiles. The OCFO then compiles the reporting entities' risk profiles to develop the agency-wide risk profile.

In addition, DOE takes steps to identify and assess risks by requiring reporting entities to evaluate their financial business processes by using the FMA and internal control systems using the EA, to ensure that these processes and controls are operating effectively.[30]

While the FMA and EA help reporting entities evaluate whether financial business processes and internal control systems are operating effectively, the FMA and EA do not constitute fraud risk assessments or fraud risk profiles that meet leading practices. Specifically, the FMA and EA may help reporting entities assess the likelihood and impact of fraud risks, but the FMA and EA do not meet other leading practices for assessing fraud risk and determining a fraud risk profile. For example, the FMA and EA do not document DOE's fraud risk tolerance or examine the extent to which existing control activities mitigate the likelihood and impact of inherent risks and whether the remaining risks exceed managers' tolerance.[31]

During this review, officials from DOE's OCFO clarified that DOE intends to meet these leading practices through an agency-wide fraud risk assessment and risk profile that it plans to develop during fiscal year 2021. Additionally, OCFO officials informed us that they intend to address leading practices at the agency level and not at the reporting entity level. This decision is consistent with GAO's Fraud Risk Framework, which

[30]The FMA documents the evaluation of relevant financial business processes, subprocesses, and risk facing each reporting entity, including key controls for each process that are relied upon to mitigate the risks. Controls that mitigate a financial risk on a risk profile must be tested and documented in the FMA. The EA is a structured self-evaluation, with the goal of providing reasonable assurance that internal control systems are designed and implemented and operating effectively and to verify that risks are mitigated and to validate that the agency's mission objectives are accomplished effectively, efficiently, and in compliance with laws and regulations. The EA is where controls that mitigate a nonfinancial risk on a risk profile must be tested and documented.

[31]According to federal internal control standards, risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. According to the Fraud Risk Framework, in the context of fraud risk management, if the objective is to mitigate fraud risks—in general, to have a very low level of fraud—the risk tolerance reflects managers' willingness to accept a higher level of fraud risks.

notes that managers decide whether to carry out each aspect of fraud risk management at the program level or agency level.

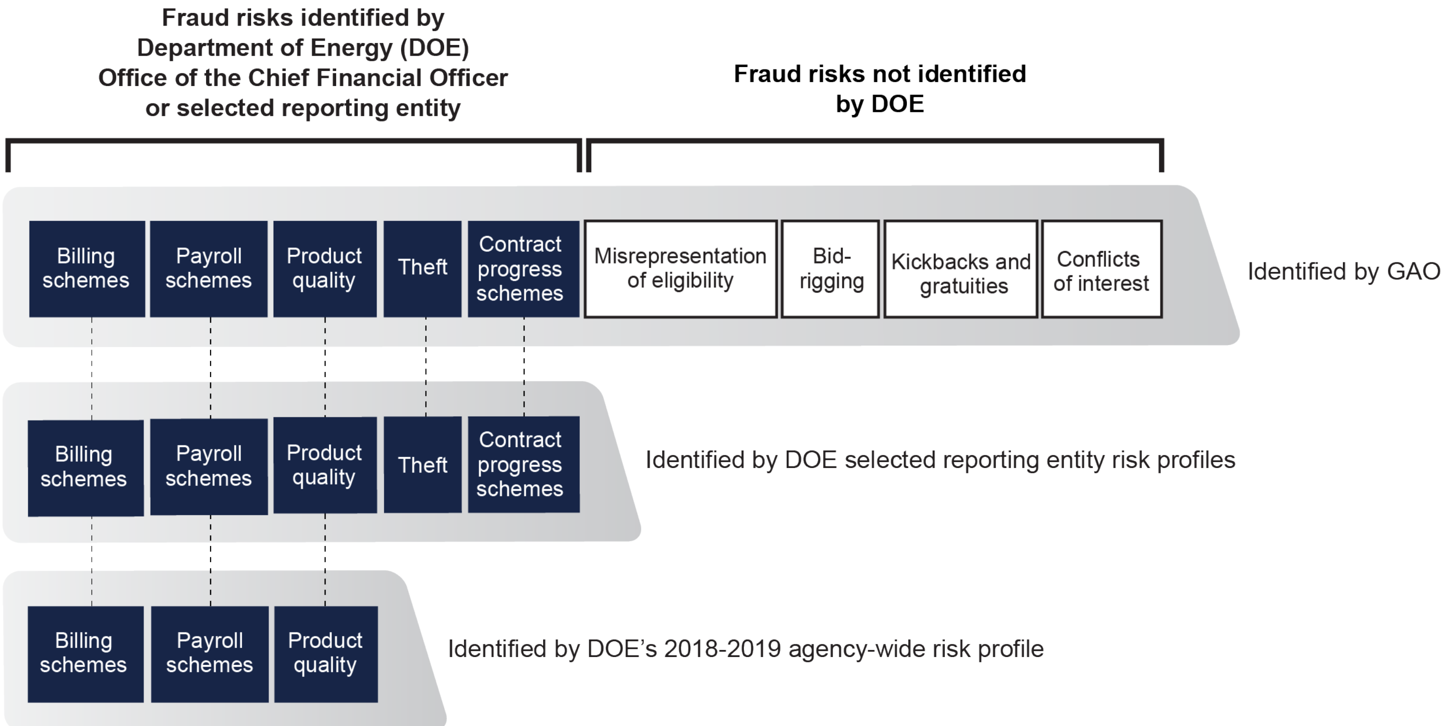
As part of the effort to conduct fraud risk assessment and document a fraud risk profile, the Fraud Risk Framework states that entities that effectively plan fraud risk assessments identify specific tools, methods, and sources for gathering information about fraud risks. As mentioned, DOE's OCFO relies on its agency-wide risk assessment process for gathering information about fraud risks it faces and documenting its agency-wide fraud risk profile. However, we found that this method for gathering information did not capture all fraud risks facing DOE programs because DOE (1) requires reporting entities to provide information on selected financial and nonfinancial fraud risks and (2) does not specify the information that reporting entities are to obtain from non-M&O contractors that they oversee.

DOE Requires Reporting Entities to Provide Information on Selected Financial and Nonfinancial Fraud Risks

DOE's guidance requires reporting entities to identify the top financial and nonfinancial fraud risks in their risk profiles. As a result, DOE does not have visibility over fraud risks that reporting entities do not consider "top risks" and are therefore not included in the reporting entities' risk profiles. An OCFO official acknowledged that the FMA includes assessments of risks at the program level that are not included in the risk profiles. As such, the FMA and the EA may provide an additional source of information on fraud risks facing the agency. OFCO officials told us they consider information from the FMA and EA as part of their agency-wide risk assessment processes, but our analysis shows that these methods did not capture specific incidents of fraud, and their related fraud risks, in DOE's risk assessments and profiles.

Specifically, our analysis of DOE's risk profiles for fiscal years 2018 and 2019 confirms that these risk profiles did not capture all fraud risks facing DOE programs. As discussed previously, our review of publicly available information from the DOE OIG and the Department of Justice on incidents and reports of contracting fraud at DOE identified nine categories of fraud schemes that have occurred at DOE sites. However, DOE entities identified fraud schemes in five of these nine categories in their risk profiles for fiscal years 2018 and 2019, and DOE's agency-wide risk profiles for those years included three of the nine schemes (see fig. 4).

Figure 4: Fraud Risks Identified in Reporting Entity and DOE Fiscal Year 2018 and 2019 Risk Profiles Compared to Types of Fraud Schemes That Have Occurred at DOE



Source: GAO analysis of DOE information. | GAO-21-44

We also found numerous instances where site-specific fraud schemes had occurred at the sites in our sample, but the associated fraud risks were not included in the reporting entity's risk profile (see fig. 5). For example, we found one reporting entity did not include any fraud risks in its fiscal year 2018 or 2019 risk profiles, yet we identified six types of fraud schemes that occurred at the entity's site through our review of publicly available information from the DOE OIG and the Department of Justice. Similarly, we found another reporting entity that identified fraud risks associated with billing schemes and product quality, while our review identified six additional types of fraud schemes that had occurred at the entity's site that were not captured in the risk profile.

Figure 5: Fraud Risks Included in Selected DOE Reporting Entities' Risk Profiles for Fiscal Years 2018 and 2019 Compared to GAO-Identified Fraud Schemes

		Fraud risks: Bid-rigging	Payroll schemes	Kickbacks and gratuities	Conflicts of interest	Misrepresentation of eligibility	Theft	Product quality	Contract progress schemes	Billing schemes
Reporting entity A	Reporting entity A's risk profile	○	○	○	○	○	○	○	○	○
	Fraud schemes identified by GAO	○	✓	✓	○	✓	○	✓	✓	✓
Reporting entity B	Reporting entity B's risk profile	○	○	○	○	○	○	✓	○	✓
	Fraud schemes identified by GAO	○	✓	✓	✓	✓	✓	✓	✓	✓
Reporting entity C	Reporting entity C's risk profile	○	○	○	○	○	○	✓	○	✓
	Fraud schemes identified by GAO	○	✓	○	○	○	✓	✓	○	✓
Reporting entity D	Reporting entity D's risk profile	○	○	○	○	○	✓	○	○	○
	Fraud schemes identified by GAO	✓	○	○	○	○	✓	○	○	○
Reporting entity E	Reporting entity E's risk profile	○	✓	○	○	○	✓	✓	✓	✓
	Fraud schemes identified by GAO	○	○	○	○	○	✓	○	○	○
Reporting entity F	Reporting entity F's risk profile	○	○	○	○	○	✓	✓	✓	✓
	Fraud schemes identified by GAO	✓	✓	✓	✓	○	✓	✓	○	✓
Reporting entity G	Reporting entity G's risk profile	○	○	○	○	○	✓	○	○	○
	Fraud schemes identified by GAO	○	✓	✓	✓	○	✓	○	○	✓

○ Did not identify fraud risk

✓ Identified fraud risk

Source: GAO analysis of Department of Energy (DOE) information. | GAO-21-44

DOE officials provided us a draft of its plans to expand its risk assessment process to include a focus on fraud risks, but the plan noted its new process would continue to rely on entities reporting top fraud risks. Considering the complex ownership relationships we found between DOE's contractors and subcontractors of its largest contracts in our March 2019 report, with some companies being parties to multiple contracts and subcontractors for other contracts, the fraud risks occurring at one site could also occur at another site.[32] Without expanding its methodology to capture, assess, and document all fraud risks facing its programs—not limited to its top fraud risks—DOE risks remaining vulnerable to these fraud risks. Further, DOE could be missing important trends in lower-level fraud risks that are present at multiple sites.

DOE Does Not Specify the Information That Reporting Entities Are to Obtain from Non-M&O contractors That They Oversee

Based on interviews with selected entities, we found that the reporting entities did not consistently obtain information on the fraud risks for the non-M&O contractors they oversee. Specifically, four of the eight reporting entities in our sample that oversee non-M&O contractors did not obtain fraud risk information from those contractors when completing their risk assessments. The other four reporting entities that oversee contractors obtained some type of fraud risk information—such as a risk assessment—from the non-M&O contractors they oversee.

Reporting entities, which include M&O contractors, did not obtain this information because DOE's internal controls guidance does not specify the information that reporting entities are to obtain from the contractors that they oversee or provide guidance on how reporting entities should assess fraud risks facing the contractors they oversee. OCFO officials acknowledged that the internal control guidance does not direct reporting entities to obtain this information from non-M&Os they oversee. However, OCFO officials told us that they expect reporting entities to assess fraud risks associated with contractors they oversee and leverage information, such as internal audits, to identify fraud risks facing those contractors. Without guidance on the information reporting entities need to obtain on contractor's fraud risks, these entities may not have a clear understanding of how to incorporate these fraud risks into a fraud risk assessment, resulting in assessments that do not cover the full range of fraud schemes that have occurred at the site.

[32]GAO, *Department of Energy Contracting: Actions Needed to Strengthen Subcontract Oversight*, GAO-19-107 (Washington, D.C.: Mar. 12, 2019).

DOE Is Planning to Develop an Antifraud Strategy and Enhance Efforts to Evaluate and Adapt Its Approach to Managing Contracting Fraud Risks

DOE Is Planning to Develop an Antifraud Strategy in Fiscal Year 2022

DOE is planning to develop an antifraud strategy in fiscal year 2022, to include a strategy to address its contracting fraud risks. According to the Fraud Risk Framework, managers who effectively manage fraud risks develop and document an antifraud strategy that describes the program's approach for addressing the prioritized fraud risks identified during the fraud risk assessment. This includes determining how to allocate resources, establishing roles and responsibilities, creating time lines for implementing fraud risk management activities, demonstrating links to the highest internal and external residual fraud risks outlined in the fraud risk profile, and linking antifraud efforts to other risk management activities.

In March 2017, we recommended that DOE implement leading practices for managing the department's risk of fraud, including developing and documenting an antifraud strategy that describes the programs' approaches for addressing the prioritized fraud risks identified during the fraud risk assessment.[33] DOE concurred with this recommendation. In June 2017, DOE told us it considered the recommendation closed, stating the agency's department-wide antifraud strategy was embedded in the DOE internal control program. However, in May 2020, OCFO officials stated that DOE did not have a documented antifraud strategy but were planning to develop one as part of the plans to expand its fraud risk assessment efforts. OCFO officials expect to implement this effort over the next 5 years using a three-phased approach.[34] According to the draft plan we reviewed, OCFO expects to develop an agency-wide risk assessment focused on fraud in the first phase, which officials expect to

[33]GAO-17-235.

[34]According to OFCO officials, progress to the later phases is contingent on meeting conditions in initial phases.

occur in fiscal year 2021. During the second phase, DOE expects to use the new fraud risk assessment to develop an agency-wide antifraud strategy.

In reviewing DOE's draft plan, we found that there is no indication of how the agency will adopt specific leading practices for developing an antifraud strategy. For example, the draft plan does not describe how DOE will use the fraud risk profile to decide how to allocate resources in response to fraud risks, among other leading practices. If implemented, developing and documenting an antifraud strategy in accordance with leading practices, as we recommended in March 2017, would help DOE ensure it is effectively mitigating its risk of fraud. As such, we continue to believe this recommendation from our March 2017 report is valid.

DOE Shares Information to Evaluate and Adapt to Fraud Risks and Is Planning to Enhance Its Efforts through Data Analytics

DOE has taken steps to evaluate and adapt to fraud risks, including those related to contractors, consistent with the leading practices in the Fraud Risk Framework, with additional steps planned over the next 5 years. The Fraud Risk Framework states that sharing information on fraud risks and emerging fraud schemes with entities responsible for control activities can help ensure effective implementation of an antifraud strategy. Further, the Fraud Risk Framework states that managers should adapt fraud risk management activities, such as by using the results of investigations and prosecutions to enhance fraud prevention and detection.

Part of DOE's effort to manage fraud risks includes adapting controls to address emerging fraud risks and sharing information that might help other reporting entities avoid similar risks. DOE officials and contractors we interviewed told us about adaptations they have made to their fraud risk controls and management strategies based on direct impacts of specific fraud cases on their organizations. For example, in response to prior incidents, some DOE field and site offices conducted reviews for labor-related payroll fraud schemes, such as time card fraud. Through these reviews, the offices identified and addressed other such schemes. Additionally, an M&O contractor developed new training and strengthened contract provisions after receiving quality-compromised materials from a vendor. Another M&O contractor strengthened its controls on confirming payment recipient information after attempted fraud that would have resulted in a monetary loss of $300,000 to the contractor had it not been identified.

DOE officials from one site office and contractors also discussed informal coordination tools they use or could use to support their organizations' fraud risk management programs. Specifically, DOE; NNSA, including six

NNSA field offices; and M&O contractors participate in a Fraud Risk Management Framework Working Group, which shares knowledge of fraud at biweekly meetings and is using that knowledge to improve fraud risk controls at the sites. Similarly, representatives from numerous DOE contractors and subcontractors we interviewed told us they are members of industry organizations and share information on impacts of fraud risks on their industries through these organizations.

In March 2017, we found that DOE had not designed and implemented some control activities, like data analytics, that could help provide assurance that managers and employees are aware of potential fraud schemes, can better detect potential fraud, and can monitor large amounts of data more efficiently.[35] We recommended that DOE implement such control activities. According to its draft plan, DOE is planning to use data analytics across the agency to help monitor fraud risks. According to the draft planning document we reviewed, DOE plans to survey organizations about their current use of data analytics and plans widespread use of data analytics beginning in fiscal year 2022. We continue to believe the use of data analytics is important in detecting potential fraud and will continue to monitor DOE's implementation of our prior recommendation.

Conclusions

DOE spends billions of dollars on contracts every year. Due to the inherent difficulties in detecting fraud, it is particularly important for DOE to implement leading practices that will help DOE to assess and manage its fraud risks. In response to the recommendations in our March 2017 report, DOE has taken some steps to implement leading practices that would help DOE to organize and focus its resources to better mitigate the likelihood and impact of fraud. However, DOE has not fully implemented our prior recommendations, and we identified some additional steps DOE could take to more fully implement leading practices in managing its fraud risks.

Since our March 2017 report, DOE expanded a senior-level group to help oversee the department's fraud risk management activities. DOE recently finalized documentation expanding the responsibilities of this group. Since this new group is in the early phases of carrying out these responsibilities, we will continue to monitor DOE's progress in this area. Similarly, DOE plans to develop an antifraud strategy—consistent with our March 2017 recommendation—in fiscal year 2022. Additionally, DOE

[35] GAO-17-235.

plans to expand its use of data analytics over the next several fiscal years, as we recommended. We continue to believe that these are important steps in implementing the Fraud Risk Framework and will continue to monitor DOE's progress in these areas.

DOE has taken steps to assess its fraud risks though various efforts, including developing risk profiles and its FMA and EA assessments, and is planning to expand its current risk assessment efforts in fiscal year 2021 to include an additional assessment focused on fraud risks. However, these assessments may not capture all fraud risks because DOE plans to continue its current methodology of requiring reporting entities to report only their top fraud risks and does not specify the information that reporting entities are supposed to gather from certain contractors that they oversee. Without expanding its methodology to capture, assess, and document all fraud risks facing its programs—not limited to its top fraud risks—DOE risks remaining vulnerable to these fraud risks. Further, without guidance on the information reporting entities need to obtain on non-M&O contractors' fraud risks, these entities may not have a clear understanding of how to incorporate this information in their risk assessments, resulting in assessments that do not cover the full range of fraud schemes that have occurred.

Recommendations for Executive Action

We are making the following two recommendations to DOE:

The Office of the Chief Financial Officer should expand its methodology for developing its agency-wide fraud risk assessment to ensure that all inherent fraud risks—not limited to top fraud risks—facing DOE programs are fully assessed and documented in accordance with leading practices. (Recommendation 1)

The Office of the Chief Financial Officer should update its internal control guidance to clarify the information that reporting entities should obtain to assess the fraud risks for non-M&O contractors they oversee. (Recommendation 2)

Agency Comments and Our Evaluation

We provided a draft of this report to DOE for review and comment and incorporated comments as appropriate. In the agency's comments, reproduced in appendix III, DOE agreed with both of our recommendations.

In its written response, DOE stated that it considers its actions to implement our first recommendation, that the Office of the Chief Financial Officer expand its methodology for developing its agency-wide fraud risk assessment to ensure all inherent fraud risks are assessed, to be complete. As part of its response, DOE stated that its Internal Control Evaluations Guidance requires that every risk identified in a reporting entity's risk profile be assessed to determine if there is a risk of fraud. We acknowledge that DOE's guidance requires every risk identified in a reporting entity's risk profile to be assessed to determine if there is a risk of fraud. However, our analysis showed that DOE's methods for gathering information on the fraud risks it faces did not capture information on the risks associated with actual fraud incidents that occurred at DOE, resulting in an incomplete accounting of fraud risks on DOE's risk profiles. Specifically, our analysis shows that DOE's risk profiles for fiscal years 2018 and 2019 did not capture four of nine fraud schemes that occurred at DOE. For example, we found bid-rigging schemes occurred at DOE that led to an indictment and prosecutions during this time, but the risk of bid-rigging was not included in the reporting entities' risk profiles or DOE's agency-wide risk profiles. Without expanding its methodology to capture those fraud risks that are missing from its risk profile, as we recommend, DOE will continue to have an incomplete assessment of the fraud risks it faces. As such, we continue to believe that DOE needs to take additional action to assess its full range of contracting fraud risks.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Energy, the Administrator of NNSA, and other interested parties. In addition, the report will be 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 Rebecca Shea at (202) 512-6722 or shear@gao.gov; or Allison Bawden at (202) 512-3841 or bawdena@gao.gov. Contact points for our Offices of

Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Sincerely yours,

Rebecca Shea
Director, Forensic Audits and Investigative Service

Allison B. Bawden
Director, Natural Resources and Environment

Appendix I: Objectives, Scope, and Methodology

Our objectives were to examine (1) the types of contracting fraud schemes that have been identified at the Department of Energy (DOE), and the financial and nonfinancial impacts of these schemes; (2) the steps DOE has taken to commit to combating contracting fraud risks, and the extent to which DOE has assessed those risks; and (3) the steps DOE has taken to design and implement an antifraud strategy and to evaluate and adapt its approach to address contracting fraud risks as they are identified.

To address our objectives, we reviewed relevant laws, regulations, and guidance, including the Federal Acquisition Regulation (FAR); the Department of Energy Acquisition Regulation (DEAR); and DOE policies and guidance on internal controls. We also reviewed relevant documentation and interviewed officials from DOE, including the Office of the Chief Financial Officer (OCFO), the Office of Inspector General (OIG), the Office of Environmental Management, the Office of Science, and the National Nuclear Security Administration (NNSA); management and operating (M&O) contractors, non-M&O contractors, and subcontractors; and officials from the DOE field and site offices that oversee these contractors.[1]

To determine the types of contracting fraud schemes that have been identified at DOE and the financial and nonfinancial impacts of those schemes, we obtained publicly available information on incidents and reports of contracting fraud at DOE. Specifically, we obtained information on contracting fraud at DOE by reviewing DOE OIG and Department of Justice media releases, DOE OIG audit reports, and DOE OIG semiannual reports to Congress. We reviewed all DOE OIG and Department of Justice media releases for calendar years 2013 through 2019 to identify instances of DOE contract fraud because it was the most recent data available at the time of our review. The process for pursuing a fraud case can be lengthy and, thus, some of the schemes we identified occurred before 2013 but were identified in our sources during the 2013 through 2019 time frame that our review covered. For our reviews of DOE OIG audit reports and semiannual reports to Congress, our scope covered those reports published in calendar year 2013 to 2019 related to contracting fraud risks that occurred at sites under the oversight of DOE

[1]M&O contracts are agreements under which the government contracts for the operation, maintenance, or support, on its behalf, of a government-owned or government-controlled research, development, special production, or testing establishment wholly or principally devoted to one or more of the major programs of the contracting federal agency.

local offices within the scope of the engagement's semistructured interview selection.[2]

In addition to reviewing DOE contracting fraud cases, we conducted a broader literature review of contracting fraud risks and organized the identified DOE schemes in general categories of contracting fraud risk identified in the literature. Sources include the Association of Government Accountants, Association of Certified Fraud Examiners, and multiple OIGs.[3] We also reviewed DOE's Agency Financial Reports from fiscal years 2018 and 2019 to identify financial impacts of contracting fraud. We reviewed contracting fraud case information identified in media releases and DOE OIG semiannual reports to Congress from fiscal years 2013 through 2019 to identify nonfinancial fraud impacts and the International Public Sector Fraud Forum for additional information on nonfinancial impacts of fraud.[4]

To determine the extent to which DOE has taken steps to commit to combating contracting fraud risks, to assess those risks, to design and implement an antifraud strategy, and to evaluate and adapt its approach, we reviewed DOE guidance and documentation related to fraud risk management. We compared the documentary and testimonial evidence obtained during our review to selected leading practices from GAO's *A Framework for Managing Fraud Risks in Federal Programs*.[5] For this review, we selected leading practices that were most relevant for our review. Specifically, we selected leading practices that aligned with themes that had been identified in previous GAO audits related to fraud

[2]The cases we identified through our review of media releases and DOE OIG reports represent a portion of contracting fraud at DOE, as not all fraud schemes are identified, investigated, or adjudicated as fraud, and some DOE fraud cases may not be made publicly available in the sources we reviewed.

[3]We reviewed documents from the OIGs from the Departments of Defense, Transportation, Health and Human Services, and Housing and Urban Development. These OIGs had publicly available information that related to contracting fraud risks.

[4]International Public Sector Fraud Forum, *Guide to Understanding the Total Impact of Fraud* (February 2020). The International Public Sector Fraud Forum consists of representatives from organizations in the governments of Australia, Canada, New Zealand, the United Kingdom, and the United States. The collective aim of the Forum is to come together to share best and leading practice in fraud management and control across public borders.

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

risk management, as well as themes identified during the course of our interviews.

Additionally, we conducted semistructured interviews with a nonprobability sample of field offices, site offices, contractors, and subcontractors.[6] To select the sample of field offices, site offices, and contractors to interview, we created a list of characteristics for active DOE contracts from fiscal year 2019 based on information provided to us by DOE and information we independently collected through a review of media releases and risk profiles.[7] To ensure we obtained diverse perspectives, we selected contractors and subcontractors with a variety of characteristics in the following categories: contract size, contract type, award type, program office, location, contractors with fraud risks present in media releases, and fraud risks identified by location from DOE's fiscal year 2019 risk assessment.[8] This selection method ensured that our sample covered a range of values across the characteristics, and also ensured that the selections we made had varying criteria combinations.

To focus our scope, we selected contractors working for three DOE program offices—the Office of Science, the Office of Environmental Management, and NNSA—because those offices comprise approximately 75 percent of all DOE obligations.[9] This resulted in 30 contractors selected for semistructured interviews. We then selected the seven field and site offices responsible for overseeing the contractors we selected. In addition, we selected subcontractors that worked for the contractors in the initial selection. To select subcontractors, we requested that the contractors provide us with data on all active subcontracts in fiscal year

[6]Because we used a nonprobability sample, we are not able to generalize the findings from these interviews. However, we were able to use the information from these interviews to develop illustrative examples of fraud risk management from the perspective of the field and site offices, contractors, and subcontractors.

[7]We selected fiscal year 2019 for review because it was the most recent fiscal year for which complete data were available at the start of our review. DOE provided us with a list of all contracts active in fiscal year 2019. To focus the scope of the engagement, we removed the following contract types: cooperative agreements, interagency agreements, grants, blanket purchase agreements, and purchase card orders.

[8]The category "contract type" distinguishes between M&O and non-M&O contractors; the category "award type" distinguishes between different contract vehicles, such as firm fixed price contracts or delivery/task orders; and the "program office" category distinguishes between contracts with the following DOE offices: the Office of Science, the Office of Environmental Management, and NNSA.

[9]To refine the scope of our review, we removed all contracts below $100,000 to focus on higher-value contracts.

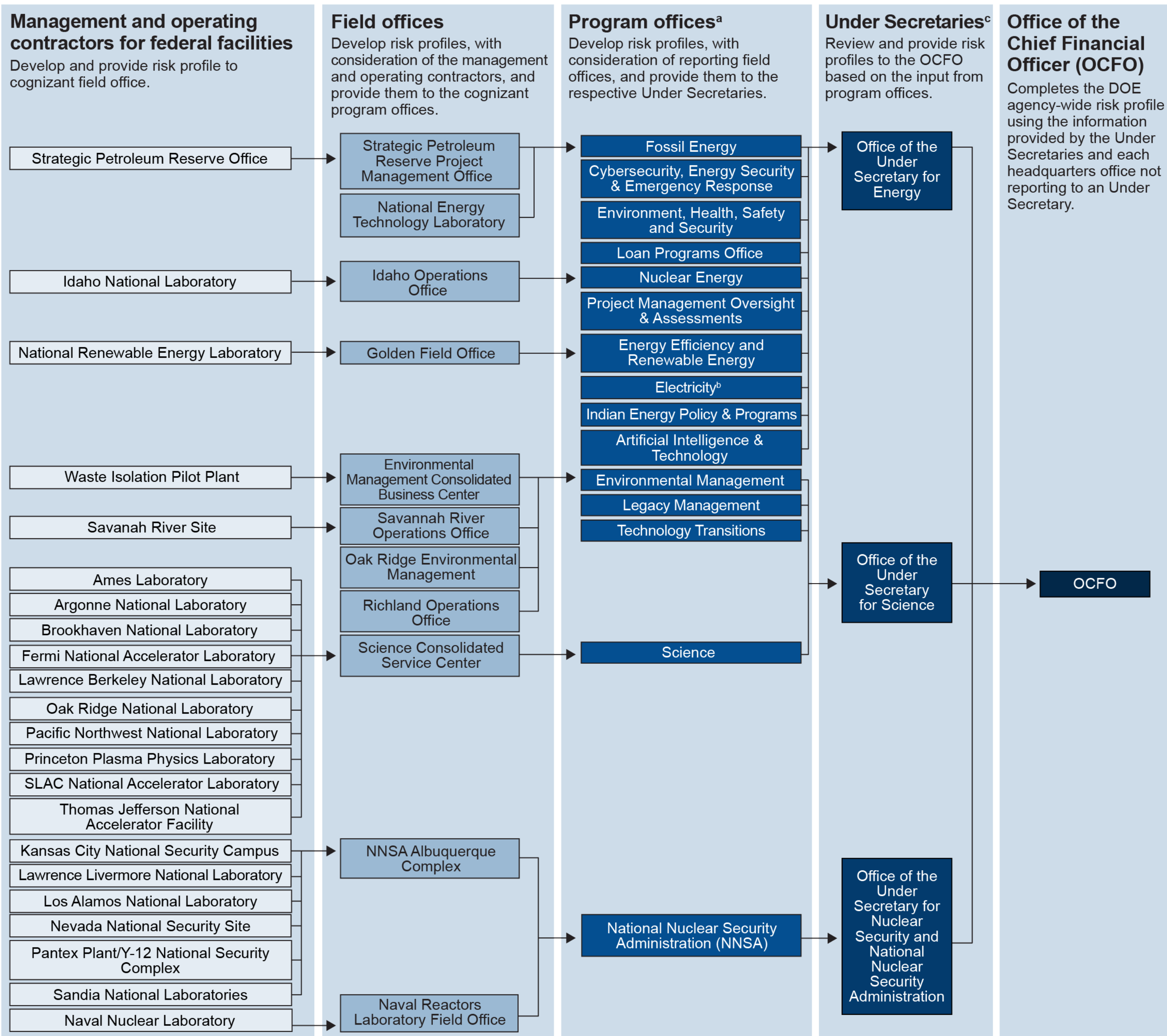
2019, including the award type and the total contract value. We then used this information to select one subcontractor from each contractor with a variety of different award types and contract values. We conducted preliminary interviews to ensure that respondents understood the questions in a consistent way and made changes to the interview questions as appropriate. From January to April 2020 we conducted 42 semistructured interviews with 12 field and site offices, 12 M&O contractors, 10 non-M&O contractors, and eight subcontractors. In addition, we interviewed officials from DOE's OCFO and the DOE OIG.

We conducted this performance audit from April 2019 to January 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Department of Energy Departmental Elements and Reporting Organizations That Participate in the Development of the Risk Profile

As part of its internal control activities, the Department of Energy (DOE) conducts annual assessments of financial and nonfinancial risk based on the requirements of Office of Management and Budget (OMB) Circular A-123. DOE requires all reporting entities—typically DOE's field and site offices and management and operating (M&O) contractors—to annually assess risk by completing their own risk profiles. DOE's Office of the Chief Financial Officer (OCFO) then compiles the reporting entities' risk profiles to develop a single DOE risk profile that functions as DOE's annual agency-wide assessment of risk. There are 74 entities that participate in this process. Figure 6 shows the review process and the entities that participate in the development of the risk profile.

Figure 6: Reporting Entities That Participate in the Development of the Department of Energy's (DOE) Risk Profile, as of September 2020



Source: GAO analysis of DOE information. | GAO-21-44

[a]The following offices are small headquarters offices that provide risk evaluations to their cognizant organization: Congressional and Intergovernmental Affairs, Economic Impact and Diversity, U.S. Energy Information Administration, Enterprise Assessments, General Counsel, Hearing and Appeals,

Intelligence and Counterintelligence, International Affairs, Public Affairs, and Small and Disadvantaged Business Utilization.

[b]Electricity oversees power marketing administrations. Specifically, the Bonneville Power Administration, Southeastern Power Administration, Southwestern Power Administration, and Western Area Power Administration.

[c]In addition to the headquarters offices under the three Offices of the Under Secretary, the Chief Financial Officer directly receives risk evaluations from the following headquarters offices: Chief Financial Officer, Chief Information Officer, Human Capital Officer, Management, Federal Energy Regulatory Commission, Inspector General, Strategic Planning and Policy, and Advanced Research Projects Agency-Energy.

Appendix III: Comments from the Department of Energy

Department of Energy
Washington, DC 20585

December 8, 2020

Ms. Allison Bawden
Director
Natural Resources and Environment
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Bawden:

This letter provides the U.S. Department of Energy (DOE) management decision on the recommendations contained in the Government Accountability Office's (GAO) draft report titled, "***Department of Energy Contracting: Improvements Needed To Ensure DOE Assesses Its Full Range of Contracting Fraud*** **Risks** ***(GAO-21-44).***"

The draft report contains two recommendations, and DOE concurs with both. DOE's full response to the recommendations is included in the Enclosure and provides detailed responses for each recommendation.

GAO should direct any questions to Lynn Harshman, Director, Internal Control and Fraud Risk Management, Office of Chief Financial Officer, at (301) 903-2556 or Lynn.Harshman@hq.doe.gov.

Sincerely,

R. M. Hendrickson
Deputy Chief Financial Officer

Enclosure

Management Response
GAO Draft Report: Department of Energy Contracting: Improvements Needed to Ensure DOE Assesses its Full Range of Contracting Fraud Risks (GAO-21-44)

Recommendation #1: *The Office of the Chief Financial Officer should expand its methodology for developing its agency-wide fraud risk assessment to ensure all inherent fraud risks-not limited to top fraud risks-facing DOE programs are fully assessed and documented in accordance with leading practices.*

Management Response: Concur

DOE's Internal Control Evaluations Guidance, Appendix A, Risk Profile Template Guidance requires that every risk identified in a reporting organization's risk profile, from top level down to lowest level, be assessed to determine if there is a financial fraud or non-financial fraud effect, or neither. Fraud risks, and related effects to DOE and the reporting organizations, are also reported in detail by each program and functional office for inclusion in the DOE enterprise wide assessment.

Estimated Completion Date: Completed

Recommendation #2: *The Office of the Chief Financial Officer should update its internal control guidance to clarify the information that reporting entities should obtain to assess the fraud risks for non-Management & Operating (M&O) contractors they oversee.*

Management Response: Concur

All of DOE's reporting organizations will be required to include all M&O and integrated non-M&O contractors in the assessment of fraud risks. DOE is updating guidance to include risk assessments for M&O and integrated non-M&O contractors. In FY 2021, the Department is focusing on and emphasizing in Risk Profile training, for cognizant organizations to consider and include integrated non-M&O contractor fraud risks. Effective also in FY 2021, *DOE Internal Control Evaluations Guidance* is requiring integrated non-M&O contractors to provide risk profiles, including the assessment of fraud risks, to DOE responsible organizations.

Estimated Completion Date: October FY 2023

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Rebecca Shea, (202) 512-6722 or shear@gao.gov

Allison B. Bawden, (202) 512-3841 or bawdena@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Hilary Benedict and Jonathon Oldmixon (Assistant Directors), Gloria Proa, Jason Trentacoste, and Ariel Vega (Analysts-in-Charge), and Celina Davidson, Caitlyn Leiter-Mason, Latesha Love, and Sabrina Streagle made key contributions to this report. Also contributing to this report were David Dornisch, Barbara Lewis, Maria McMullen, Sara Ann Moessbauer, and Kathy Pedalino.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

Stephen J. Sanford, Acting Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548