



SMALL BUSINESS RESEARCH PROGRAMS

Opportunities Exist for SBA and Agencies to Reduce Vulnerabilities to Fraud, Waste, and Abuse

Report to Congressional Committees

September 2024
GAO-24-105470
United States Government Accountability Office

Accessible Version

GAO Highlights

View [GAO-24-105470](#). For more information, contact Rebecca Shea at 202-512-6722 or SheaR@gao.gov.
Highlights of [GAO-24-105470](#), a report to congressional committees

September 2024

SMALL BUSINESS RESEARCH PROGRAMS

Opportunities Exist for SBA and Agencies to Reduce Vulnerability to Fraud, Waste, and Abuse

Why GAO Did This Study

Since the inception of the programs, federal agencies have invested over \$68 billion in SBIR/STTR awards for research and development and to commercialize technologies. SBA oversees the programs, which are carried out by 11 participating agencies. In response to the Small Business Act, as amended, the SBA established 10 minimum requirements for participating agencies to prevent fraud, waste, and abuse. The act also includes a provision that GAO report to Congress every 4 years on agencies' and their Offices of Inspector General (OIG) efforts related to fraud, waste, and abuse in the programs.

This GAO report, its fourth, assesses (1) SBIR/STTR fraud schemes from fiscal years 2016 through 2023 and participants and impacts; (2) SBA and agency antifraud activities against fraud, waste, and abuse requirements; (3) agency fraud risk assessments against leading practices; and (4) applicant and award data to identify fraud, waste, and abuse vulnerabilities.

GAO reviewed documentation from SBA and the 11 participating agencies and OIGs; analyzed criminal, civil, and administrative actions; compared SBA and agencies' processes against leading practices; conducted data matching to identify potentially ineligible awardees for fiscal years 2016 through 2021; and interviewed SBA, agency, and OIG officials.

What GAO Recommends

GAO is making eight recommendations, including six to SBA to provide agencies with guidance to support their fraud risk management. The agencies generally agreed with the recommendations

What GAO Found

GAO's analysis of 37 fraud schemes targeting the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs demonstrates control vulnerabilities and fraud risks with a range of financial and other impacts. These schemes often involved multiple participating agencies and programs. For example, 25 schemes involved awards from more than one agency, and 14 involved both SBIR and STTR awards. GAO identified approximately \$34.7 million in civil settlements associated with these schemes. Fraudsters' diversion of funds affects the programs' economic stimulus goals and makes funds unavailable to eligible businesses. It can also result in prison time, financial penalties, and loss of employment for those involved in the schemes.

In addition to its Policy Directive guidance, the U.S. Small Business Administration (SBA) uses several tools, including its monthly program manager meetings, annual survey to participating agencies, and listing of fraud convictions and civil liabilities on SBIR.gov, to monitor and support agencies' fraud, waste, and abuse prevention efforts. However, GAO identified opportunities for SBA to better leverage these tools. For example, some agencies

were unaware of the requirement to report fraud convictions and civil liabilities for listing on SBIR.gov, limiting the site's usefulness as an information source and fraud deterrent.

Most agencies did not conduct SBIR/STTR fraud risk assessments in alignment with GAO's leading practices and identified lack of guidance, training, and resources as related challenges. Through its guidance and other tools, SBA is in a position to reinforce fraud risk assessment requirements for agencies, in support of Policy Directive goals for fraud, waste, and abuse prevention.

GAO's analysis of SBIR.gov award data from fiscal years 2016 through 2021 identified thousands of awardees with one or more fraud, waste, or abuse risk indicator. Among the 10,570 awardees in this period, 842 were associated with four or more such indicators. GAO designed 27 analytic tests for (1) applicant eligibility, including foreign ownership, business size, essentially equivalent work, research facility address; and (2) other fraud, waste, or abuse risks, such as having prior criminal or civil actions. Data quality issues in SBIR.gov, such as incomplete project summaries, may impede agencies' full use of analytics for managing these risks. By improving the data through guidance and verification, SBA can support agencies' risk management activities.

Awardees by Number of Fraud, Waste, or Abuse Risk Indicators Identified in Analytic Tests



Source: GAO analysis of U.S. Small Business Administration data. | GAO-24-105470

Accessible Data for Awardees by Number of Fraud, Waste, or Abuse Risk Indicators Identified in Analytic Tests

Number of tests that identified risk of fraud, waste, or abuse	Number of fiscal years 2016 to 2021 awardees
0	1842
1	3744
2	2878
3	1264
4 or more	842

Source: GAO analysis of U.S. Small Business Administration data. | GAO-24-105470

Contents

GAO Highlights	ii	
Why GAO Did This Study	ii	
What GAO Recommends	ii	
What GAO Found	ii	
<hr/>		
Letter	1	
Background	5	
Fraud Schemes Demonstrate SBIR/STTR Control Vulnerabilities and Fraud Risks	19	
SBA Can Better Leverage Oversight Mechanisms for Fraud, Waste, and Abuse Prevention and Ensure All Agencies Have Training in Place	28	
Some Agency Efforts Partially Align with Leading Practices for Fraud Risk Assessment, and SBA Guidance Could Improve Agencies' Alignment to Support SBIR/STTR Fraud Prevention Requirements	35	
Participating Agencies Could Benefit from Improved Data Analytics and Data Quality to Identify Potentially Ineligible Applicants, Awardees, and Other Risks	51	
Conclusions	77	
Recommendations for Executive Action	78	
Agency Comments and Our Evaluation	79	
<hr/>		
Appendix I	Objectives, Scope, and Methodology	83
Appendix II	Analysis of Nonfinancial Impacts of Fraud Schemes	95
Appendix III	Comparison of GAO Fraud Risk Framework Leading Practices with the Policy Directive	97
Appendix IV	Fraud, Waste, or Abuse Risk Categories, Descriptions, and Examples	106
Appendix V	Comments from the U.S. Small Business Administration	110
Accessible Text for Appendix V	Comments from the U.S. Small Business Administration	112
Appendix VI	Comments from the U.S. Department of Agriculture	114
Accessible Text for Appendix VI	Comments from the U.S. Department of Agriculture	115
Appendix VII	GAO Contact and Staff Acknowledgments	116
<hr/>		
Tables		
Table 1: The U.S. Small Business Administration's Policy Directive's 10 Minimum Requirements for Participating Agencies to Prevent Fraud, Waste, and Abuse in the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs, as of April 2024	11	

Table 2: Nonfinancial Impacts of Fraud in Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs	26
Table 3: Examples of Broader Efforts That Participating Agencies Leverage to Manage Small Business Innovation (SBIR) and Small Business Technology Transfer (STTR) Program Risk	40
Table 4: Reasons Participating Agencies Provided for Not Conducting Small Business Innovation (SBIR) and Small Business Technology Transfer (STTR) Fraud Risk Assessments	42
Table 5: Resources to Identify Applicant Foreign Ownership Risks That Participating Agencies Reported Using	56
Table 6: Resources to Identify Applicant Size Risks That Participating Agencies Reported Using	58
Table 7: Resources to Identify Applicant Principal Investigator Risks That Participating Agencies Reported Using	60
Table 8: Resources to Identify Applicant Equivalent Work Risks That Participating Agencies Reported Using	63
Table 9: Resources to Identify Applicant Facility Address Risks That Participating Agencies Reported Using	66
Table 10: Data Quality Limitations Identified in Our Analysis of the U.S. Small Business Administration’s Company Registry	74
Table 11: Data Quality Limitations Identified in Our Analysis of the U.S. Small Business Administration’s SBIR.gov Awards Database	75
Table 12: Analytic Tests Designed and Performed to Identify Potential Fraud, Waste, or Abuse Risks in Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs	89
Table 13: Fraud, Waste, or Abuse Risk Categories, Descriptions, and Examples	106

Figures

Awardees by Number of Fraud, Waste, or Abuse Risk Indicators Identified in Analytic Tests	iii
Accessible Data for Awardees by Number of Fraud, Waste, or Abuse Risk Indicators Identified in Analytic Tests	iii
Figure 1: Goals of the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs	5
Accessible Data for Figure 1: Goals of the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs	6
Figure 2: Agencies and Subcomponents Participating in the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs and The Types of Award Vehicles Used	8
Accessible Data for Figure 2: Agencies and Subcomponents Participating in the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs and The Types of Award Vehicles Used	9
Figure 3: A Framework for Managing Fraud Risks in Federal Programs	13

Accessible Data for Figure 3: A Framework for Managing Fraud Risks in Federal Programs 14

Figure 4: Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Program Fraud Risk Management Requirements 17

Accessible Data for Figure 4: Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Program Fraud Risk Management Requirements 18

Figure 5: Small Business Innovation Research and Small Business Technology Transfer Fraud Schemes Based on Actions Reported, Fiscal Years 2016 through 2023 21

Accessible Data for Figure 5: Small Business Innovation Research and Small Business Technology Transfer Fraud Schemes Based on Actions Reported, Fiscal Years 2016 through 2023 21

Figure 6: Individuals and Businesses Associated with Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Fraud Schemes, Based on Actions Reported, Fiscal Years 2016 through 2023 22

Accessible Data for Figure 6: Individuals and Businesses Associated with Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Fraud Schemes, Based on Actions Reported, Fiscal Years 2016 through 2023 23

Figure 7: Fraud Schemes Involving Awards from Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Participating Agencies, Fiscal Years 2016 through 2023 24

Accessible Data for Figure 7: Fraud Schemes Involving Awards from Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Participating Agencies, Fiscal Years 2016 through 2023 24

Figure 8: Sentencing Outcomes and Ranges for Criminal Defendants in Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Fraud Schemes, Fiscal Years 2016 through 2023 28

Accessible Data for Figure 8: Sentencing Outcomes and Ranges for Criminal Defendants in Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Fraud Schemes, Fiscal Years 2016 through 2023 28

Figure 9: Participating Agencies' Use of Program-Specific Fraud Risk Assessments and Enterprise Risk Management Processes for Their Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs, as of April 2023 38

Accessible Data for Figure 9: Participating Agencies' Use of Program-Specific Fraud Risk Assessments and Enterprise Risk Management Processes for Their Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs, as of April 2023 39

Figure 10: Examples of Challenges Participating Agencies Identified in Conducting Small Business Innovation (SBIR) and Small Business Technology Transfer (STTR) Fraud Risk Assessments 43

Accessible Data for Figure 10: Examples of Challenges Participating Agencies Identified in Conducting Small Business Innovation (SBIR) and Small Business Technology Transfer (STTR) Fraud Risk Assessments 44

Figure 11: Participating Agencies' Subcomponents That Conducted, or Contributed to, Program-Specific Fraud Risk Assessments, as of April 2023 46

Accessible Data for Figure 11: Participating Agencies' Subcomponents That Conducted, or Contributed to, Program-Specific Fraud Risk Assessments, as of April 2023 46

Figure 12: Inherent Fraud Risks Identified in Participating Agency and Subcomponent Fraud Risk Assessments, as of April 2023 48

Accessible Data for Figure 12: Inherent Fraud Risks Identified in Participating Agency and Subcomponent Fraud Risk Assessments, as of April 2023 49

Figure 13: Analytic Tests and Results for Selected Program Eligibility Requirements 52

Accessible Data for Figure 13: Analytic Tests and Results for Selected Program Eligibility Requirements 53

Figure 14: Analytic Tests of Selected Policy Directive Guidelines and Results for Awardees with Potential Fraud, Waste, or Abuse Risks 70

Accessible Data for Figure 14: Analytic Tests of Selected Policy Directive Guidelines and Results for Awardees with Potential Fraud, Waste, or Abuse Risks 70

Figure 15: Analytic Tests of Selected Office of Inspector General Fraud Detection Indicators and Fraud Schemes and Results for Awardees with Potential Fraud, Waste, or Abuse Risks 72

Accessible Data for Figure 15: Analytic Tests of Selected Office of Inspector General Fraud Detection Indicators and Fraud Schemes and Results for Awardees with Potential Fraud, Waste, or Abuse Risks 72

Figure 16: Awardees by Number of Fraud, Waste, or Abuse Risk Indicators Identified in Analytic Tests of Small Business Innovation Research and Small Business Technology Transfer Awards, Fiscal Years 2016 through 2021 73

Accessible Data for Figure 16: Awardees by Number of Fraud, Waste, or Abuse Risk Indicators Identified in Analytic Tests of Small Business Innovation Research and Small Business Technology Transfer Awards, Fiscal Years 2016 through 2021 73

Figure 17: Comparison of Fraud Risk Framework Leading Practices for Creating a Culture and Structure to Manage Fraud Risks (Component 1) and Policy Directive Guidance 98

Accessible Data for Figure 17: Comparison of Fraud Risk Framework Leading Practices for Creating a Culture and Structure to Manage Fraud Risks (Component 1) and Policy Directive Guidance 99

Figure 18: Comparison of Fraud Risk Framework Leading Practices for Planning and Conducting Fraud Risk Assessments (Component 2) and Policy Directive Guidance 100

Accessible Data for Figure 18: Comparison of Fraud Risk Framework Leading Practices for Planning and Conducting Fraud Risk Assessments (Component 2) and Policy Directive Guidance 100

Figure 19: Comparison of Fraud Risk Framework Leading Practices for Designing and Implementing an Antifraud Strategy with Control Activities (Component 3) and Policy Directive Guidance 102

Accessible Data for Figure 19: Comparison of Fraud Risk Framework Leading Practices for Designing and Implementing an Antifraud Strategy with Control Activities (Component 3) and Policy Directive Guidance 103

Figure 20: Comparison of Fraud Risk Framework Leading Practices for Monitoring, Evaluating, and Adapting Fraud Risk Management Activities (Component 4) and Policy Directive Guidance 104

Accessible Data for Figure 20: Comparison of Fraud Risk Framework Leading Practices for Monitoring, Evaluating, and Adapting Fraud Risk Management Activities (Component 4) and Policy Directive Guidance

104

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.

Abbreviations

C.F.R.	Code of Federal Regulations
DHS	U.S. Department of Homeland Security
DOD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOJ	U.S. Department of Justice
DOT	U.S. Department of Transportation
DUNS number	Data Universal Numbering System
FAR	Federal Acquisition Regulation
Federal Internal Control Standards	<i>Standards for Internal Control in the Federal Government</i>
Fraud Risk Framework	<i>A Framework for Managing Fraud Risks in Federal Programs</i>
EPA	U.S. Environmental Protection Agency
HHS	U.S. Department of Health and Human Services
NASA	National Aeronautics and Space Administration
NSF	U.S. National Science Foundation
OIG	Office of Inspector General
OMB	Office of Management and Budget
Policy Directive	U.S. Small Business Administration Policy Directive
SBA	U.S. Small Business Administration
SBIR	Small Business Innovation Research
STTR	Small Business Technology Transfer
USDA	U.S. Department of Agriculture
Working Group	SBIR Investigations Working Group



September 9, 2024

Congressional Committees

Federal agencies support research and development by small businesses through the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs. The U.S. Small Business Administration (SBA)'s Office of Investment and Innovation oversees these programs, which are carried out by 11 participating agencies and their subcomponents.¹ Participating agencies make SBIR/STTR awards through grants, contracts, or cooperative agreements to small businesses to meet agency mission needs for research and development in different technology areas.² In some instances, these mission needs focus on supporting research and development that would ultimately provide benefit beyond the agency, such as for the American public at large. In other instances, agencies' mission needs focus on advancing the development of technologies that would be used by the agencies themselves.

According to data from SBA, collectively, in fiscal year 2022, the 11 participating agencies provided more than 6,500 awards, valued at more than \$4.4 billion, to more than 4,000 small businesses. Since the inception of SBIR in 1982, as of January 2023, federal agencies have made over 180,000 awards, totaling about \$61.6 billion. For STTR, which started in 1992, federal agencies have made over 18,000 awards, totaling more than \$6.4 billion.

Fraud, waste, and abuse compromise the SBIR/STTR programs' resources and limit opportunities for legitimate small businesses to contribute to program goals for technological innovation, increased productivity, and economic growth.³ Participating agencies must guard against a wide range of fraud, waste, and abuse schemes.⁴ GAO's *Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework) provides a comprehensive set of leading practices for agency managers to use to combat fraud in a strategic,

¹The 11 agencies that participate in the SBIR program are the U.S. Departments of Agriculture (USDA), Commerce, Defense (DOD), Education, Energy (DOE), Health and Human Services (HHS), Homeland Security (DHS), and Transportation (DOT); the National Aeronautics and Space Administration (NASA), the U.S. Environmental Protection Agency (EPA), and the U.S. National Science Foundation (NSF). Five of these agencies also participate in the STTR program: DOD, DOE, HHS, NASA, and NSF. USDA began participating in the STTR program in fiscal year 2023; however, these awards are not within our audit scope.

²One agency uses grants exclusively (USDA); five agencies use contracts exclusively (DHS, DOT, Education, NASA, and EPA); three agencies use cooperative agreements and grants (Commerce, DOE, and NSF); and two agencies use contracts, cooperative agreements, and grants (DOD and HHS).

³Fraud involves obtaining something of value through willful misrepresentation (e.g., materially false statements of fact based on actual knowledge, deliberate ignorance, or reckless disregard of falsity). Whether an act is, in fact, fraud is a determination to be made through the judicial or other adjudicative system and is beyond management's professional responsibility for assessing risk. Waste is the act of using or expending resources carelessly, extravagantly, or to no purpose. Abuse involves behavior that is deficient or improper, when compared with behavior that a prudent person would consider reasonable and necessary operational practice, given the facts and circumstances. GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014); and *Standards for Internal Control in the Federal Government: 2024 Exposure Draft*, [GAO-24-106889](#) (Washington, D.C.: June 27, 2024).

⁴GAO, *GAO Overview: Fraud in the Federal Government – Challenges Determining the Extent of Federal Fraud*, [GAO-23-106110](#) (Washington, D.C.: Jan. 23, 2023); *GAO Overview: Understanding Waste in Federal Programs*, [GAO-24-107198](#) (Washington, D.C.: May 9, 2024); and *GAO Overview: Understanding Abuse of Federal Programs: Challenges Identifying and Determining Abuse of Federal Programs*, [GAO-24-106458](#) (Washington, D.C.: Dec. 12, 2023).

risk-based way.⁵ Although waste and abuse do not necessarily involve fraud or illegal acts, they may be an indication of potential fraud or illegal acts and may affect the achievement of defined objectives.

The SBIR/STTR Reauthorization Act of 2011 required SBA to add fraud, waste, and abuse prevention requirements to its guidance, the SBIR/STTR Policy Directive (Policy Directive), for agencies to implement.⁶ SBA issued revised guidance for the SBIR/STTR programs in August 2012 that included requirements designed to help participating agencies identify and prevent potential fraud, waste, and abuse in the programs.⁷ Specifically, SBA's guidance update included 10 minimum requirements related to fraud, waste, and abuse that the 11 participating agencies and their subcomponents must meet. This includes providing information on how to report fraud, waste, and abuse on their program websites and in solicitations, among other things. In this report, we reference the October 2020 Policy Directive.

The Small Business Act, as amended, includes a provision for GAO to review every 4 years what the participating agencies and their Offices of Inspector General (OIG) are doing to prevent; identify; respond to; and reduce fraud, waste, and abuse in the SBIR/STTR programs.⁸ We issued prior reports in June 2021, April 2017, and November 2012.⁹ In June 2021, we found that agencies used differing approaches to implement the Policy Directive requirements related to fraud, waste, and abuse. Of the 21 recommendations we made in June 2021, three recommendations remain open for two DOD subcomponents that participate in the SBIR/STTR programs as of May 2024. The remaining 18 recommendations have been implemented by the participating agencies.

This fourth report (1) describes SBIR/STTR fraud schemes in fiscal years 2016 through 2023, participants, and impacts; (2) evaluates the extent to which selected SBA and participating agency antifraud activities align with program fraud, waste, and abuse prevention requirements and leading practices; (3) evaluates the extent to which agencies assessed fraud risks in alignment with leading practices; and (4) evaluates the extent to which applicant and award data from fiscal years 2016 through 2021 indicate vulnerabilities to fraud, waste, and abuse, and identifies opportunities for participating agencies and SBA to leverage data analytics.

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

⁶Pub. L. No. 112-81, Div. E, Title LI, § 5143, 125 Stat. 1298, 1854 (2011), codified at 15 U.S.C. § 638b.

⁷SBA issued revised guidance for the SBIR/STTR programs in August 2012 that included new requirements designed to help agencies identify and prevent potential fraud, waste, and abuse in the programs—changes that SBA developed in consultation with participating agencies and a working group of inspectors general. The Policy Directive has since been updated in February 2014, May 2019, October 2020 and, most recently, in May 2023. The May 2023 Policy Directive update did not change fraud, waste, and abuse requirements and does not apply to the awards within our review.

⁸15 U.S.C. § 638b(b). Responsibility for investigating fraud, waste, and abuse in SBIR and STTR programs is typically found within the participating agencies' OIGs. However, in the three DOD military departments of the Army, Navy, and Air Force, investigative responsibilities are instead located in the Army Criminal Investigation Command, Naval Criminal Investigative Service, and Air Force Office of Special Investigations. We refer to them collectively as the OIGs and military investigative offices.

⁹GAO's provision includes reviewing the effectiveness of the risk management strategies of each federal agency that participates in the SBIR or STTR program in identifying areas of the programs that are at high risk for fraud and the success of each federal agency that participates in the SBIR or STTR program in reducing fraud, waste, and abuse in the programs of the federal agency, among other things. Previous reports are GAO, *Small Business Innovation Research: Agencies Need to Fully Implement Requirements for Managing Fraud, Waste, and Abuse*, [GAO-21-413](#) (Washington, D.C.: June 30, 2021); *Small Business Research Programs: Additional Actions Needed to Implement Fraud, Waste, and Abuse Prevention Requirements*, [GAO-17-337](#) (Washington, D.C.: Apr. 15, 2017); and *Small Business Research Programs: Agencies Are Implementing New Fraud, Waste, and Abuse Requirements*, [GAO-13-70R](#) (Washington, D.C.: Nov. 15, 2012).

For the first objective, we analyzed 60 SBIR/STTR publicly reported criminal, civil, and administrative actions to identify instances of alleged and adjudicated fraud. These actions were initiated or resolved during fiscal years 2016 through 2023 and closed by the end of fiscal year 2023.¹⁰ To identify actions, we received U.S. Department of Justice (DOJ) press releases through a subscription to Westlaw and used other available sources, such as the SBIR.gov and Law360 websites.¹¹ For identified actions, we obtained relevant court documents by searching Public Access to Court Electronic Records.¹² We conducted thematic analyses based on the GAO Conceptual Fraud Model using action information identified in DOJ press releases and court documents.¹³ Specifically, we analyzed information on charged individuals and businesses, as well as judgment and settlement amounts, among other things, related to these actions to identify the characteristics and areas of impact of SBIR/STTR fraud schemes. We also selected individual schemes as illustrative examples of how fraud occurred. These illustrative examples are not generalizable to other schemes.

For the second objective, we assessed the efforts of SBA, the 11 participating agencies, and their OIGs to manage fraud risks against the Policy Directive and leading practices in GAO's Fraud Risk Framework, as appropriate. We included all subcomponents issuing SBIR/STTR awards from fiscal years 2016 through 2021 for the five participating agencies with multiple subcomponents that participate in the SBIR/STTR programs—the Department of Commerce, the Departments of Defense (DOD), Energy (DOE), Homeland Security (DHS), and Health and Human Services (HHS). As a result, we included 23 agency subcomponents in the scope of our review.¹⁴ We compared SBA's guidance (the 2020 Policy Directive) with leading practices in GAO's Fraud Risk Framework, components 1 through 4, to identify areas where the guidance aligned with specific leading practices. We examined SBA's oversight efforts in this context, considering both the Policy Directive goals for fraud, waste, and abuse prevention and leading practices from the Fraud Risk Framework that support those goals. Further, we interviewed SBIR/STTR program officials from the 11 participating agencies and their OIGs regarding their efforts to improve training and develop SBIR fraud detection indicators. We also discussed how the agencies have addressed open recommendations from our June 2021 report on fraud, waste, and abuse in the SBIR/STTR programs.

For the third objective, we evaluated participating agencies' fraud risk profiles and assessments, where available, as well as other documentation, against component 2 leading practices of the Fraud Risk

¹⁰We selected fiscal years 2016 through 2023 to align with our data testing of awards made during fiscal years 2016 through 2021, discussed below, and to capture the most recent information available as of our mandated reporting in fiscal year 2024.

¹¹SBIR.gov is SBA's primary government-wide website for the SBIR/STTR programs. Westlaw and Law360 are legal news services.

¹²Public Access to Court Electronic Records is a service of the federal judiciary that enables the public to search online for case information from U.S. District, Bankruptcy, and Appellate courts. Federal court records available through this system include case information (such as names of parties, proceedings, and documents filed), as well as information on case status.

¹³The model is organized as an ontology, which provides an explicit description of categories of federal fraud, their characteristics, and the relationships among them. GAO, *GAO Fraud Ontology Version 1.0* (Washington, D.C.: Jan. 10, 2022), https://gaoinnovations.gov/antifraud_resource/howfraudworks.

¹⁴DOD added two additional subcomponents in the last 6 fiscal years: (1) the Strategic Capabilities Office was added in fiscal year 2018, and (2) the Space Development Agency was added in fiscal year 2021. We did not assess their participation, as it is outside the scope of our review. In addition, DOE's Office of Science oversees the following seven DOE subcomponent SBIR/STTR programs: (1) the National Nuclear Security Administration; (2) Office of Cybersecurity, Energy Security, and Emergency Response; (3) Office of Electricity; (4) Office of Energy Efficiency and Renewable Energy; (5) Office of Environmental Management; (6) Office of Fossil Energy and Carbon Management; and (7) Office of Nuclear Energy. We did not include these seven DOE subcomponents in our review. The Advanced Research Projects Agency for Health within HHS began participating in the SBIR/STTR programs in June 2023. We did not assess these subcomponents' participation, which is outside of the scope of our review.

Framework. Specifically, we assessed whether agencies within our scope have developed comprehensive fraud risk assessments that identified, analyzed, and responded to inherent fraud risks for the SBIR/STTR program and used available OIG SBIR fraud detection indicators.¹⁵ We interviewed SBA and the 11 participating agency officials to discuss policies and processes relevant to managing fraud risks and to describe how they identify, assess, and manage program fraud risks.

For the fourth objective, we matched data from participating agencies for fiscal years 2016 through 2021 SBIR and STTR program awards found on SBIR.gov to government contracting and grant performance, wage, exclusions, and other data. We did so to identify potential fraud, waste, and abuse, as well as to assess data reliability.¹⁶ We interviewed SBA officials to determine how SBIR/STTR awards data are managed. We also interviewed officials from the 11 participating agencies to describe how they identify, assess, and manage potential applicant and awardee fraud risks. We also analyzed the extent to which SBA's and agencies' practices align with relevant leading practices in GAO's Fraud Risk Framework. A relevant leading practice from the Fraud Risk Framework encourages agencies to conduct data analytics activities to prevent and detect fraud. For example, agencies can consider program rules and known or previously encountered fraud schemes to design analytic tests. Where able, agencies combine data across programs and from separate databases to facilitate analytics and to verify applicant information to determine eligibility. Additionally, agencies can conduct data mining to identify inconsistencies and other anomalies within the data. We also analyzed the extent to which the SBA's and agencies' practices align with *Standards for Internal Control in the Federal Government* (Federal Internal Control Standards).¹⁷

We took steps to review data reliability, as well as to ensure the accuracy of the data used for testing and to standardize the data, where necessary. All data were reviewed to ensure that fields were imported correctly and contained the appropriate information for data testing. Any limitations on the data were documented and determined to not cause a material impact to test for potential fraud, waste, and abuse. On the basis of our data analysis, we selected awardees for on-site observation or inspection by GAO criminal investigators. We selected these awardees with addresses that may not be appropriate based on the type of research conducted for the SBIR/STTR award. Results from our analysis and investigation where we found the presence of fraud, waste, or abuse risks will result in referrals to relevant agency OIGs for further investigation.

Additional details regarding our objectives, scope, and methodology can be found in appendix I.

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

¹⁵As discussed in the Fraud Risk Framework, a fraud risk profile documents the fraud risk assessment and serves as the basis for an overall antifraud strategy, [GAO-15-593SP](#). We used the most recent fraud risk assessments and profiles as of March 2023, according to agency officials. The Policy Directive requires that participating agencies collaborate with their OIGs on developing SBIR fraud detection indicators. Fraud detection indicators range from specific fraud risks—such as “bait-and-switch” schemes, in which contractors propose an experienced researcher as the principal investigator and then use a less-qualified, lower-cost employee to serve in that role—to general indicators of potential fraud, such as significant levels of foreign ownership.

¹⁶We selected this scope of awards, given that it was the most complete set of more than 5 years of awards data at the time of our review.

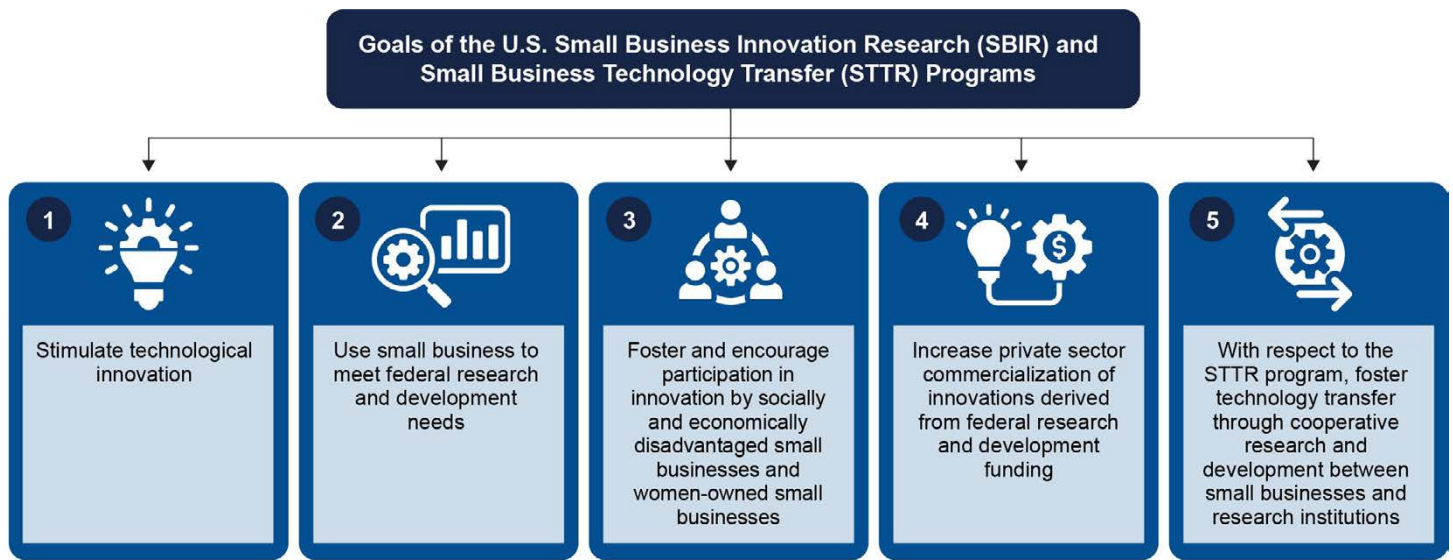
¹⁷[GAO-14-704G](#).

findings and conclusions based on our audit objectives. We conducted our related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

Background

Congress established the SBIR/STTR programs to enable small businesses to undertake and obtain the benefits of research and development.¹⁸ The SBIR/STTR programs are similar in that participating agencies identify topics for research and development projects and support small businesses.¹⁹ The STTR program also requires the small business to partner with a research institution—such as a nonprofit college or university or federally funded research and development center. See figure 1 for the goals of the SBIR/STTR programs.

Figure 1: Goals of the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs



Sources: U.S. Small Business Administration documentation; Icon-Studio/stock.adobe.com (icons). | GAO-24-105470

¹⁸The Small Business Innovation Development Act of 1982 established the SBIR program. Pub. L. No. 97-219, 96 Stat. 217. This act amended section 9 of the Small Business Act, Pub. L. No. 85-536, 72 Stat. 384 (1958), codified as amended at 15 U.S.C. § 638. The Small Business Technology Transfer Act of 1992 established the STTR program. Pub. L. No. 102-564, §§ 201-02, 106 Stat. 4249, 4256-61. This act made additional amendments to section 9 of the Small Business Act.

¹⁹Research topics can be conventional or open topics. For conventional topics, agencies define specific problems or mission needs, and small businesses propose solutions. For open topics, agencies define broad topics, and small businesses propose both the potential needs and solutions to address the needs. GAO, *Small Business Research Programs: Most Agencies Allow Applicants to Define Needs and Propose Solutions*, GAO-23-106338 (Washington, D.C.: Sept. 29, 2023).

Accessible Data for Figure 1: Goals of the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs

Goals of the U.S. Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs

1. Stimulate technological innovation
2. Use small business to meet federal research and development needs
3. Foster and encourage participation in innovation by socially and economically disadvantaged small businesses and women-owned small businesses
4. Increase private sector commercialization of innovations derived from federal research and development funding
5. With respect to the STTR program, foster technology transfer through cooperative research and development between small businesses and research institutions

Sources: U.S. Small Business Administration documentation; Icon-Studio/stock.adobe.com (icons). | GAO-24-105470

Note: Program goals one through four apply to the SBIR program, and all five goals apply to the STTR program.

Each participating agency must manage its SBIR/STTR programs in accordance with program laws, regulations, and guidance issued by SBA. The SBA's Office of Investment and Innovation oversees and coordinates agency efforts for the programs by setting overarching policy, issuing guidance, collecting program data, reviewing agency progress, and reporting annually to Congress, among other responsibilities. Each participating agency has considerable flexibility to design and manage the specifics of these programs, such as determining research topics, issuing solicitations, selecting awardees, and administering funding agreements.²⁰

SBIR/STTR awards to small businesses are generally \$50,000 to about \$300,000 for the initial award (commonly called phase I awards) and \$750,000 to about \$2 million for subsequent follow-on awards (commonly called phase II awards).²¹ Phase I awards are intended to determine the scientific and technical merit and feasibility of ideas that appear to have commercial potential. Phase II supports further research and development efforts initiated in phase I that meet particular program needs and exhibit potential for commercial application. Phase III is focused on commercialization of the results of phase I and phase II awards; however, the SBIR/STTR programs do not provide funding in phase III.

At least once per year, each participating agency issues a solicitation requesting proposals for projects in a variety of topic areas determined by the agency.²² Each participating agency uses its own process to review proposals and determine which proposals should receive awards and then negotiates contracts, grants, or

²⁰The Policy Directive defines a funding agreement as any contract, grant, or cooperative agreement entered into between any federal agency and any small business for the performance of experimental, developmental, or research work, including products or services, funded in whole, or in part, by the federal government.

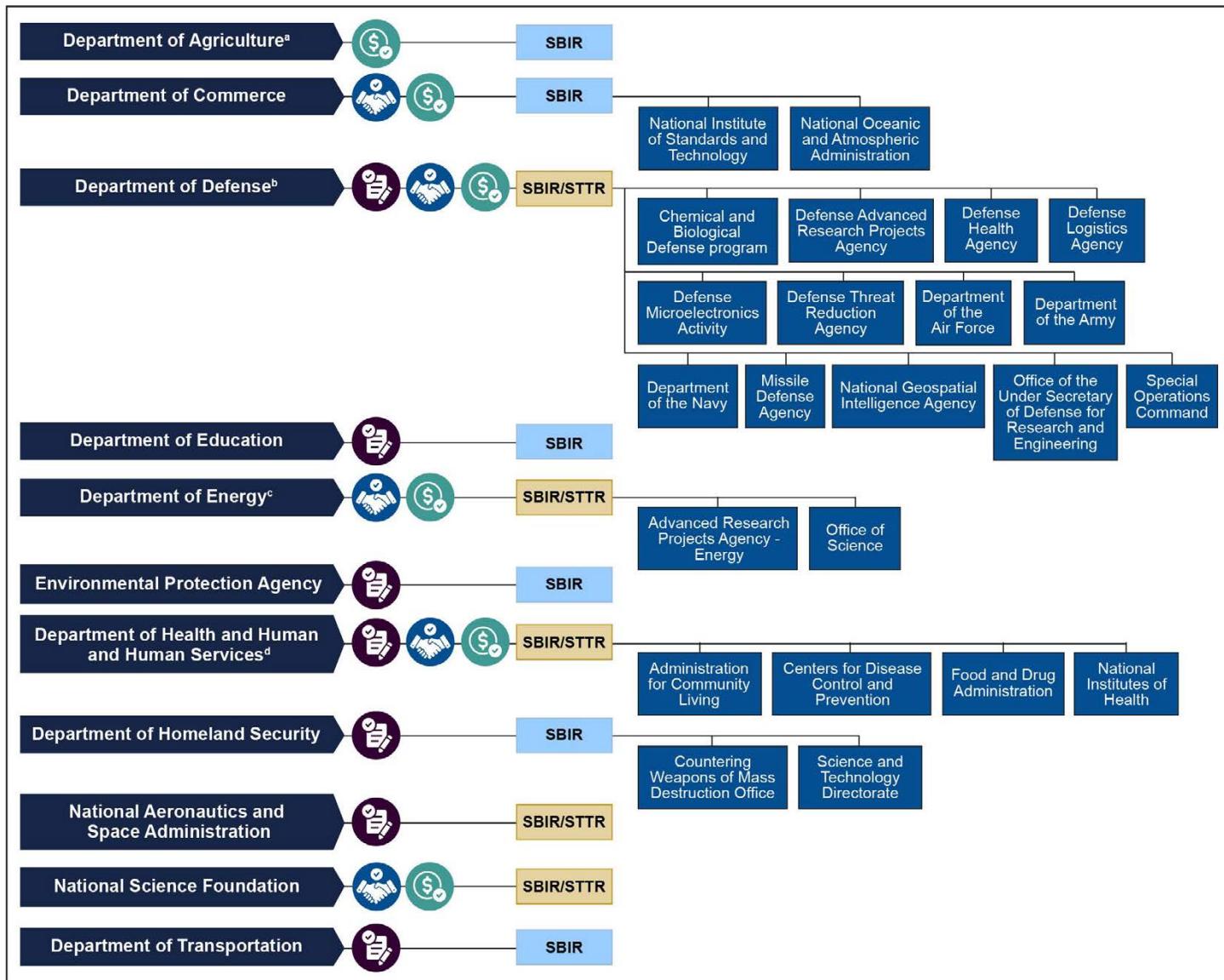
²¹As of October 2023, agencies may issue a phase I award (including modifications) up to \$306,872 and a phase II award (including modifications) up to \$2,045,816 without seeking SBA approval. Any award above those levels requires a waiver. Generally, SBIR phase I awards are 6 months, and STTR phase I awards are 1 year. SBIR/STTR phase II awards are generally 2 years.

²²Some agencies issue awards on open topics. In response to solicitations with open topics, small businesses submit proposals that both define research needs and propose solutions to address them. [GAO-23-106338](#).

cooperative agreements to issue the awards to the selected small business applicants.²³ The agencies that have both SBIR and STTR programs usually use the same process for both programs. See figure 2 for participating agencies and subcomponents that participate in the programs.

²³An applicant is the organizational entity (business) that qualifies as a small business concern and submits a contract proposal, grant application, or cooperative agreement for a funding agreement under the SBIR/STTR programs.

Figure 2: Agencies and Subcomponents Participating in the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs and The Types of Award Vehicles Used



Agency
 Participating
 Subcomponent

Award vehicle
 Contracts
 Cooperative agreements
 Grants

Program type
 SBIR Small Business Innovation Research
 SBIR/STTR Small Business Innovation Research and Small Business Technology Transfer

Sources: GAO analysis of U.S. Small Business Administration and participating agency documentation; Icons-Studio/stock.adobe.com (icons). | GAO-24-105470

Accessible Data for Figure 2: Agencies and Subcomponents Participating in the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs and The Types of Award Vehicles Used

Agency (participating)	Award vehicle	Program type	Agency (subcomponent)
Department of Agriculture ^a	Grants	Small Business Innovation Research	
Department of Commerce	Cooperative agreements Grants	Small Business Innovation Research	National Institute of Standards and Technology National Oceanic and Atmospheric Administration
Department of Defense ^b	Contracts Cooperative agreements Grants	Small Business Innovation Research and Small Business Technology Transfer	Chemical and Biological Defense program Defense Advanced Research Projects Agency Defense Health Agency Defense Logistics Agency Defense Microelectronics Activity Defense Threat Reduction Agency Department of the Air Force Department of the Army Department of the Navy Missile Defense Agency National Geospatial Intelligence Agency Office of the Under Secretary of Defense for Research and Engineering Special Operations Command
Department of Education	Contracts	Small Business Innovation Research	
Department of Energy ^c	Cooperative agreements Grants	Small Business Innovation Research and Small Business Technology Transfer	Advanced Research Projects Agency – Energy Office of Science
Environmental Protection Agency	Contracts	Small Business Innovation Research	
Department of Health and Human Services ^d	Contracts Cooperative agreements Grants	Small Business Innovation Research and Small Business Technology Transfer	Administration for Community Living Centers for Disease Control and Prevention Food and Drug Administration National Institutes of Health
Department of Homeland Security	Contracts	Small Business Innovation Research	Countering Weapons of Mass Destruction Office Science and Technology Directorate

Agency (participating)	Award vehicle	Program type	Agency (subcomponent)
National Aeronautics and Space Administration	Contracts	Small Business Innovation Research and Small Business Technology Transfer	
National Science Foundation	Grants Cooperative agreements	Small Business Innovation Research and Small Business Technology Transfer	
Department of Transportation	Contracts	Small Business Innovation Research	

Sources: GAO analysis of U.S. Small Business Administration and participating agency documentation; icons-Studio/stock.adobe.com (icons) | GAO-24-105470

^aThe U.S. Department of Agriculture began participating in the STTR program in fiscal year 2023. We did not assess its participation, as it is outside the scope of our review of awards from fiscal years 2016 through 2021.

^bThe U.S. Department of Defense also uses other transaction authorities for a limited number of awards, according to agency officials. Other transaction authority is the term commonly used to refer to the 10 U.S.C. § 4021 authority of the U.S. Department of Defense to carry out certain prototypes, research, and production projects. These authorities were created to give the department the flexibility necessary to adopt and incorporate business practices that reflect commercial industry standards and best practices into its award instruments. The U.S. Department of Defense added two additional subcomponents in the last 6 fiscal years: (1) the Strategic Capabilities Office was added in fiscal year 2018, and (2) the Space Development Agency was added in fiscal year 2021. We did not assess their participation, as it is outside the scope of our review. Not all award vehicle types listed for each agency are utilized by every subcomponent within that agency.

^cThe U.S. Department of Energy’s Office of Science oversees the following seven subcomponent SBIR/STTR programs: the (1) National Nuclear Security Administration; (2) Office of Cybersecurity, Energy Security, and Emergency Response; (3) Office of Electricity; (4) Office of Energy Efficiency and Renewable Energy; (5) Office of Environmental Management; (6) Office of Fossil Energy and Carbon Management; and (7) Office of Nuclear Energy. We did not assess their participation, as it is outside the scope of our review. The Office of Science also uses the Consolidated Services Center to conduct internal efforts, such as conducting the office’s fraud risk assessments.

^dThe Centers for Disease Control and Prevention and the Food and Drug Administration do not participate in the STTR program. In May 2023, U.S. Department of Health and Human Services officials informed us that the Office of the Assistant Secretary for Financial Resources assumed the role as the department’s SBIR/STTR Coordinator in 2016 and later revised its roles and responsibilities document in February 2024. According to agency officials, this office does not have direct authority over the small business programs, just an oversight role for the department. The Advanced Research Projects Agency for Health began participating in the SBIR program in June 2023. We did not assess these subcomponents’ participation, which is outside of the scope of our review.

SBIR/STTR Fraud, Waste, and Abuse Requirements

In an August 2009 Senate Committee on Commerce, Science, and Transportation hearing on fraud, waste, and abuse in the SBIR program, committee members raised concerns about a prior case of fraud in the SBIR program. They also raised concerns about the potential for additional fraud, waste, and abuse in the programs. Shortly after that hearing, the Council of the Inspectors General on Integrity and Efficiency’s Misconduct in Research Working Group began to discuss fraud in the SBIR/STTR programs and coordinate efforts related to these programs among the inspectors general from SBA and each of the 11 participating agencies.²⁴ The Council of the Inspectors General on Integrity and Efficiency’s Misconduct in Research Working Group also established a separate subgroup of investigative agents from SBA, the 11 participating agencies, and DOJ to share information on ongoing cases, lessons learned, and best practices related to SBIR investigations.²⁵

The SBIR Investigations Working Group (Working Group) strives to foster collaboration between OIGs from the participating agencies investigating fraud, waste, and abuse in SBIR/STTR programs and develop fraud

²⁴The Council of the Inspectors General on Integrity and Efficiency is an independent entity established within the executive branch to address integrity, economy and effectiveness issues that transcend individual government agencies and aid in the establishment of a professional, well-trained, and highly skilled workforce in the OIGs.

²⁵In 2009, special agents from the NSF OIG and DOE OIG co-chaired the interagency, agent-level, investigations working group focused on SBIR- and STTR-related investigative issues. According to Working Group officials, in March 2023, the U.S. Department of Commerce OIG took over the co-chair positions held by the NASA OIG and DOE OIG. The other co-chair remains with the NSF OIG.

indicators. According to the Working Group, OIGs and military investigative offices opened at least 471 SBIR-related fraud, waste, or abuse investigations since the start of the Working Group in 2009, including at least 91 investigations that involved awards made by multiple agencies. According to Working Group officials, these investigations resulted in 53 indictments; 70 guilty verdicts or pleas; and more than \$164 million in criminal restitution, civil settlements, or administrative actions through July 2023. In addition, these investigations resulted in the suspension or debarment of more than 78 individuals or businesses from participation in the programs, according to Working Group officials.

Further, the Small Business Act, as amended, required that SBA add fraud, waste, and abuse prevention requirements to its Policy Directive for agencies to implement.²⁶ SBA, in consultation with the Working Group and the participating agencies, developed 10 minimum requirements to prevent fraud, waste, and abuse in the programs, summarized in table 1.

Table 1: The U.S. Small Business Administration’s Policy Directive’s 10 Minimum Requirements for Participating Agencies to Prevent Fraud, Waste, and Abuse in the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs, as of April 2024

- i. Require certifications of ownership and other eligibility requirements from the SBIR/STTR awardee at the time of award and during the funding agreement life cycle.^a
- ii. Include information on the agency’s SBIR/STTR web page and an awards solicitation that explains how an individual can report fraud, waste, and abuse, as provided by the Office of Inspector General (OIG).
- iii. Designate at least one individual in the agency to serve as the liaison for the programs, the OIG, and the agency’s suspension and debarment official.^b
- iv. Include on the agency’s SBIR/STTR web page information concerning successful prosecutions of fraud, waste, and abuse in the programs.
- v. Establish and communicate a written policy requiring all agency personnel involved with the programs to notify the OIG if anyone suspects fraud, waste, or abuse.
- vi. Ensure there is an adequate system to enforce accountability (through suspension and debarment, fraud referrals, or other efforts to deter wrongdoing and promote integrity) by developing separate standardized templates for each referral made to the OIG or the suspension and debarment official and a process for tracking such referrals.
- vii. Ensure compliance with the eligibility requirements of the programs and the terms of the SBIR/STTR funding agreement.
- viii. Work with the agency’s OIG on efforts to establish fraud detection indicators; coordinate the sharing of information on fraud, waste, and abuse with other federal agencies; and improve education and training of SBIR/STTR program officials, applicants, and awardees on issues related to fraud, waste, and abuse.^c
- ix. Develop policies and procedures to avoid funding essentially equivalent work. Among other things, agencies could comprehensively search SBIR.gov (the U.S. Small Business Administration’s primary government-wide website for the programs) prior to the award or document the funding agreement file with

²⁶Pub. L. No. 112-81, Div. E, Title LI, § 5143, 125 Stat. 1298, 1854 (2011), codified at 15 U.S.C. § 638b. The Policy Directive was updated in August 2012, February 2014, May 2019, October 2020, and May 2023. In this report, we reference the October 2020 Policy Directive. The May 2023 Policy Directive update did not change fraud, waste, and abuse requirements and does not apply to the awards within our review.

a certification showing that the small business concern has not already received funding for essentially equivalent work.

x. Consider enhanced reporting requirements during the funding agreement.

Source: GAO analysis of the U.S. Small Business Administration's SBIR/STTR Policy Directive (effective October 1, 2020). | GAO-24-105470

Note: The Policy Directive was updated in May 2023 and remains in effect as of April 2024. The fraud, waste, and abuse 10 minimum requirements did not change between the October 2020 Policy Directive and the May 2023 Policy Directive.

^aA funding agreement is any contract, grant, or cooperative agreement entered into between any federal agency and any small business for the performance of experimental, developmental, or research work, including products or services, funded in whole or in part by the federal government.

^bThe suspension and debarment process helps protect the federal government from fraud, waste, and abuse by using several tools to avoid doing business with nonresponsible contractors.

^cA program administrator is an official that manages or coordinates the SBIR/STTR program of the participating agency. An applicant is the organizational entity (business) that qualifies as a small business concern and submits a contract proposal, grant application, or cooperative agreement for a funding agreement under the SBIR/STTR programs. An awardee is the business that receives a SBIR/STTR award.

Fraud Risk Management and Broader Enterprise Risk Management Requirements

In June 2021, we found that multiple participating agencies did not fully implement certain Policy Directive requirements, such as collecting eligibility certifications and collaborating with the OIGs.²⁷ Because agencies did not fully implement all 10 requirements, we concluded that they could miss opportunities to implement leading practices GAO identified for managing fraud risks in federal programs.

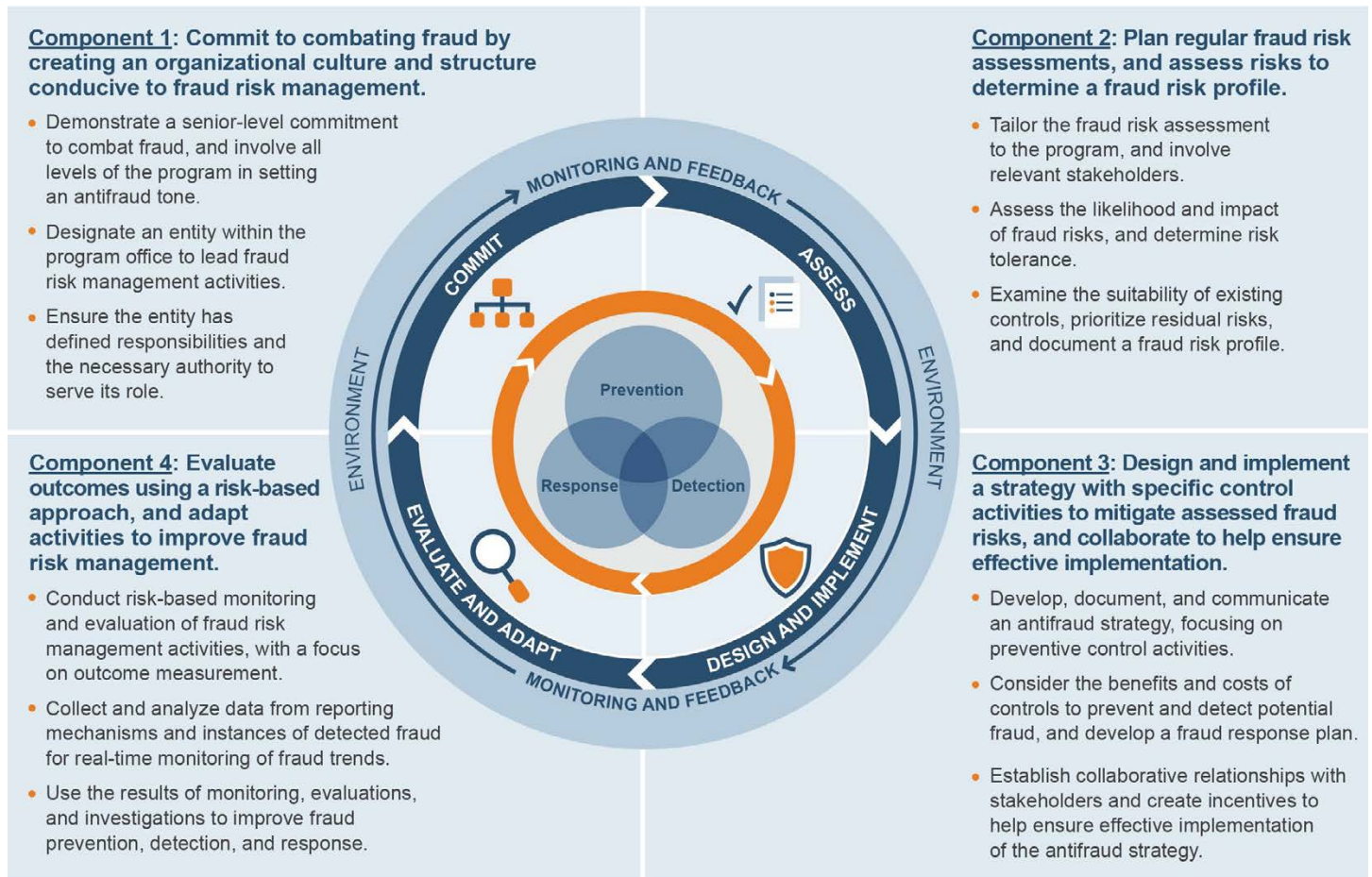
The objective of fraud risk management is to ensure program integrity by continuously and strategically mitigating the likelihood and effects of fraud. It encourages a preventative approach by program managers over a detection and response (or “pay-and-chase”) approach to managing fraud risks in federal programs. Effectively managing fraud risk helps to ensure that federal programs’ services fulfill their intended purpose, that funds are spent effectively, and that assets are safeguarded. Federal agency managers are responsible for managing fraud risks and implementing practices for combating those risks.

GAO’s Fraud Risk Framework provides a comprehensive set of key components, overarching concepts, and leading practices that serve as a guide for agency managers to use when developing efforts to combat fraud in a strategic, risk-based way.²⁸ As depicted in figure 3, the Fraud Risk Framework describes leading practices within four components: commit, assess, design and implement, and evaluate and adapt.

²⁷In June 2021, GAO made 21 recommendations to 10 agencies to take steps to fully implement all 10 minimum requirements established by SBA. As of May 2024, 18 recommendations had been implemented by nine agencies, and three recommendations to one agency remained open.

²⁸[GAO-15-593SP](#).

Figure 3: A Framework for Managing Fraud Risks in Federal Programs



Source: GAO. | GAO-24-105470

Accessible Data for Figure 3: A Framework for Managing Fraud Risks in Federal Programs

Component 1: Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.

- Demonstrate a senior-level commitment to combat fraud, and involve all levels of the program in setting an antifraud tone.
- Designate an entity within the program office to lead fraud risk management activities.
- Ensure the entity has defined responsibilities and the necessary authority to serve its role.

Component 2: Plan regular fraud risk assessments, and assess risks to determine a fraud risk profile.

- Tailor the fraud risk assessment to the program, and involve relevant stakeholders.
- Assess the likelihood and impact of fraud risks, and determine risk tolerance.
- Examine the suitability of existing controls, prioritize residual risks, and document a fraud risk profile.

Component 3: Design and implement a strategy with specific control activities to mitigate assessed fraud risks, and collaborate to help ensure effective implementation.

- Develop, document, and communicate an antifraud strategy, focusing on preventive control activities.
- Consider the benefits and costs of controls to prevent and detect potential fraud, and develop a fraud response plan.
- Establish collaborative relationships with stakeholders and create incentives to help ensure effective implementation of the antifraud strategy.

Component 4: Evaluate outcomes using a risk-based approach, and adapt activities to improve fraud risk management.

- Conduct risk-based monitoring and evaluation of fraud risk management activities, with a focus on outcome measurement.
- Collect and analyze data from reporting mechanisms and instances of detected fraud for real-time monitoring of fraud trends.
- Use the results of monitoring, evaluations, and investigations to improve fraud prevention, detection, and response.

Source: GAO. | GAO-24-105470

As required under the Fraud Reduction and Data Analytics Act of 2015 and its successor provisions in the Payment Integrity Information Act of 2019, the leading practices in GAO's Fraud Risk Framework are incorporated into the Office of Management and Budget's (OMB) guidelines for agency controls.²⁹ Specifically, OMB's Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, directs executive agencies, including SBA and SBIR/STTR participating agencies, to adhere to the Fraud Risk Framework's leading practices as part of their efforts to effectively design, implement, and operate an internal

²⁹The Fraud Reduction and Data Analytics Act of 2015, enacted in June 2016, required OMB to establish guidelines for federal agencies to create controls to identify and assess fraud risks and to design and implement antifraud control activities. Pub. L. No. 114-186, 130 Stat. 546 (2016). The Fraud Reduction and Data Analytics Act of 2015 was replaced in March 2020 by the Payment Integrity Information Act of 2019, which required these guidelines to remain in effect, subject to modification by OMB, as necessary, and in consultation with GAO. Pub. L. No. 116-117, § 2(a), 134 Stat. 113, 131 - 132 (2020), codified at 31 U.S.C. § 3357.

control system that addresses fraud risks.³⁰ Among other things, the guidance also directs agencies to use the Federal Internal Control Standards—which include requirements for considering the potential for fraud when identifying, analyzing, and responding to risks—to annually evaluate the effectiveness of internal controls.³¹

The Fraud Risk Framework acknowledges that agencies may have other efforts to manage program risks, such as enterprise risk management efforts that may be incorporated into, or aligned with, such activities. However, this does not eliminate the need for separate and independent fraud risk management efforts, such as fraud risk assessment processes. In October 2022, OMB issued a Controller Alert that clarified the distinction between requirements to establish fraud-related financial and administrative controls and Enterprise Risk Management to ensure that fraud risks are appropriately managed. The Controller Alert reminds agencies that they should adhere to leading practices in GAO’s Fraud Risk Management Framework as part of their efforts to effectively design, implement, and operate an internal control system that addresses fraud risks, including fraud risks that do not rise to the level of enterprise-wide risks.³² Therefore, all programs, regardless of their improper payment risks or rates, should be strategically managing their fraud risks.

SBA, Participating Agencies, and OIGs Share Responsibilities to Prevent Fraud, Waste, and Abuse in the SBIR/STTR Programs

The SBA’s and participating agencies’ SBIR/STTR fraud risk management requirements, broader enterprise risk management requirements, and directives ensure that program and payment integrity and appropriate systems of internal control are in place to reduce vulnerability to fraud, waste, and abuse. Fraud prevention guidance and efforts can also help to reduce potential waste and abuse. According to the Fraud Risk Framework, to effectively prevent and detect instances of potential fraud, managers are to take steps to verify reported information, particularly self-reported data, and other key data necessary to determine eligibility for enrolling in programs or receiving benefits.³³ For example, if an applicant reports that it is a small business in order to receive federal contracts, an agency can use third-party data sources to verify that the applicant actually meets requirements to qualify as a small business, thereby reducing the risk of fraud, waste, and abuse.

In addition to requiring SBA to issue guidance through its Policy Directive, the Small Business Act, as amended, requires that SBA maintain a database that lists any individual or small business that has been convicted of a fraud-related crime or found civilly liable for a fraud-related violation involving funding received under SBIR/STTR programs.³⁴ The SBA’s Policy Directive requires participating agencies to provide notice to

³⁰Office of Management and Budget, *Management’s Responsibility for Enterprise Risk Management and Internal Control*, [OMB Circular A-123](#) (Washington, D.C.: July 15, 2016).

³¹[GAO-14-704G](#).

³²The Controller Alert also reminds agencies that the dollar thresholds established in 31 U.S.C. § 3352 for “significant” improper payments are for the purposes of improper payment reporting and not for managing fraud risks, pursuant to 31 U.S.C. § 3357. Office of Management and Budget, *Establishing Financial and Administrative Controls to Identify and Assess Fraud Risk*, CA-23-03 (Washington, D.C.: Oct. 17, 2022).

³³[GAO-15-593SP](#).

³⁴15 U.S.C. § 638(k)(2)(G).

SBA of any case or controversy before any federal judicial or administrative tribunal concerning the SBIR or STTR programs within 15 business days of the agency's written notification from the adjudicative body.³⁵

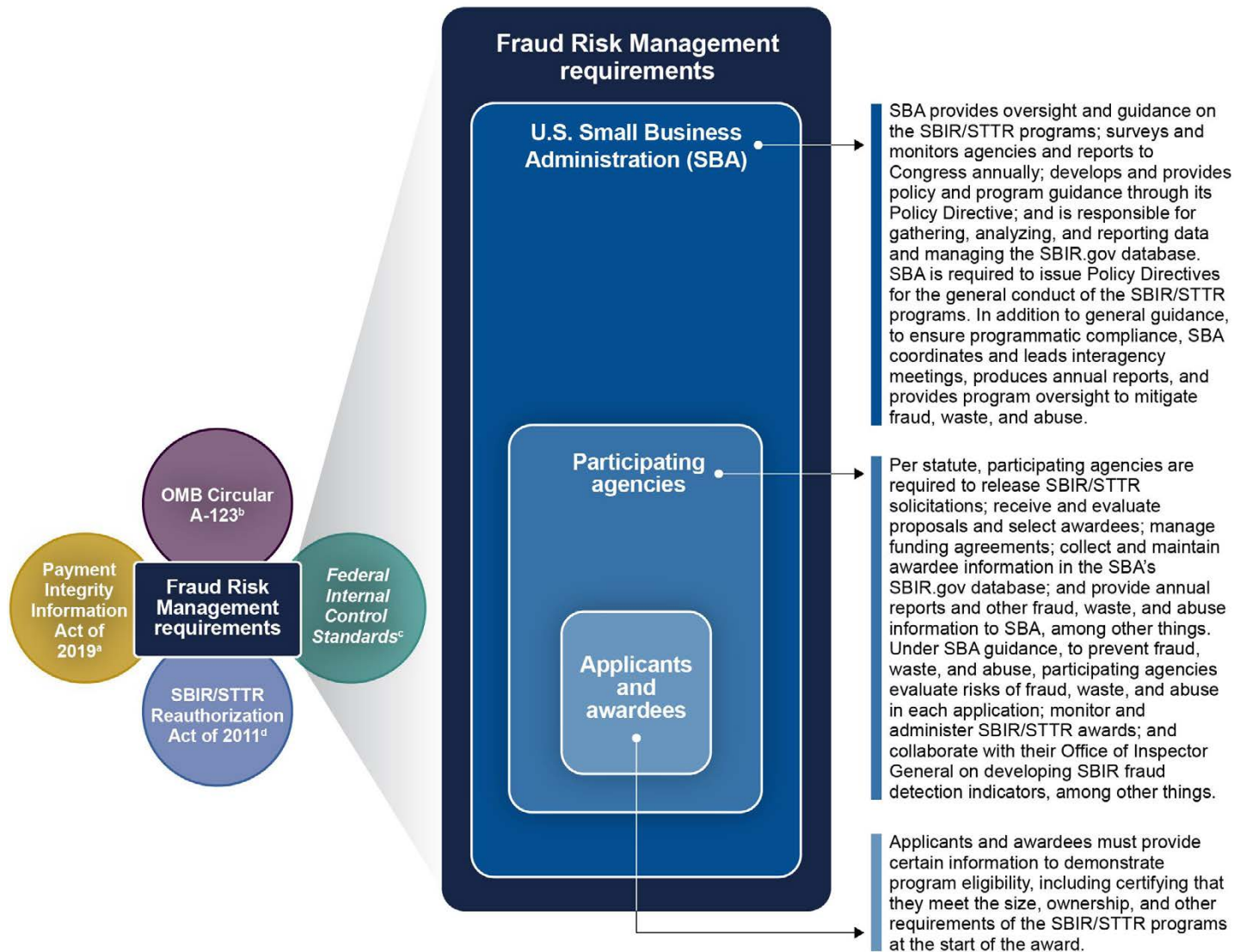
Participating agencies are required to follow the SBA's Policy Directive to ensure that applicants and awardees use the SBA's SBIR.gov website to enroll into the programs and meet program eligibility requirements related to principal investigators and the facilities where research is conducted, among others.³⁶ For example, the SBA's Policy Directive requires that the principal investigator's primary employment—more than half their time based on a 40-hour work week—be with the applicant's small business or research institution (for STTR only) at the time of, and during the performance of, the award. The Policy Directive further requires that SBIR/STTR research and development work be performed in the United States.

See figure 4 for the SBIR/STTR programs' fraud risk management requirements.

³⁵According to SBA officials, controversies are broader than items related to fraud, waste, and abuse and could include notifications related to protests or other SBIR/STTR matters before the agency.

³⁶The principal investigator is the individual designated by the applicant to provide the scientific and technical direction to a project supported by the funding agreement.

Figure 4: Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Program Fraud Risk Management Requirements



Source: GAO analysis of laws, standards, and SBA's Policy Directive. | GAO-24-105470

Accessible Data for Figure 4: Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Program Fraud Risk Management Requirements

Payment Integrity Information Act of 2019^a

OMB Circular A-123^b

Federal Internal Control Standards^c

SBIR/STTR Reauthorization Act of 2011^d

Fraud Risk Management requirements

- U.S. Small Business Administration (SBA):
SBA provides oversight and guidance on the SBIR/STTR programs; surveys and monitors agencies and reports to Congress annually; develops and provides policy and program guidance through its Policy Directive; and is responsible for gathering, analyzing, and reporting data and managing the SBIR.gov database. SBA is required to issue Policy Directives for the general conduct of the SBIR/STTR programs. In addition to general guidance, to ensure programmatic compliance, SBA coordinates and leads interagency meetings, produces annual reports, and provides program oversight to mitigate fraud, waste, and abuse.
- Participating agencies:
Per statute, participating agencies are required to release SBIR/STTR solicitations; receive and evaluate proposals and select awardees; manage funding agreements; collect and maintain awardee information in the SBA's SBIR.gov database; and provide annual reports and other fraud, waste, and abuse information to SBA, among other things. Under SBA guidance, to prevent fraud, waste, and abuse, participating agencies evaluate risks of fraud, waste, and abuse in each application; monitor and administer SBIR/STTR awards; and collaborate with their Office of Inspector General on developing SBIR fraud detection indicators, among other things.
- Applicants and awardees:
Applicants and awardees must provide certain information to demonstrate program eligibility, including certifying that they meet the size, ownership, and other requirements of the SBIR/STTR programs at the start of the award.

Source: GAO analysis of laws, standards, and SBA's Policy Directive. | GAO-24-105470

^aThe Payment Integrity Information Act of 2019 requires Office of Management and Budget (OMB) guidelines to remain in effect for federal agencies to create controls to identify and assess fraud risks and to design and implement antifraud control activities, subject to modification by OMB, as necessary, and in consultation with GAO. Pub. L. No. 116-117, § 2(a), 134 Stat. 113, 131 - 132 (2020), codified at 31 U.S.C. § 3357.

^bThe OMB's *Management's Responsibility for Enterprise Risk Management and Internal Control* (OMB Circular A-123) includes the guidelines for agencies to create controls.

^cGAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014) sets the standards for an effective internal control system for federal agencies.

^dThe SBIR/STTR Reauthorization Act of 2011 required SBA to add fraud, waste, and abuse prevention requirements to its guidance, the SBIR/STTR Policy Directive. Pub. L. No. 112-81, Div. E, Title LI, § 5143, 125 Stat. 1298, 1854 (2011), codified at 15 U.S.C. § 638b.

OIGs share responsibilities with participating agencies to prevent and detect fraud, waste, and abuse in their agencies' programs and operations. In addition to requiring the conduction and supervision of audits, inspections, and investigations, the Small Business Act, as amended, includes requirements for participating agencies' OIGs to prevent fraud, waste, and abuse in the SBIR/STTR programs. For example, OIGs must cooperate in fraud prevention activities, including establishing fraud detection indicators and improving the education and training of, and outreach to, SBIR/STTR officials, applicants, and awardees.

Fraud Schemes Demonstrate SBIR/STTR Control Vulnerabilities and Fraud Risks

Our analysis of 37 SBIR/STTR fraud schemes demonstrates the programs' control vulnerabilities and fraud risks by illustrating the role of misrepresentation in facilitating fraud. Our analysis also identified a range of financial and nonfinancial impacts of SBIR/STTR fraud.

SBIR/STTR Fraud Schemes Involved Various Alleged or Adjudicated Misrepresentations

We identified 37 fraud schemes targeting the SBIR/STTR programs that resulted in criminal, civil, and administrative actions during fiscal years 2016 through 2023.³⁷ The SBIR/STTR fraud schemes involved various falsehoods. These included alleged or adjudicated misrepresentation of employees' and businesses' eligibility to participate in SBIR/STTR projects, the costs associated with the projects, and the facilities used to complete the work.³⁸ The individual and business participants made, or were alleged to have made, these misrepresentations at various points in the award process, such as in proposals, invoices, and financial statements. Specifically, of the 37 schemes,³⁹

- twenty-three related to misrepresentation of businesses' or individuals' eligibility to participate in SBIR/STTR projects, of which 12 resulted in criminal convictions. For example, some schemes that resulted in convictions involved misrepresentations of businesses' financial health and compliance with financial management requirements, principal investigators' education and professional backgrounds and the extent to which they actually performed principal investigator duties, and whether employees conducting sensitive SBIR/STTR research were U.S. citizens or permanent residents when required under the award terms;
- twelve related to billing manipulation, of which six resulted in criminal convictions. For example, some schemes that resulted in convictions involved participants submitting inflated invoices and invoices for personal or otherwise ineligible purchases; and
- seven related to misrepresentation of the facilities used to complete SBIR/STTR projects, of which five resulted in criminal convictions. For example, in some schemes that resulted in convictions, participants

³⁷For our analysis, a fraud scheme is defined as alleged or adjudicated illegal conduct involving misrepresentation carried out against the SBIR or STTR programs using one or more processes, techniques, or systems for profit or other gain. We used the GAO Conceptual Fraud Model to conduct thematic analyses of information from the alleged or adjudicated cases to identify fraud schemes. The definitions provided in the Conceptual Fraud Model and used in this report are tailored to our specific purpose and context. Accordingly, it is possible that these terms may be used in other sources, including other GAO products, with alternative definitions. We identified fraud schemes by analyzing publicly available criminal, civil, and administrative actions initiated or resolved during fiscal years 2016 through 2023. Thus, our results do not reflect any of the at least 471 SBIR-related fraud, waste, and abuse investigations opened by OIGs and military investigative offices since late 2009 that have not resulted in publicly reported criminal, civil, or administrative cases.

³⁸As previously discussed, the SBA's Policy Directive requires that the principal investigator's primary employment be with the applicant's small business or research institution (for STTR only) at the time of, and during the performance of, the award. The Policy Directive also requires that SBIR/STTR research and development work be performed in the United States.

³⁹As discussed later in this report, some schemes resulted in more than one type of outcome. Thus, the schemes resulting in criminal convictions that we discuss in the bullets below may have also resulted in other outcomes, such as civil settlements without admissions of liability or exclusions.

attested that SBIR/STTR projects would be completed in the United States, when, in fact, the work was performed in other countries.

See text box for an illustrative example.

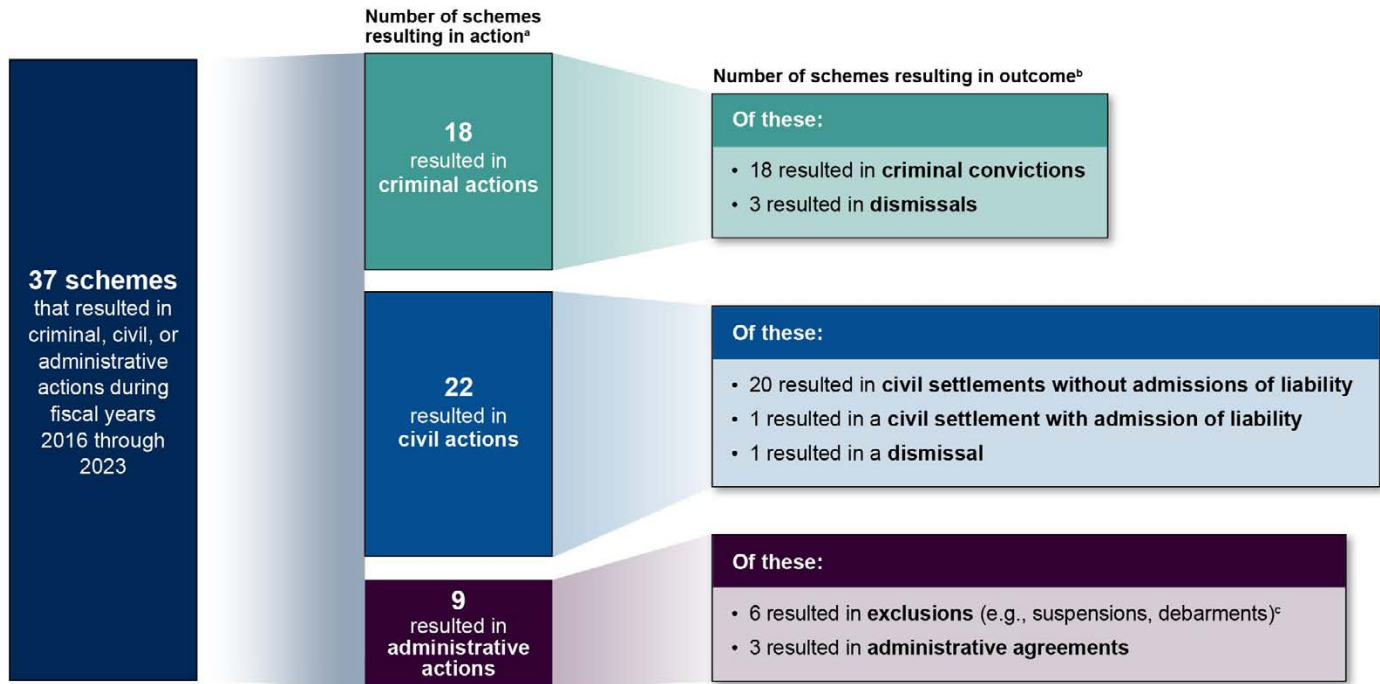
Two companies and their owner misrepresented business and employee eligibility, facilities, and billing to receive seven Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) awards. An individual and his two businesses made various misrepresentations to obtain seven SBIR and STTR awards from the U.S. Department of the Army, U.S. Department of the Air Force, Defense Advanced Research Projects Agency, Missile Defense Agency, the National Aeronautics and Space Administration, and U.S. Department of Energy. For example, the individual and businesses misrepresented one business's ability to complete work under the awards by submitting letters that made it appear that the second business had committed significant funding to support the work, without disclosing that the individual owned both businesses and that the purported funding would come from other fraudulently obtained SBIR and STTR award payments. Further, the individual repeatedly certified that U.S. citizens or permanent residents would perform all work in support of the awards at facilities in the United States, as was required, given the sensitivity of the research. In reality, the individual subcontracted work to engineers in Venezuela, to whom they granted access to U.S. government computers and software. After using these unauthorized, lower-cost personnel in support of the awards, the individual and businesses kept funds allocated in award agreements for employee salaries and consulting fees. The individual pleaded guilty to aiding and abetting computer access without authorization and was sentenced to 32 months in prison and 1 year of supervised release. The two businesses—the business that received the awards and the business that purportedly committed funding to support the work—each pleaded guilty to conspiracy to commit wire fraud and were placed on probation for 3 years. The three defendants were ordered to pay a total of \$2.9 million in restitution.

Source: GAO analysis of the U.S. Department of Justice, court, and participating agency documents. | GAO-24-105470

DOJ and participating agencies responded to these fraud schemes through criminal, civil, and administrative actions.⁴⁰ These actions had various outcomes. Some schemes resulted in multiple actions (e.g., two or more criminal cases) and multiple outcomes (e.g., two or more criminal convictions). Similarly, some schemes resulted in more than one type of action (e.g., both one or more criminal cases and one or more civil actions) and more than one type of outcome (e.g., criminal convictions of some defendants and dismissal of criminal charges against others) (see fig. 5).

⁴⁰“Civil actions” include both civil claims adjudicated in court and settlements to which the participants agreed out of court, such as civil settlements without admissions of liability.

Figure 5: Small Business Innovation Research and Small Business Technology Transfer Fraud Schemes Based on Actions Reported, Fiscal Years 2016 through 2023



Sources: GAO analysis of U.S. Department of Justice and Small Business Innovation Research and Small Business Technology Transfer participating agency information; court documents. | GAO-24-105470

Accessible Data for Figure 5: Small Business Innovation Research and Small Business Technology Transfer Fraud Schemes Based on Actions Reported, Fiscal Years 2016 through 2023

37 schemes that resulted in criminal, civil, or administrative actions during fiscal years 2016 through 2023

Number of schemes resulting in action ^a	Number of schemes resulting in outcome ^b
18 resulted in criminal actions	Of these: 18 resulted in criminal convictions 3 resulted in dismissals
22 resulted in civil actions	Of these: 20 resulted in civil settlements without admissions of liability 1 resulted in a civil settlement with admission of liability. 1 resulted in a dismissal
9 resulted in administrative actions	Of these: 6 resulted in exclusions (e.g., suspension, debarments) ^c 3 resulted in administrative agreements.

Sources: GAO analysis of U.S. Department of Justice and Small Business Innovation Research and Small Business Technology Transfer participating agency information; court documents. | GAO-24-105470

^aSome schemes resulted in more than one action, so the numbers of schemes resulting in criminal, civil, and administrative actions add up to more than the 37 total schemes we identified.

^bSome schemes resulted in more than one type of outcome, so the numbers of schemes resulting in each type of criminal, civil, or administrative outcome add up to more than the total numbers of schemes resulting in criminal, civil, or administrative actions.

^cAn excluded party is any individual or entity that has been suspended or debarred from doing business with federal funds. If an individual or entity has been debarred, they are generally banned from doing business with the federal government for a period that generally does not exceed 3 years. If an

individual or entity has been suspended, they generally cannot do business with the federal government during the duration of legal or debarment proceedings, or if proceedings have not commenced, generally not more than 12 months.

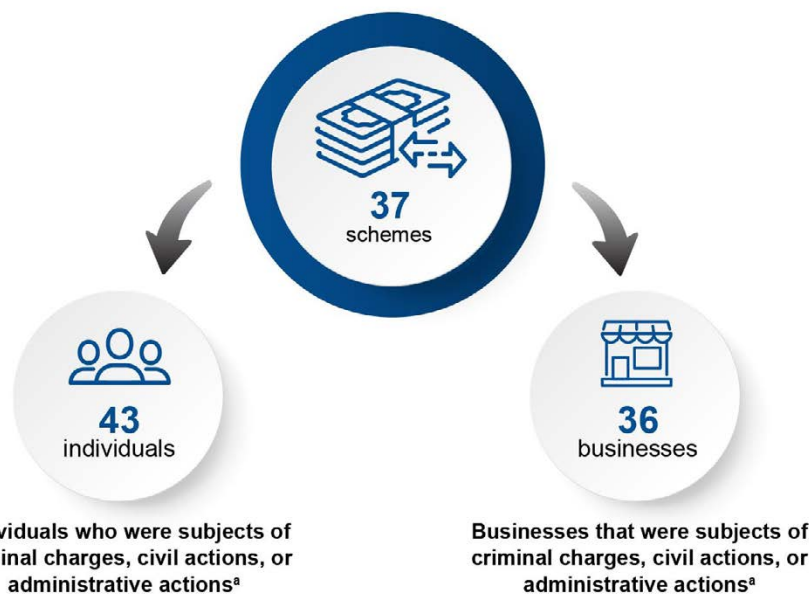
The criminal and civil violations alleged by DOJ when responding to these schemes further reflect the role of misrepresentation and falsification in SBIR/STTR fraud. Specifically, of the 18 schemes involving at least one criminal case, 13 resulted in wire fraud charges, and four resulted in false statements charges. Of the 22 schemes involving at least one civil case, 20 resulted in allegations of civil False Claims Act violations.⁴¹

Fraud Scheme Participants and Their Targets Demonstrate Vulnerabilities of SBIR/STTR

The participants, awarding agencies, programs, and award types involved in these 37 fraud schemes demonstrate the SBIR/STTR programs' vulnerability to fraud. We identified individuals and businesses that participated in SBIR/STTR fraud schemes, some of which involved multiple participants (see fig. 6).

Figure 6: Individuals and Businesses Associated with Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Fraud Schemes, Based on Actions Reported, Fiscal Years 2016 through 2023

Our analysis identified 37 Small Business Innovation Research and Small Business Technology Transfer fraud schemes, as of October 2023



Sources: GAO analysis of U.S. Department of Justice and SBIR/STTR participating agency information; court documents; enotmaks/stock.adobe.com (icons). | GAO-24-105470

⁴¹The False Claims Act is an antifraud statute providing that any person who knowingly submits, or causes the submission of, false claims for government funds or property is liable for damages and penalties.

Accessible Data for Figure 6: Individuals and Businesses Associated with Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Fraud Schemes, Based on Actions Reported, Fiscal Years 2016 through 2023

Our analysis identified 37 Small Business Innovation Research and Small Business Technology Transfer Program fraud schemes, as of October 2023

- 37 schemes
- 43 individuals: Individuals who were subjects of criminal charges, civil actions, or administrative actions^a
- 36 businesses: Businesses that were subjects of criminal charges, civil actions, or administrative actions^a

Sources: GAO analysis of U.S. Department of Justice and SBIR/STTR participating agency information; court documents; enotmaks/stock.adobe.com (icons). | GAO-24-105470

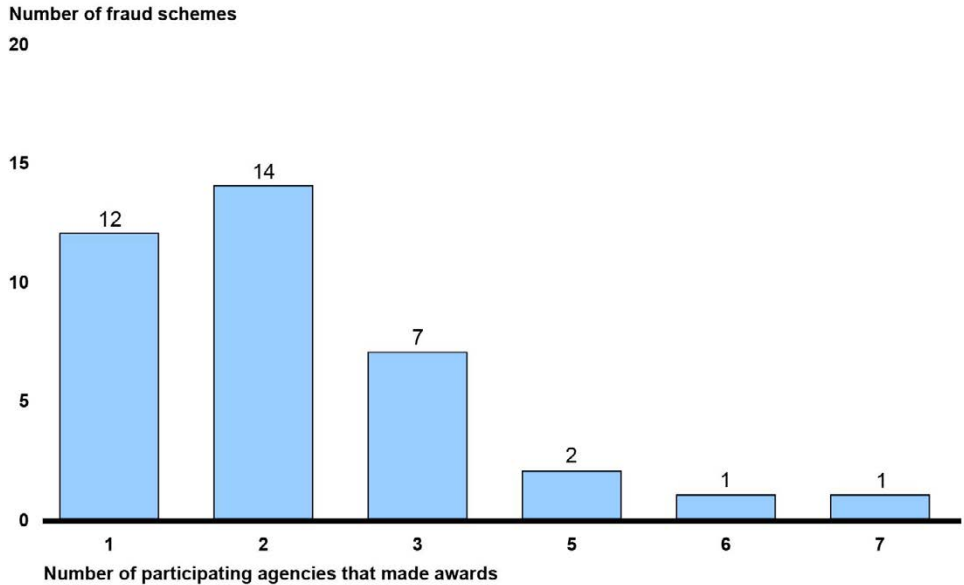
^aCivil actions include civil charges and settlements, including civil settlements with and without admissions of liability.

Scheme participants varied in number and their relationship, if any, to the SBIR/STTR programs. Specifically, 12 of the 37 schemes we identified involved two or more individuals, and four involved two or more businesses, possibly suggesting coordinated efforts to defraud the SBIR/STTR programs. Relatedly, prosecutors filed conspiracy-related charges in response to seven schemes. Further, business participants included both applicants and awardees of SBIR/STTR funds and businesses that were not applicants or awardees (such as entities that were parents of, or investors in, applicants or awardees).⁴² Similarly, individual participants included owners, officers, principal investigators, and other employees of applicant, awardee, and nonapplicant or awardee businesses.

Some fraud schemes involved multiple participating agencies, programs, and award types. Specifically, the 37 schemes involved awards from nine participating agencies. We did not identify schemes involving Commerce or Education. The number of schemes involving awards from each participating agency depends on a variety of factors, including how often fraudsters target each agency and the effectiveness of agencies' control activities at identifying SBIR/STTR fraud schemes. Twenty-five schemes involved awards from more than one participating agency (see fig. 7). For example, in one scheme that occurred from 2008 through at least 2016, an SBIR/STTR awardee stole award funds for personal use, forged letters of support for their business, and misrepresented their employees' education and experience in proposals to seven different participating agencies and subcomponents.

⁴²An applicant is the organizational entity (business) that qualifies as a small business concern and submits a contract proposal, grant application, or cooperative agreement for a funding agreement under the SBIR/STTR programs. An awardee is the business that receives a SBIR/STTR award.

Figure 7: Fraud Schemes Involving Awards from Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Participating Agencies, Fiscal Years 2016 through 2023



Sources: GAO analysis of U.S. Department of Justice and SBIR/STTR participating agency information; court documents. | GAO-24-105470

Accessible Data for Figure 7: Fraud Schemes Involving Awards from Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Participating Agencies, Fiscal Years 2016 through 2023

Number of participating agencies that made awards	Number of fraud schemes
1	12
2	14
3	7
5	2
6	1
7	1

Sources: GAO analysis of U.S. Department of Justice and SBIR/STTR participating agency information; court documents. | GAO-24-105470

Further, 14 fraud schemes involved both SBIR and STTR awards, and nine involved both contracts and grants. Scheme participants sometimes committed, or were alleged to have committed, similar fraudulent conduct with respect to the different awarding agencies, programs, and award types involved (see text box for an illustrative example).

An individual and three businesses obtained Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) contracts and grants for essentially equivalent work from the U.S. National Science Foundation (NSF), the National Aeronautics and Space Administration (NASA), and U.S. Department of Energy (DOE). An individual and three businesses applied for and received over \$1 million in SBIR and STTR grants and contracts from NSF, NASA, and DOE on behalf of four related businesses. These awards were for essentially equivalent work, and the individual and businesses concealed from each participating agency the existence of the other agencies' awards and the relationships between the businesses. In proposals for each award, the individual and businesses represented that each business had distinct facilities, equipment, and operations. In reality, the businesses shared a common facility and resources. The individual and businesses further misrepresented in each proposal, among other things, costs, employees, and the eligibility of their principal investigators to perform work under the awards. In criminal proceedings, the individual pleaded guilty to wire fraud, and the three businesses pleaded guilty to conspiracy to commit wire fraud. The individual was sentenced to 2 years of probation and, along with the three businesses, ordered to pay over \$1 million in restitution. In addition, the individual, the three businesses, and the businesses' principals agreed to pay over \$600,000 pursuant to a civil settlement without admission of liability.

Source: GAO analysis of the U.S. Department of Justice, court, and participating agency documents. | GAO-24-105470

Fraud Schemes Have Financial and Nonfinancial Impacts

We identified financial and nonfinancial impacts associated with the 37 SBIR and STTR fraud schemes. The range and magnitude of these impacts demonstrate the importance of fraud prevention to avoid costly and far-reaching impacts of the “pay-and-chase” approach to managing fraud risks.⁴³

We analyzed reported financial impacts, including restitution, forfeitures, and fines associated with criminal convictions, and settlement amounts associated with civil settlements with and without admissions of liability. These figures do not account for all the financial impacts of adjudicated SBIR/STTR fraud schemes, such as detection, investigation, and prosecution costs; the costs of negotiating civil settlements and administrative agreements; or the costs of SBIR/STTR funds going to ineligible awardees. Further, the full extent of fraud is difficult to measure because some fraud schemes may remain undetected by the government, and others may not ever be adjudicated.⁴⁴

Restitution: Courts ordered restitution in response to 13 of 37 schemes, for a total of about \$17.5 million in restitution.

Forfeitures: Courts ordered cash forfeitures in response to seven of 37 schemes, for a total of \$7.5 million in cash forfeitures. Beyond cash forfeitures, we identified three schemes in response to which courts ordered forfeitures of noncash assets. For example, in one scheme, the court ordered the fraudsters to forfeit properties, a vehicle, and jewelry. In another scheme, the court ordered the fraudster to forfeit any property used, or intended to be used, to commit the fraudulent conduct.

Fines: Courts ordered criminal defendants to pay fines for seven schemes. The fines ranged from \$1,000 to \$175,000, for a total of over \$300,000.

⁴³“Pay-and-chase” refers to the practice of detecting fraudulent transactions and attempting to recover funds after payments have been made. The Fraud Risk Framework describes “pay-and-chase” as a costly and inefficient model.

⁴⁴Direct measures of undetected fraud, by definition, do not exist, and direct measures of fraud and potential fraud are incomplete or unreliable. GAO recently developed an estimate of fraud across the federal government—a projection or inference based on fraud or fraud-related measures, assumptions, or analytical techniques—because of these limitations with measures and undetected fraud. See GAO, *Fraud Risk Management: 2018-2022 Data Show Federal Government Loses an Estimated \$233 Billion to \$521 Billion Annually to Fraud, Based on Various Risk Environments*, [GAO-24-105833](#) (Washington, D.C.: Apr. 16, 2024).

Civil settlements: We identified approximately \$34.7 million in civil settlements. Of these, about \$28 million resulted from civil settlements without admissions of liability, and about \$6.5 million resulted from civil settlements with admissions of liability.

Our analysis also identified various types of nonfinancial impacts of SBIR/STTR fraud schemes on businesses, individuals, and the federal government. These nonfinancial impacts included those affecting the SBIR/STTR programs’ economic stimulus goals and impacts on fraudsters, among others. See table 2.

Table 2: Nonfinancial Impacts of Fraud in Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs

Nonfinancial impact type	Affected parties and impact
Economic stimulus goal	Federal government’s ability to achieve SBIR/STTR program goals
Stakeholder	Resource commitments by law enforcement for responding to SBIR/STTR fraud
Health and security	Ability of participating agencies with a public health and national security focus to advance their mission; potential inappropriate or unauthorized exposure of sensitive information
Reputational	U.S. government institutions distrusted by the public
Impact on victim	Universities, employees, researchers, and students harmed by SBIR/STTR fraud schemes
Impact on fraudster	Consequences that participants in SBIR/STTR fraud schemes suffered after being caught

Sources: GAO analysis of GAO’s Conceptual Fraud Model; International Public Sector Fraud Forum; U.S. Department of Justice; and SBIR/STTR participating agency documentation. | GAO-24-105470

Among the examples of nonfinancial impacts of SBIR/STTR fraud schemes, two areas are notable, given (1) the program’s goals for stimulating technological innovation, small business development, and meeting federal research and development needs; and (2) the academic or professional standing of those typically involved in these schemes. See appendix II for information regarding other nonfinancial impacts of SBIR/STTR fraud schemes.

Economic Stimulus Goal Impact

Fraudsters’ diversion of funds from the SBIR/STTR programs affect the extent to which these programs achieve economic stimulus goals. For example, in one scheme, fraudsters did not hire consultants and employees named in proposals and failed to make promised investments. As a result, they were unable to complete SBIR/STTR projects according to proposed time frames, limiting the programs’ effectiveness at stimulating technological innovation, meeting federal research and development needs, and achieving other program goals.

Further, funds diverted by scheme participants were unavailable to eligible businesses. For example, in three schemes, participants were alleged to have misrepresented the sizes of their companies, potentially depriving eligible small business concerns of opportunities to pursue research under the programs. Also, some scheme participants redirected or allegedly redirected award funds from intended purposes for their own benefit. Specifically, 13 of the 37 schemes we reviewed involved asset misappropriation. In schemes that resulted in convictions, participants used these misappropriated funds for mortgage payments; to purchase vehicles and

international travel; and to cover personal charges at hospitals, department stores, gun ranges, opera houses, and cruise ships.

Impact on Fraudster

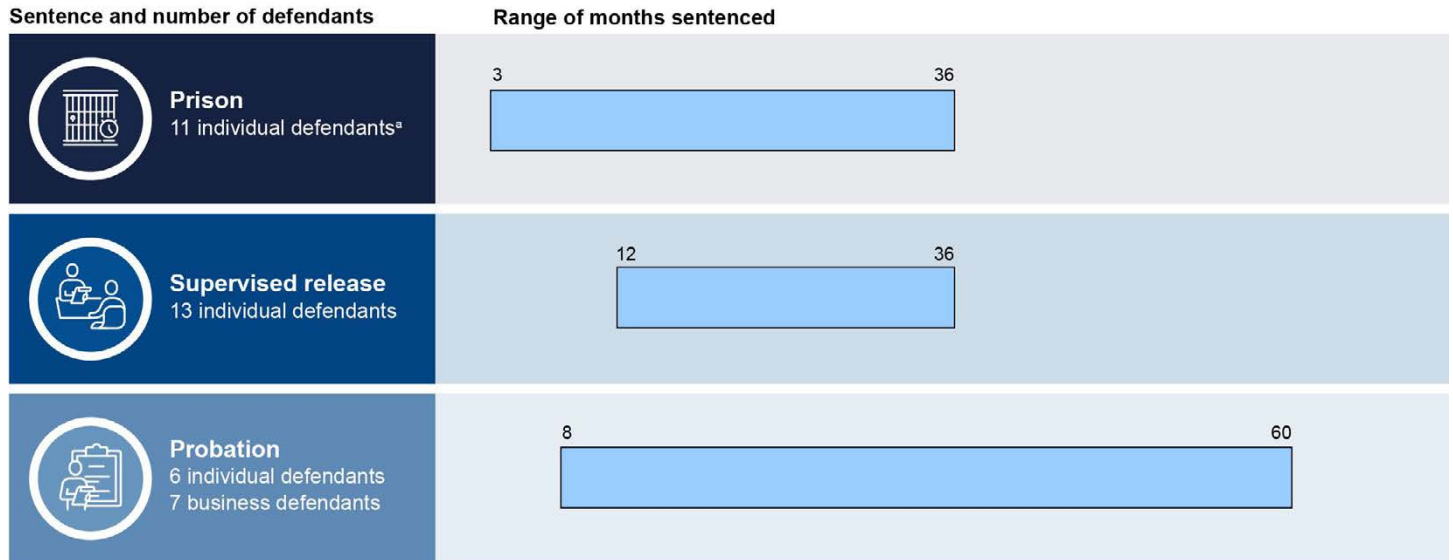
When committing a crime, fraudsters may experience a sense of satisfaction from illicit enrichment. Once caught, however, they can experience prison time, financial penalties, loss of employment, and unfavorable publicity.⁴⁵ For example, one couple—a well-respected university professor of electrical engineering and a scientist with a Ph.D. in nonlinear optics and optoelectronics—was convicted of wire fraud related to misrepresentations in proposals they submitted for NASA SBIR awards. They were sentenced to prison and ordered to pay fines and restitution. Similarly, another fraudster who pleaded guilty to wire fraud in furtherance of a scheme to fraudulently obtain NSF SBIR awards was barred from doing business with the federal government for 3 years and resigned their position as a tenured university professor.

Some SBIR and STTR fraud schemes resulted in fraudsters losing personal freedom. Specifically, our analysis identified 18 schemes that resulted in at least one criminal action where individuals or businesses were sentenced to prison, supervised release, or probation. Across these actions, 11 individuals had been sentenced to prison, cumulatively sentenced to serving over 148 months, with an average sentence of about 13 months. Two additional schemes resulted in two individuals being sentenced to time served.⁴⁶ Thirteen individuals were sentenced to a cumulative 312 months of supervised release, with an average term of 24 months. Thirteen individuals and businesses were sentenced to a cumulative 440 months of probation, with an average term of about 34 months. See figure 8 for information on sentencing ranges for defendants sentenced to prison, probation, and supervised release.

⁴⁵We have previously reported that the possibility of such punishment can deter would-be fraudsters. See [GAO-15-593SP](#).

⁴⁶A time served sentence is when a defendant is sentenced to the same term of imprisonment that the defendant is credited with serving while in custody awaiting trial. The sentence results in the defendant's release from custody.

Figure 8: Sentencing Outcomes and Ranges for Criminal Defendants in Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Fraud Schemes, Fiscal Years 2016 through 2023



Sources: GAO analysis of U.S. Department of Justice and SBIR/STTR participating agency information; court documents; enotmaks/stock.adobe.com (icons). | GAO-24-105470

Accessible Data for Figure 8: Sentencing Outcomes and Ranges for Criminal Defendants in Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Fraud Schemes, Fiscal Years 2016 through 2023

Sentence and number of defendants	Range of months sentenced
Prison 11 individual defendants ^a	3 – 36
Supervised release 13 individual defendants	12 – 36
Probation 6 individual defendants 7 business defendants	8 – 60

Sources: GAO analysis of U.S. Department of Justice and SBIR/STTR participating agency information; court documents; enotmaks/stock.adobe.com (icons). | GAO-24-105470

^aTwo additional individual defendants were sentenced to time served. A time served sentence is when a defendant is sentenced to the same term of imprisonment that the defendant is credited with serving while in custody awaiting trial. The sentence results in the defendant's release from custody.

SBA Can Better Leverage Oversight Mechanisms for Fraud, Waste, and Abuse Prevention and Ensure All Agencies Have Training in Place

SBA uses a variety of oversight mechanisms to support its mandated fraud, waste, and abuse prevention requirements. For example, in addition to issuing Policy Directive guidance, SBA uses information from monthly program manager meetings and an annual survey of participating agencies to monitor agencies' alignment with requirements to prevent fraud, waste, and abuse in the SBIR/STTR programs. Further, as a fraud deterrence mechanism and information source on program risk for participating agencies, SBA maintains a list of SBIR/STTR fraud convictions and findings of civil liability on the SBIR.gov website that some agencies use to support their requirement to report successful prosecutions. Yet SBA had not identified all such cases,

and some participating agencies were unaware of the requirement to report, or had challenges reporting, information on fraud convictions and civil liabilities to SBA. In addition, per the Policy Directive, most participating agencies have processes to ensure that program officials, applicants, and awardees receive fraud, waste, and abuse training, according to agency officials. However, we found that two participating agencies did not have processes in place to ensure such training, as required. Both agencies had provided information in the SBA's annual survey regarding compliance with these training requirements, but SBA had not followed up on the responses. SBA has opportunities to leverage its existing oversight mechanisms to ensure the accuracy of agencies' survey responses and reported compliance with fraud, waste, and abuse training requirements from the Policy Directive.

SBA Uses Various Tools to Support Its Fraud, Waste, and Abuse Prevention Requirements, but One Tool for Fraud Deterrence Has Limitations

SBA's SBIR/STTR Oversight Mechanisms Include Its Policy Directive, Program Manager Meetings, Annual Survey, and Website of Program Fraud Cases

The Small Business Act, as amended, required that SBA add fraud, waste, and abuse prevention requirements to its Policy Directive, which it did with the inclusion of the 10 minimum requirements.⁴⁷ Although not as comprehensive as the leading practices in the Fraud Risk Framework, the Policy Directive and the 10 minimum requirements are consistent with the Fraud Risk Framework's goals for strategic fraud risk management. In our comparison of the 10 minimum requirements and other guidance in the Policy Directive with the Fraud Risk Framework's leading practices, we identified areas where they were directly complimentary and areas where the Policy Directive did not speak to specific leading practices. For example, the Policy Directive aligns with the component 3 leading practice to refer instances of fraud to the OIG, but it does not require agencies to conduct program-level fraud risk assessments, among other actions, consistent with component 2 leading practices. See appendix III for additional details.

SBA is required to monitor the operation of SBIR and STTR programs within participating agencies.⁴⁸ It does so through its monthly program manager meetings, the annual survey of participating agencies, and its listing of fraud cases on its SBIR.gov website.

Monthly program manager meetings. To monitor participating agencies' implementation of the 10 minimum requirements and support continual program improvement, SBA's Office of Investment and Innovation convenes the program manager meetings. According to SBA officials, the program manager meetings maintain a standing item on fraud, waste, and abuse and discuss fraud, waste, and abuse lessons learned or best practices that agencies may choose to consider, among other things. SBA holds these peer-driven discussions monthly and invites an official from every agency to attend.

Annual survey. Beginning in fiscal year 2018, SBA has required participating agencies to complete a survey that provides information on the implementation status of each of the 10 minimum fraud, waste,

⁴⁷15 U.S.C. § 638b(a).

⁴⁸15 U.S.C. § 638(b)(6).

and abuse requirements.⁴⁹ According to SBA officials, the survey of the 10 minimum fraud, waste, and abuse requirements is part of their monitoring and program oversight efforts, and they discuss survey responses with the agencies on an individual, ad hoc basis.

Website of fraud cases. The Small Business Act, as amended, also requires SBA to develop and maintain a database that lists any individual or small business concern that has been convicted of a fraud-related crime or found civilly liable for a fraud-related violation involving funding received under SBIR/ STTR programs.⁵⁰ To meet this requirement, SBA maintains a list of instances of fraud on its SBIR.gov website. According to SBA officials, the purpose of this requirement is to deter SBIR/STTR fraud and support participating agencies' requirement to post successful prosecutions of fraud, waste, and abuse in the programs on their SBIR/STTR web page. The Policy Directive's fourth minimum requirement also directs agencies to include information concerning successful prosecutions of fraud, waste, and abuse in the programs on their SBIR/STTR web page.⁵¹ The majority (eight of 11) of participating agencies have a link to the SBIR.gov website to meet this requirement. In March 2021, SBA began sharing new instances of fraud with agencies during program manager meetings, according to SBA officials.⁵²

SBA's Website Highlights SBIR/STTR Fraud Cases as a Deterrence Mechanism, but Information Gaps Limit Its Utility

As discussed in the Fraud Risk Framework, the likelihood that individuals who engage in fraud will be identified and punished serves to deter others from engaging in fraudulent behavior. SBA's website highlighting SBIR/STTR fraud cases reflects this principle. However, we found that SBIR.gov listed most, but not all, of the individuals and businesses associated with the fraud schemes we identified in our review of criminal, civil, and administrative actions during fiscal years 2016 through 2023, limiting the website's utility for fraud deterrence.

⁴⁹According to SBA officials, before fiscal year 2018, SBA relied on the program managers' meetings, rather than annual report responses, to obtain information from the participating agencies about the program, as required by the Small Business Act, as amended. The survey asks questions regarding the agencies' implementation of the Policy Directive's 10 minimum requirements, among other things, on an annual basis and requests agencies to provide explanations for responses or documentation, as appropriate. Each agency participating in the SBIR/STTR programs must respond using standardized templates that SBA provides and maintains on SBIR.gov. SBA reviews agencies' responses to the fraud, waste, and abuse sections as a component of SBA oversight efforts, according to officials.

⁵⁰15 U.S.C. § 638(k)(2)(G).

⁵¹The Policy Directive requires that participating agencies include information concerning successful prosecutions of fraud, waste, and abuse in the programs on the agency's SBIR/STTR web page. For the purposes of this report, a successful prosecution of fraud is a case that was adjudicated favorably for the United States; criminal cases in which the subjects were found guilty, pled guilty, or pled no contest to at least one of the charges; and civil cases that resulted in a judgment for the United States, or a settlement.

⁵²According to SBA officials, SBA provides updates on new cases that are incorporated into SBIR.gov. According to SBA program manager meeting slides, SBA discussed the instances of fraud within the SBIR.gov website, including the number of instances, outcomes, and information that may be useful for training and awareness purposes (e.g., falsifying proposal information). These instances were discussed in March 2021, December 2021, and August 2023.

Some of these fraud schemes resulted in civil settlements without admissions of liability.⁵³ Specifically, as of May 2023, the website listed 30 of the 37 schemes we identified. Seven schemes were missing in full, or in part, from the website. For example, two fully missing schemes resulted in guilty pleas by one business and two individuals to false statements charges. In December 2023, SBA added a DOJ press release regarding one of these fully missing schemes to the website in response to our inquiry and did not take action on the other six.

One partially missing scheme resulted in two criminal cases (each against a separate individual defendant) and two civil cases (each against one of the individual defendants and one or more businesses). Both criminal cases resulted in guilty pleas, and both civil cases resulted in civil settlements. Although SBIR.gov listed the criminal and civil cases involving one of the defendants, it did not list the criminal and civil cases involving the other defendants. As of May 2024, the website did not list the missing information regarding this partially missing scheme and the other five schemes.

SBA uses two methods to obtain information for the website, both of which have limitations. First, SBA uses publicly available information (i.e., results from quarterly internet searches, notifications of DOJ press releases, and reviews of OIG websites and semiannual reports) to identify convictions and findings of civil liability associated with the SBIR/STTR programs. According to SBA officials, they primarily check DOJ's website to update the list of SBIR/STTR fraud cases on SBIR.gov. SBA officials stated that this process is repeatable, consistent, and manageable and that posting such instances online by year is sufficient for capturing information as a deterrent to fraud, waste, and abuse.

This methodology has some limitations, however, as not all instances of convictions and settlement agreements pursued by DOJ have an associated press release. Of the seven missing schemes we identified involving additional individuals and businesses that were convicted, or that were parties to civil settlements, four had DOJ press releases but three did not. Resources such as legal research databases and legal news sites, which we used to identify SBIR/STTR convictions and findings of civil liability, provide a more robust way of monitoring press releases, through custom alerts, as well as news coverage on new and ongoing cases. Using such resources would allow SBA to enhance its ability to identify additional information on convictions and findings of civil liability to populate its website—and thus enhance the effect of this fraud-deterrence tool.

The second method that SBA uses to obtain information for its web page is through participating agencies. The SBA's Policy Directive requires participating agencies to provide notice to SBA of any case or controversy before any federal judicial or administrative tribunal concerning the SBIR/STTR program within 15 business days of the agency receiving written notification of the case or controversy from the adjudicative body. According to SBA officials, controversies are broader than items related to fraud, waste, and abuse and could include notifications related to bid protests or other SBIR/STTR matters before the agency.

However, we found that most agencies with SBIR/STTR fraud convictions and findings of civil liability did not report them to SBA, despite the requirement existing in the Policy Directive. Specifically, we found that most

⁵³While SBA is not required to report settlements in which there is no admission of liability, its website reports these types of cases. In this report, a fraud scheme is alleged or adjudicated illegal conduct involving misrepresentation carried out against the SBIR or STTR programs using one or more processes, techniques, or systems for profit or other gain. We could not identify DOJ press releases containing information for three schemes, given that not all cases pursued by DOJ have an associated press release. To identify SBIR/STTR schemes, we received alerts through subscriptions to the Westlaw and Law360 (legal news services) website to identify DOJ press releases and other information. For identified schemes, we obtained relevant court documents by searching Public Access to Court Electronic Records.

(nine of 11) agencies were the awarding agencies in the 37 schemes we identified from fiscal years 2016 through 2023 (described earlier in this report).⁵⁴ Yet four of the nine awarding agencies were unaware of the requirement to report cases and controversies to SBA. For example, we identified 13 schemes where DOE was the awarding agency in our review of SBIR/STTR fraud schemes, but one DOE subcomponent was not aware of the reporting requirement until our inquiry in November 2023.

In addition, most (eight of 11) participating agencies and subcomponents identified challenges in complying with the requirement to report any case or controversy within 15 business days of the agency receiving written notification. Officials with these agencies cited challenges related to the confidential nature of investigations, working with the OIG to identify cases, and meeting the 15-day requirement to report cases to SBA, among others. For example, NASA officials noted the need for clarity from SBA officials on what types of matters they envision will be reported regarding judicial and administrative tribunals. One DOE subcomponent noted that this requirement would best be addressed by the OIG because the OIG carries out investigations and has knowledge of cases brought before a federal judicial or administrative tribunal.

The SBA's oversight mechanisms are designed to address challenges that agencies experience in meeting Policy Directive requirements. For example, the purpose of the program manager meetings is to share information and ensure compliance with Policy Directive requirements. SBA's program manager meetings include a standing item to discuss fraud, waste, and abuse. However, SBA has not discussed the requirement to provide notification to SBA of a case or controversy during the meetings. According to SBA officials, the Policy Directive clearly identifies agencies' need to report cases and controversies. SBA officials also noted that they have not held such a discussion because they have not received requests from agencies to clarify this long-standing Policy Directive requirement.⁵⁵ Nevertheless, agencies reported these challenges, and we identified related gaps in reporting.

According to SBA officials, it is their understanding that the list of cases on the SBA's website was not meant to be exhaustive. However, as noted earlier, agencies use the web page to meet the Policy Directive's fourth minimum requirement. Further, most (eight of 11) agency officials told us that they use the website to obtain information about fraud, waste, and abuse in the SBIR/STTR programs. For example, officials from three of 11 agencies stated that they use the SBA's website when identifying and assessing program vulnerabilities, as well as informing and adapting fraud risk management efforts. Agencies' use of the website for fraud risk management, as well as its intended purpose for deterrence, points to the website's utility and the importance of keeping it as current and comprehensive as possible. Without as comprehensive a case listing as possible, the website's utility to agencies for fraud risk management and as a fraud deterrent is diminished. The SBA's program manager meeting discussions provide an appropriate opportunity to address these challenges—for agencies to share information and report on cases and for SBA to address participating agencies' challenges in understanding and meeting the 15-day reporting requirement.

⁵⁴We did not identify schemes related to Commerce or Education.

⁵⁵According to SBA officials, this statutory requirement has been legislated since 2012.

Most Participating Agencies Have Processes to Ensure Program Officials, Applicants, and Awardees Receive Required Fraud, Waste, and Abuse Training

The SBA's Policy Directive minimum requirement eight requires participating agencies to work with their OIGs to improve education and training of SBIR/STTR program officials, applicants, and awardees on issues related to fraud, waste, and abuse.⁵⁶ SBA collects agencies' responses regarding the status of their training efforts and actions on the other nine minimum requirements in its annual survey.

Fraud Risk Framework Component 1

Create an organizational culture and structure to combat fraud



Source: GAO. | GAO-24-105470

The Fraud Risk Framework's component 1 identifies training as one way of demonstrating an agency's commitment to combating fraud. Training and education are intended to increase fraud awareness among stakeholders (e.g., applicants and awardees) and managers serves as a preventive measure to support compliance within the program.

Most participating agencies have processes to ensure that program officials, applicants, and awardees receive fraud, waste, and abuse training, according to the SBA's survey responses, documentation, and our interviews with agency officials. Specifically, 10 of 11 participating agencies' fiscal year 2022 survey responses to SBA reported that they worked with their OIGs to improve training of program officials, applicants, and awardees.⁵⁷

However, we found that not all participating agencies had training processes for applicants and officials. For example, although USDA officials responded "yes" to the SBA survey question pertaining to training, according to documentation and our interviews with agency officials, we found that USDA trained officials and awardees but not applicants. According to USDA officials, they include information in the request for applications about how to report fraud, waste, and abuse and have information posted on its SBIR website, as required by the Policy Directive. However, USDA officials acknowledged that they do not currently train applicants about the definitions of fraud, waste, and abuse and the possible consequences of engaging in such activity. According to USDA officials, because they provide training to program awardees, they reasoned that any SBIR applicants

⁵⁶A program official manages or coordinates the SBIR/STTR program of the participating agency. An applicant is the organizational entity (business) that qualifies as a small business concern and submits a proposal or application for a contract, grant, or cooperative agreement for a funding agreement under the SBIR/STTR programs. An awardee is the business that receives a SBIR/STTR award.

⁵⁷As of September 2023, fiscal year 2022 was the most recent year of available survey responses. According to SBA officials, fiscal year 2023 survey responses would be collected in March 2024.

would also receive training. Therefore, USDA is not providing required training to applicants before they apply and awards are made. In April 2024, USDA officials noted that they would consult with SBA to obtain additional guidance regarding requirements to train potential applicants and will evaluate options for providing training to applicants after getting input from SBA regarding expectations and best practices.

According to USDA officials, they consulted with SBA regarding the requirement to train applicants on fraud, waste, and abuse. According to USDA officials, SBA advised them that each agency should address the matter individually because the needs for applicant training in fraud, waste, and abuse vary by agency. In response, USDA officials noted that they will work with their OIG and also review the fraud, waste, and abuse training that other SBIR/STTR programs provide to applicants.

We also found that although DOD requires applicants to review SBA's fraud, waste, and abuse tutorial on the SBIR.gov website and provide a training completion certificate in their proposal, DOD responded "no" to this SBA survey question in fiscal year 2022. Further, the extent to which DOD subcomponent program officials received training and provided training to awardees varied. According to DOD subcomponent officials,

- four of 13 DOD subcomponent program officials did not participate in fraud, waste, and abuse training;
- ten of 13 DOD subcomponent program officials did not provide fraud, waste, and abuse training to awardees; and
- twelve of 13 DOD subcomponents did not coordinate with OIGs to improve awardee training.

In a December 2023 response to our inquiries, the DOD's Office of the Under Secretary of Defense for Research and Engineering officials, the office that administers DOD's SBIR/STTR program, stated that they intend to implement a fraud, waste, and abuse module in DOD's SBIR/STTR Innovation Portal.⁵⁸ They have a goal of deploying and implementing the module for applicants and awardees in 2025.⁵⁹ Additionally, they were considering holding a webinar for SBIR/STTR applicants and awardees that would include a fraud, waste, and abuse section. In April 2024, DOD officials noted that, when implemented, the DOD SBIR/STTR Innovation Portal's fraud, waste, and abuse module will address the Policy Directive's eighth minimum requirement to provide fraud, waste, and abuse training to applicants and awardees. However, the officials did not state that the portal will be used for program official fraud, waste, and abuse training.

According to SBA officials, they provide clear guidance to agencies, including indicating they should only answer "yes" if training for officials, applicants, and awardees is executed. They also discuss agencies' survey responses with the agencies on an individual, ad hoc basis as part of their oversight efforts, according to SBA officials. However, according to SBA officials, SBA did not follow up with USDA or DOD officials regarding their survey responses to ensure that the Policy Directive requirement was being met. SBA officials received the USDA's survey response in which USDA's National Institute of Food and Agriculture officials, the institute that administers the USDA's SBIR/STTR program, noted that only the program's officials were trained but did not provide evidence of training for applicants or awardees.⁶⁰ SBA did not inquire, for example, either individually

⁵⁸DOD's SBIR/STTR Innovation Portal is the official website for DOD SBIR/STTR proposal submission.

⁵⁹According to the Policy Directive, participating agencies may use up to 3 percent of their SBIR budget for one or more specific activities, including oversight and fraud, waste, and abuse prevention. Participating agencies must submit a work plan to SBA at least 30 calendar days prior to the start of each fiscal year for which the pilot program is in operation.

⁶⁰In August 2024, USDA officials told us that they provide training to awardees during the New Awardee Webinar. During these webinars, the USDA OIG provides fraud, waste, and abuse training to awardees, according to officials.

or through the monthly program manager meetings, why USDA had taken that approach. Similarly, SBA officials did not follow up with DOD's "no" survey response to the training requirement, which DOD has consistently reported from fiscal years 2019 through 2022.

Both USDA and DOD have made recent efforts to attract new applicants and awardees to the programs. For example, USDA began implementing the STTR program as of fiscal year 2023, and DOD has ongoing efforts to attract awardees new to the program.⁶¹ Without fraud, waste, and abuse training, managers, applicants, and awardees new to the program, or dealing with a program new to the agency, may not be familiar with requirements for managing SBIR/STTR fraud, waste, and abuse, increasing the vulnerability to these risks. SBA is in a position to leverage its oversight mechanisms to better ensure that all program participants understand their responsibilities to prevent fraud, waste, and abuse, as intended by Policy Directive guidance. Specifically, the SBA's annual survey to agencies is designed to provide SBA with information to identify gaps in agencies' compliance with training requirements, while the monthly program manager meetings provide a venue to discuss and assure the accuracy of those responses and redress compliance concerns.

Some Agency Efforts Partially Align with Leading Practices for Fraud Risk Assessment, and SBA Guidance Could Improve Agencies' Alignment to Support SBIR/STTR Fraud Prevention Requirements

Participating agencies conducted various activities to assess SBIR/STTR fraud risks, but none reflect a comprehensive assessment that aligns with leading practices from the Fraud Risk Framework. As noted earlier, the Policy Directive and the 10 minimum requirements are consistent with the Fraud Risk Framework's goals for strategic fraud risk management.

The second component of the Fraud Risk Framework calls for federal managers to plan regular fraud risk assessments and assess risks to determine a fraud risk profile.⁶² Specifically, leading practices include tailoring fraud risk assessments to the program, planning to conduct assessments at regular intervals, and involving relevant stakeholders responsible for the design and implementation of fraud controls.

⁶¹In September 2023, we reported that DOD subcomponents have planned a variety of approaches to attract new applicants. [GAO-23-106338](#).

⁶²As discussed in the Fraud Risk Framework, a fraud risk profile is the summation of effectively assessing fraud risks. The profile includes the analysis of the types of internal and external fraud risks facing the program, their perceived likelihood and impact, managers' risk tolerance, and the prioritization of risks. It is the basis of an overall antifraud strategy that informs the design and implementation of specific fraud control activities and should also include managers' risk tolerance and prioritization, among other things. [GAO-15-593SP](#).

Fraud Risk Framework Component 2

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



Source: GAO. | GAO-24-105470

In conducting a comprehensive fraud risk assessment, key elements include (1) identifying inherent fraud risks affecting the program, (2) assessing the likelihood and impact of inherent fraud risks, (3) determining fraud risk tolerance, (4) examining the suitability of existing fraud controls and prioritizing residual fraud risks, and (5) documenting the program’s fraud risk profile.⁶³ Robust inherent fraud risk identification helps to ensure that fraud risks are managed appropriately. Further, leading practices direct managers to involve relevant stakeholders and identify specific sources for gathering information about fraud risks, including data on fraud schemes and trends from monitoring and detection activities.

Most participating agencies (eight of 11) did not assess SBIR/STTR program fraud risks independently or as part of fraud risk assessments for grants, contracts, or cooperative agreements. Instead, these agencies relied on enterprise risk management, internal controls, and other processes for SBIR/STTR fraud risk assessment purposes. While these broader processes are supportive of fraud risk management generally, they are not a replacement for program-level fraud risk assessments, even if one or more SBIR/STTR fraud risks are reflected in them. Some officials from these agencies noted challenges related to a lack of guidance, training, and resources with respect to conducting program-specific fraud assessments. As discussed later in this report, for the three participating agencies that conducted SBIR/STTR-specific fraud risk assessments, we found opportunities for improving the comprehensiveness of these assessments.

Most Participating Agencies Do Not Conduct Program-Specific Fraud Risk Assessments, and SBA Guidance Could Improve Awareness of This Requirement















We found that most participating agencies (eight of 11) do not conduct SBIR/STTR-specific fraud risk assessments, as called for in the Fraud Risk Framework component 2. Instead, seven of these agencies reported that they leverage enterprise-wide and other risk management efforts that consider fraud concerns for

⁶³According to Federal Internal Control Standards, risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. [GAO-14-704G](#). 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. Additionally, managers consider the extent to which existing control activities mitigate the likelihood and impact of inherent risks and whether the remaining risks exceed managers’ tolerance. The risk that remains after inherent risks have been mitigated by existing control activities is called residual risk. [GAO-15-593SP](#).

grants, contracts, or cooperative agreements generally for their SBIR/STTR programs.⁶⁴ One participating agency—the Environmental Protection Agency (EPA)—indicated that it does not perform SBIR fraud risk assessments and is not aware of any enterprise-wide fraud risk reporting requirements. According to EPA officials, SBIR is a small program and noted limited staff and budget as challenges to conducting fraud risk assessments. The three agencies that do conduct SBIR/STTR program-specific fraud risk assessments also reported that they leverage broader enterprise-wide processes for their SBIR/STTR programs. Of the 10 agencies leveraging such processes, six identified some fraud risks as relevant to SBIR/STTR programs. See figure 9.

⁶⁴Participating agencies with multiple subcomponents—Commerce, DOD, DOE, DHS, and HHS—are counted if one or more subcomponents provided a “yes” response. Thus, participating agencies are counted as having conducted an activity even though not all subcomponents may have conducted the activity in question.

Figure 9: Participating Agencies' Use of Program-Specific Fraud Risk Assessments and Enterprise Risk Management Processes for Their Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs, as of April 2023

Participating agency ^a	 Participating agency conducted SBIR/STTR fraud risk assessments	 Participating agency leveraged enterprise-wide processes	 Participating agency identified enterprise-wide fraud risks as relevant to SBIR/STTR programs
 Department of Agriculture (USDA)	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 Department of Commerce (Commerce)	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 Department of Defense (DOD)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 Department of Education (Education)	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 Department of Energy (DOE)	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 Environmental Protection Agency (EPA)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 Department of Health and Human Services (HHS)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 Department of Homeland Security (DHS)	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 National Aeronautics and Space Administration (NASA)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 National Science Foundation (NSF)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/> ^b
 Department of Transportation (DOT)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Participating agency status

- Participating agency and all subcomponents
- Participating agency or one or more subcomponent(s)
- Participating agency and subcomponents did not identify information

Sources: GAO analysis of SBIR/STTR participating agency responses and documentation; USDA, Commerce, DOD, Education, DOE, EPA, HHS, DHS, NASA, NSF, and DOT (agency seal); Icons-Studio/stock.adobe.com (icons). | GAO-24-105470

Accessible Data for Figure 9: Participating Agencies' Use of Program-Specific Fraud Risk Assessments and Enterprise Risk Management Processes for Their Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs, as of April 2023

Participating Agency^a	Participating agency conducted SBIR/STTR fraud risk assessments	Participating agency leveraged enterprise-wide processes	Participating agency identified enterprise-wide fraud risks as relevant to SBIR/STTR programs
Department of Agriculture (USDA)	Participating agency and subcomponents did not identify information	Participating agency and all subcomponents	Participating agency and all subcomponents
Department of Commerce (Commerce)	Participating agency and subcomponents did not identify information	Participating agency and all subcomponents	Participating agency and all subcomponents
Department of Defense (DOD)	Participating agency and subcomponents did not identify information	Participating agency or one or more subcomponent(s)	Participating agency or one or more subcomponent(s)
Department of Education (Education)	Participating agency and subcomponents did not identify information	Participating agency and all subcomponents	Participating agency and all subcomponents
Department of Energy (DOE)	Participating agency and all subcomponents	Participating agency and all subcomponents	Participating agency and all subcomponents
Environmental Protection Agency (EPA)	Participating agency and subcomponents did not identify information	Participating agency and subcomponents did not identify information	Participating agency and subcomponents did not identify information
Department of Health and Human Services (HHS)	Participating agency or one or more subcomponent(s)	Participating agency or one or more subcomponent(s)	Participating agency and subcomponents did not identify information
Department of Homeland Security (DHS)	Participating agency and all subcomponents	Participating agency and all subcomponents	Participating agency and all subcomponents
National Aeronautics and Space Administration (NASA)	Participating agency and subcomponents did not identify information	Participating agency or one or more subcomponent(s)	Participating agency and subcomponents did not identify information
National Science Foundation (NSF)	Participating agency and subcomponents did not identify information	Participating agency and all subcomponents	Participating agency and subcomponents did not identify information ^b
Department of Transportation (DOT)	Participating agency and subcomponents did not identify information	Participating agency or one or more subcomponent(s)	Participating agency and subcomponents did not identify information

Sources: GAO analysis of SBIR/STTR participating agency responses and documentation; USDA, Commerce, DOD, Education, DOE, EPA, HHS, DHS, NASA, NSF, and DOT (agency seal); Icons-Studio/stock.adobe.com (icons). | GAO-24-105470

^aResults include responses and documentation provided by DOD, DOE, HHS, DHS, and Commerce subcomponents. Results do not include subcomponents that started participating in the SBIR/STTR programs in 2023, as these awards are not within the scope of this audit.

^bAccording to NSF officials, NSF's 2024 Interim Fraud Report item related to duplicative funding was relevant to the SBIR/STTR program during the application process, within the proposal, and during the award period of performance.

Although they are not program-specific fraud risk assessments, participating agencies reported they leverage these broader risk management processes for grants, contracts, and cooperative agreements to manage fraud risks. Some of these processes touch specifically on SBIR/STTR program risks, while others do not. These broader processes are assessments conducted under OMB Circular No. A-123 guidelines, such as for

enterprise risk management and grant and contract payments.⁶⁵ While six of 10 participating agencies leveraging enterprise-wide processes identified some fraud risks relevant to the SBIR/STTR programs, the identified risks generally reflect “pay-and-chase” activities, such as focusing on postaward billing. See table 3 for examples of broader efforts that participating agencies leverage to manage fraud and other risks in their SBIR/STTR programs.

Table 3: Examples of Broader Efforts That Participating Agencies Leverage to Manage Small Business Innovation (SBIR) and Small Business Technology Transfer (STTR) Program Risk

Type of broader effort that participating agencies leverage to manage SBIR/STTR program risks	What we found	Examples of agency responses
Enterprise risk management processes that identify SBIR/STTR fraud risks	Three agencies—The U.S. Departments of Commerce, Agriculture (USDA), and Energy (DOE)—identified enterprise fraud risks specific to the SBIR programs. Within DOE, one of two subcomponents identified enterprise fraud risks specific to the SBIR/STTR programs, and the other did not. Five of the agencies did not identify enterprise fraud risks as relevant to the programs.	Both Commerce subcomponents’ enterprise documentation identified multiple grant projects billed for equivalent work as a fraud risk. While this fraud risk is related to the program, it is a “pay-and-chase” activity, instead of a risk-based preventative activity, as called for in the Fraud Risk Framework. ^a In March 2023, USDA added a SBIR-specific risk related to due diligence requirements to its enterprise risk profile, pursuant to new program requirements, according to program officials. ^b Not all program inherent fraud risks are included in due diligence requirements.
Enterprise risk management processes that identify fraud risks that could apply to SBIR/STTR grant and contracting processes	Five agencies—USDA, DOE, the U.S. Departments of Homeland Security, Education, and Defense (DOD)—identified one or more enterprise fraud risk relevant to the programs. Within DOD, two of seven subcomponents leveraging broader processes identified one or more enterprise fraud risks that could apply to SBIR/STTR grant and contracting processes, and five DOD subcomponents did not.	Education’s enterprise documentation identified agency employees’ conflicts of interest as a fraud risk. One DOD subcomponent’s enterprise documentation identified an applicant falsifying its qualifications to receive an award as a fraud risk. One of two DOE subcomponents identified grant financial fraud as a fraud risk. However, a program not meeting its purpose is also a nonfinancial fraud risk that should be assessed, consistent with Fraud Risk Framework leading practices.
General risk management processes applied to SBIR/STTR applicant and awardees	Several agencies noted that they use other processes, such as award screening and monitoring, to manage fraud risks associated with applicants and awardees. These efforts reflect control activities to manage individual applicant and awardee risks and, while important, are not program fraud risk assessments. ^c	The U.S. Department of Transportation and USDA conduct preaward checks in systems such as the System for Award Management. Commerce subcomponents conduct postaward improper payment checks. This is a “pay-and-chase” activity, instead of a risk-based preventative activity, consistent with Fraud Risk Framework leading practices. DOD is working to establish an SBIR/STTR due diligence program, which may assist in identifying fraud risks and processes needed to manage them.

⁶⁵We did not assess agencies’ enterprise-wide documentation against Fraud Risk Framework leading practices. The enterprise-wide documentation was outside of our audit scope. Further, they are not fraud risk assessments specific to the SBIR/STTR programs.

Source: GAO analysis of participating agency documentation. | GAO-24-105470

^a“Pay-and-chase” refers to the practice of detecting fraudulent transactions and attempting to recover funds after payments have been made.

^bThe SBIR and STTR Extension Act of 2022 (Extension Act)—enacted in September 2022—builds on actions to help agencies, universities, and businesses counter foreign influence on federally funded research by requiring each participating agency to establish and implement a due diligence program to manage these risks. We did not assess agencies’ due diligence efforts, as these requirements were promulgated after the scope of our review of awards made from fiscal years 2016 through 2021. For more information, see GAO, *Small Business Research Programs: Agencies Are Implementing Programs to Manage Foreign Risks and Plan Further Refinement*, [GAO-24-106400](#) (Washington, D.C.: Nov. 16, 2023). USDA began participating in the STTR program in fiscal year 2023; however, we did not assess its efforts, as they are outside the scope of our review.

^cAccording to Federal Internal Control Standards, control activities are the policies, procedures, techniques, and mechanisms that enforce managers’ directives to achieve the program’s objectives and address related risks. GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

The Fraud Risk Framework acknowledges that agencies may have other efforts to manage program risks, such as enterprise risk management efforts, and that fraud risk management activities may be incorporated into, or aligned with, such activities. However, this does not eliminate the need for separate and independent fraud risk assessment and management processes, as reinforced in a 2022 OMB Controller Alert.⁶⁶ The Controller Alert clarifies the distinction between requirements for fraud-related financial and administrative controls and enterprise risk management to ensure that fraud risks are appropriately managed. Further, it reminds agencies that they should adhere to leading practices in GAO’s Fraud Risk Framework to address fraud risks, even those that do not rise to the level of enterprise-wide risks and financial thresholds, regardless of their improper payment risks or rates.

Further, integrating antifraud efforts into a broader risk management and internal control approach may pose trade-offs. Leveraging enterprise risk management processes may provide a broad view of potentially aberrant behaviors, ranging from unintentional errors to sophisticated bribery or corruption schemes. These processes could inform the development of control activities that serve multiple risk management and internal functions, including fraud risk management. However, without careful planning and input from SBIR/STTR programs, integrating fraud risk management into a larger risk management and internal control approach may limit the amount of resources and attention focused specifically on fraud prevention, detection, and response.⁶⁷ Unless activities are based on a comprehensive fraud risk assessment process that includes the SBIR/STTR programs, officials cannot ensure that internal controls are appropriate to identified and prioritized program fraud risks, in alignment with Fraud Risk Framework leading practices.

Eight participating agencies noted various reasons why their agency did not conduct SBIR/STTR fraud risk assessments independently or as part of fraud risk assessments for grants, contracts, or cooperative agreements. See table 4.

⁶⁶Office of Management and Budget, Controller Alert [CA], *Establishing Financial and Administrative Controls to Identify and Assess Fraud Risk*, CA-23-03 (Washington, D.C.: Oct. 17, 2022).

⁶⁷Additionally, fraud’s deceptive nature makes it harder to detect, potentially requiring control activities that are specifically designed to prevent and detect criminal intent.

Table 4: Reasons Participating Agencies Provided for Not Conducting Small Business Innovation (SBIR) and Small Business Technology Transfer (STTR) Fraud Risk Assessments

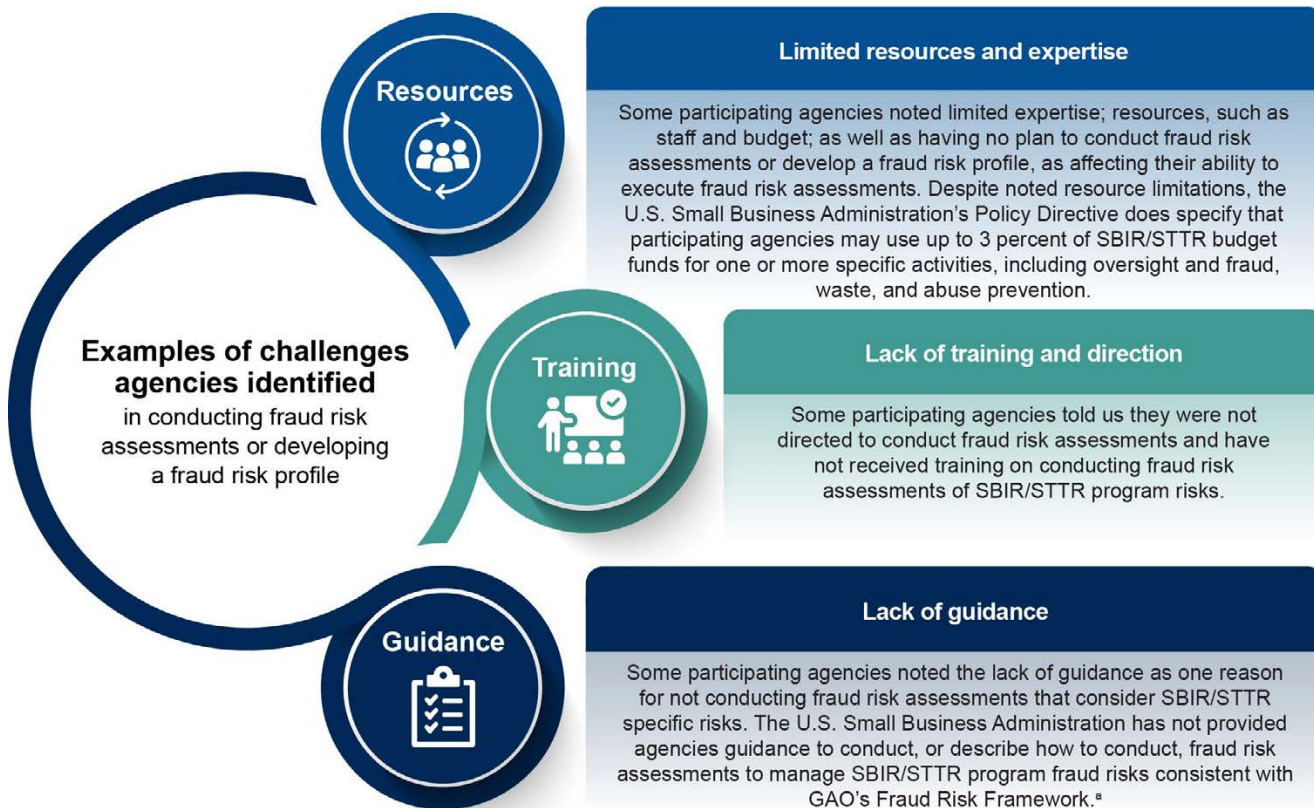
Reason for not conducting SBIR/STTR fraud risk assessments	Examples of agency responses
Lack of awareness or use of GAO's Fraud Risk Framework and related requirements to the SBIR/STTR program	Two agencies were not aware of GAO's Fraud Risk Framework and related requirements. Three agencies had not used, or considered using, GAO's Fraud Risk Framework for SBIR/STTR programs.
Broader fraud risk assessment or enterprise-wide efforts are conducted by other offices, not SBIR/STTR program offices	Six agencies noted that offices outside the SBIR/STTR program, such as the Offices of the Chief Finance Officer or Grants Management, conduct risk assessments of the grantmaking and contracting processes.
SBIR/STTR fraud risks were not incorporated into enterprise or broader risk assessments due to the program being at low risk for fraud, or not meeting financial risk assessment thresholds ^a	Three agencies' SBIR/STTR programs are not reported to the enterprise-wide level due to being historically low risk. Two agencies' SBIR/STTR programs are not included in enterprise-wide assessments due to the programs not meeting financial risk thresholds.
SBIR/STTR-specific fraud risk assessments or other risk assessment approaches are underway	One agency is coordinating internally to develop a program-specific fraud risk assessment of SBIR internal controls. As of April 2024, the agency is working with internal stakeholders and expect the fraud risk assessment to be completed in fiscal year 2025. One agency is coordinating internally to implement a fraud risk assessment process that includes SBIR/STTR programs.

Source: GAO analysis of participating agency documentation. | GAO-24-105470

^aAs described in the Office of Management and Budget's (OMB) Controller Alert, *Establishing Financial and Administrative Controls to Identify and Assess Fraud Risk*, CA [Controller Alert]-23-03 (Washington, D.C.: Oct. 17, 2022), such thresholds do not negate requirements to adhere to leading practices in GAO's Fraud Risk Framework: GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 2015).

In addition, as mentioned earlier, training and education are intended to increase fraud awareness among managers and serve as a preventive measure to support compliance within the program, according to the Fraud Risk Framework. Participating agencies noted resources, training, and guidance as examples of challenges related to conducting fraud risk assessments and developing a fraud risk profile. See figure 10.

Figure 10: Examples of Challenges Participating Agencies Identified in Conducting Small Business Innovation (SBIR) and Small Business Technology Transfer (STTR) Fraud Risk Assessments



Sources: GAO analysis of SBIR/STTR participating agency responses; Surapong/stock.adobe.com and Icons-Studio/stock.adobe.com (image). | GAO-24-105470

Accessible Data for Figure 10: Examples of Challenges Participating Agencies Identified in Conducting Small Business Innovation (SBIR) and Small Business Technology Transfer (STTR) Fraud Risk Assessments

Examples of challenges agencies identified in conducting fraud risk assessments or developing a fraud risk profile

Resources:

- Limited resources and expertise
Some participating agencies noted limited expertise; resources, such as staff and budget; as well as having no plan to conduct fraud risk assessments or develop a fraud risk profile, as affecting their ability to execute fraud risk assessments. Despite noted resource limitations, the U.S. Small Business Administration's Policy Directive does specify that participating agencies may use up to 3 percent of SBIR/STTR budget funds for one or more specific activities, including oversight and fraud, waste, and abuse prevention.

Training

- Lack of training and direction
Some participating agencies told us they were not directed to conduct fraud risk assessments and have not received training on conducting fraud risk assessments of SBIR/STTR program risks.

Guidance

- Lack of guidance
Some participating agencies noted the lack of guidance as one reason for not conducting fraud risk assessments that consider SBIR/STTR specific risks. The Small Business Administration has not provided agencies guidance to conduct, or describe how to conduct, fraud risk assessments to manage SBIR/STTR program fraud risks consistent with GAO's Fraud Risk Framework.^a

Sources: GAO analysis of SBIR/STTR participating agency responses; Surapong/stock.adobe.com and Icons-Studio/stock.adobe.com (image). | GAO-24-105470

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

Officials from five participating agencies stated that they would welcome additional guidance from SBA on the topic. According to one subcomponent's officials, they do not plan to conduct SBIR/STTR-specific assessments until further guidance is provided by the DOD's Office of the Under Secretary of Defense Research and Engineering SBIR/STTR.

SBA officials noted a variety of reasons why they had not provided guidance for conducting SBIR/STTR fraud risk assessments. For example, while SBA engages with agencies through its program manager meetings to discuss recurring fraud, waste, and abuse agenda items, officials stated that participating agencies have not made requests for guidance related to fraud risk assessment. According to SBA officials, detailed and strategic management guidance, including utilization of GAO's Fraud Risk Framework, is not a function of the Policy Directive due to the statutory framework allowing variation in agency processes. SBA officials further noted that agencies should leverage their OIGs in the fraud risk assessment processes, given the duties explicitly assigned to the OIGs under the law.⁶⁸ However, as the Fraud Risk Framework makes clear, fraud risk assessments are to be tailored to the program because of their inherent variation and are the agency's responsibility, not the OIGs.

⁶⁸SBA officials noted that the Small Business Act, as amended, requires participating agencies' OIGs to cooperate to prevent fraud, waste, and abuse in the SBIR/STTR programs by reviewing agencies' regulations and operating procedures, among other things.

SBA officials also noted that providing fraud risk assessment guidance should be the responsibility of the agency's enterprise risk management process, and directing agencies to conduct such assessments may be outside of the SBA's authority. According to SBA officials, although these broader efforts may not consider SBIR/STTR fraud risks, the agencies have all the information needed to consider such risks. While managers can leverage other efforts to manage program risks, this does not eliminate the need for separate and independent fraud risk management efforts, as reinforced in the 2022 OMB Controller Alert. Further, while we acknowledge that the Small Business Act does not direct SBA to provide detailed fraud risk assessment guidance to agencies, providing guidance in support of fraud risk management is within the SBA's authority under the law.⁶⁹ Doing so aligns with its efforts to ensure that agencies have taken steps to prevent fraud, waste, and abuse in the program.

In the absence of clarifying guidance, agencies have taken various approaches to meeting the Policy Directive's requirement to manage fraud risks. Tailored fraud risk assessments are foundational to effective management of risk. But by relying on enterprise assessments or broader risk management processes, SBA and program officials cannot be assured that they are appropriately managing SBIR/STTR fraud risks.

Three Agencies Conducted Program-Specific Fraud Risk Assessments, but SBA Guidance Could Enhance Their Comprehensiveness

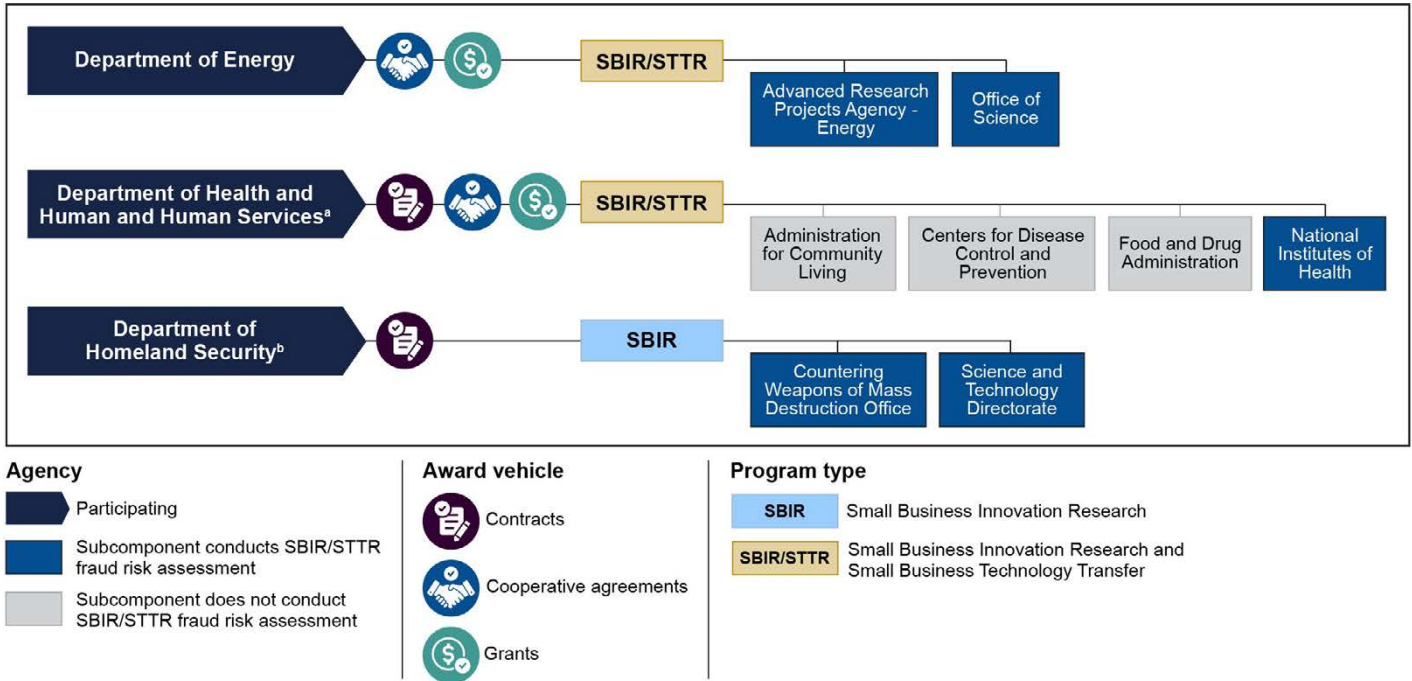
Three of the 11 participating agencies had conducted SBIR/STTR fraud risk assessments, as of April 2023.⁷⁰ Specifically, five agency subcomponents within three agencies either conducted, or contributed to, fraud risk assessments for the SBIR/STTR programs.⁷¹ See figure 11.

⁶⁹Pub. L. No. 112-81, Div. E, Title LI, § 5143, 125 Stat. 1298, 1854 (2011), codified at 15 U.S.C. § 638b.

⁷⁰We evaluated the most recent fraud risk assessments and profiles as of April 2023, according to agency officials.

⁷¹Participating agencies with multiple agency subcomponents—Commerce, DOD, DOE, DHS, and HHS—are counted, if one or more subcomponent provided a “yes” response. However, this does not mean all subcomponents conducted or contributed to fraud risk assessments.

Figure 11: Participating Agencies' Subcomponents That Conducted, or Contributed to, Program-Specific Fraud Risk Assessments, as of April 2023



Sources: GAO analysis of U.S. Department of Energy, U.S. Department of Homeland Security, and U.S. Department of Health and Human Services SBIR/STTR documentation; Icons-Studio/stock.adobe.com (icons). | GAO-24-105470

Accessible Data for Figure 11: Participating Agencies' Subcomponents That Conducted, or Contributed to, Program-Specific Fraud Risk Assessments, as of April 2023

Agency (participating)	Award vehicle	Program type	Agency (subcomponent)
Department of Energy ^a	Cooperative agreements Grants	Small Business Innovation Research and Small Business Technology Transfer	Advanced Research Projects Agency – Energy (Subcomponent conducts SBIR/STTR fraud risk assessments) Office of Science (Subcomponent conducts SBIR/STTR fraud risk assessments)
Department of Health and Human Services ^b	Contracts Cooperative agreements Grants	Small Business Innovation Research and Small Business Technology Transfer	Administration for Community Living (Subcomponent does not conduct SBIR/STTR fraud risk assessments) Centers for Disease Control and Prevention (Subcomponent does not conduct SBIR/STTR fraud risk assessments) Food and Drug Administration (Subcomponent does not conduct SBIR/STTR fraud risk assessments) National Institutes of Health (Subcomponent conducts SBIR/STTR fraud risk assessments)
Department of Homeland Security ^c	Contracts	Small Business Innovation Research	Countering Weapons of Mass Destruction Office (Subcomponent conducts SBIR/STTR fraud risk assessments) Science and Technology Directorate (Subcomponent conducts SBIR/STTR fraud risk assessments)

Sources: GAO analysis of U.S. Department of Energy, U.S. Department of Homeland Security, and U.S. Department of Health and Human Services SBIR/STTR documentation; Icons-Studio/stock.adobe.com (icons). | GAO-24-105470

^aThe U.S. Department of Health and Human Services' Centers for Disease Control and Prevention does not participate in the STTR program, according to the department's officials.

^bIn December 2023, the U.S. Department of Homeland Security's SBIR Program provided a fiscal year 2023 fraud risk assessment. We did not assess the fraud risk assessment, as it is outside the scope of our review.

We analyzed these SBIR/STTR fraud risk assessments to determine their alignment with Fraud Risk Framework leading practices.⁷² Specifically, we assessed whether they (1) used available fraud information, such as OIG fraud detection indicators and fraud schemes on SBIR.gov to identify inherent risks; and (2) included the five key elements of a comprehensive assessment described earlier.

Identifying inherent fraud risks. In conducting fraud risk assessments, the Fraud Risk Framework directs agencies to identify specific tools, methods, and sources for gathering information about fraud risks, including data on fraud schemes and trends from monitoring and detection activities. Participating agencies have access to information on fraud schemes through SBIR.gov, the SBA's monthly program manager meetings, and from the OIGs. For example, SBIR.gov identifies a wide variety of misrepresentations related to principal investigators' education and research facilities used to complete projects, among others. According to agency OIGs, they work with the participating agencies to establish fraud detection indicators to prevent fraud, waste, and abuse in the SBIR/STTR programs, as mandated. Among these indicators are risks related to business size, principal investigators, work performed, and research facilities.























Using the SBIR OIG fraud detection indicators and our Conceptual Fraud Model, which contains fraud schemes described earlier, we developed 21 fraud, waste, and abuse risk categories of inherent risks facing the programs. Some of the categories reflect specific risks, like bid rigging, bribery and kickbacks, and product substitution. Other categories reflect where the risks reside—such as with agency oversight and program compliance. Additional categories relate to misrepresentations associated with business ownership, principal investigators, research facilities, and other areas.⁷³ We evaluated agencies' use of this information when conducting the fraud risk assessment process.

In our comparison of these 21 risk categories with the inherent fraud risks identified in the three agencies' assessments, we found that one or more risks were identified in many of these categories. For example, agencies and subcomponents generally identified inherent fraud risks related to agency oversight and program compliance. Specifically, the three agencies' and the five subcomponents' documentation identified fraud risks in two categories: (1) agency oversight risks—program officials making inappropriate payments (e.g., excessive purchases of unneeded items); and (2) program compliance risks—actions taken by the awardee (e.g., performance not meeting the award purpose). However, we identified instances where the agencies did not use available fraud risk information to conduct more comprehensive SBIR/STTR fraud risk assessments. For example, although OIG fraud detection indicators and SBIR/STTR fraud scheme information related to principal investigators, research facilities, and other SBIR/STTR risks are available to program managers, these risks were not present in the fraud risk assessments and profiles we evaluated. See figure 12 illustrating the extent to which the three participating agencies' and subcomponents' documentation identified fraud risks addressing the 21 fraud, waste, or abuse categories.

⁷²We evaluated fraud risk assessments and profiles from the five subcomponents within the three participating agencies that had conducted a SBIR/STTR fraud risk assessment.

⁷³See app. IV for descriptions and examples of the 21 fraud, waste, and abuse risk categories.

Figure 12: Inherent Fraud Risks Identified in Participating Agency and Subcomponent Fraud Risk Assessments, as of April 2023

 Participating Agency and Subcomponents Identified Inherent Fraud Risks, as of April 2023		Department of Energy ^a	Department of Homeland Security ^b	Department of Health and Human Services ^c
	Agency oversight	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Affiliated firms	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Applicant employees	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Bid-rigging	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Bribery and kickbacks	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Business ownership	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Conflict of interest	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Essentially equivalent work	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Excluded parties	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Financial responsibility	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Foreign ownership	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Inappropriate billing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Misrepresentation during the award life cycle ^d	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Number of type of awards	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Poor performance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Principal investigator	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Program compliance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Product substitution	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Research facilities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Shell company	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Subcontract	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- Risk included in both agency and subcomponent assessment
- Risk included in agency or one, but not all, subcomponent assessments
- Risk not included in agency or subcomponent assessment

Sources: GAO analysis of U.S. Department of Energy, U.S. Department of Homeland Security, and U.S. Department of Health and Human Services SBIR/STTR documentation; Icons-Studio/stock.adobe.com (icons). | GAO-24-105470

Accessible Data for Figure 12: Inherent Fraud Risks Identified in Participating Agency and Subcomponent Fraud Risk Assessments, as of April 2023

Participating Agency and Subcomponents Identified Inherent Fraud Risks, as of April 2023

	Department of Energy^a	Department of Homeland Security^b	Department of Health and Human Services^c
Agency oversight	Risk included in both agency and subcomponent assessment	Risk included in both agency and subcomponent assessment	Risk included in both agency and subcomponent assessment
Affiliated firms	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment	Risk included in both agency and subcomponent assessment
Applicant employees	Risk included in agency or one, but not all, subcomponent assessments	Risk included in both agency and subcomponent assessment	Risk included in both agency and subcomponent assessment
Bid rigging	Risk included in agency or one, but not all, subcomponent assessments	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment
Bribery and kickbacks	Risk not included in agency or subcomponent assessment	Risk included in both agency and subcomponent assessment	Risk included in both agency and subcomponent assessment
Business ownership	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment
Conflict of interest	Risk not included in agency or subcomponent assessment	Risk included in both agency and subcomponent assessment	Risk included in both agency and subcomponent assessment
Essentially equivalent work	Risk not included in agency or subcomponent assessment	Risk included in both agency and subcomponent assessment	Risk included in both agency and subcomponent assessment
Excluded parties	Risk not included in agency or subcomponent assessment	Risk included in both agency and subcomponent assessment	Risk included in both agency and subcomponent assessment
Financial responsibility	Risk included in agency or one, but not all, subcomponent assessments	Risk included in both agency and subcomponent assessment	Risk not included in agency or subcomponent assessment
Foreign ownership	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment
Inappropriate billing	Risk included in agency or one, but not all, subcomponent assessments	Risk included in both agency and subcomponent assessment	Risk included in both agency and subcomponent assessment
Misrepresentation during the award life cycle ^a	Risk included in agency or one, but not all, subcomponent assessments	Risk included in agency or one, but not all, subcomponent assessments	Risk included in agency or one, but not all, subcomponent assessments
Number of type of awards	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment
Poor performance	Risk included in both agency and subcomponent assessment	Risk not included in agency or subcomponent assessment	Risk included in both agency and subcomponent assessment
Principal investigator	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment
Program compliance	Risk included in both agency and subcomponent assessment	Risk included in both agency and subcomponent assessment	Risk included in both agency and subcomponent assessment
Product substitution	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment
Research facilities	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment

	Department of Energy ^a	Department of Homeland Security ^b	Department of Health and Human Services ^c
Shell company	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment
Subcontract	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment	Risk not included in agency or subcomponent assessment

Sources: GAO analysis of U.S. Department of Energy, U.S. Department of Homeland Security, and U.S. Department of Health and Human Services SBIR/STTR documentation; Icons-Studio/stock.adobe.com (icons). | GAO-24-105470

^aWe evaluated the U.S. Department of Energy’s SBIR/STTR Advanced Research Projects Agency – Energy and Office of Science subcomponent for fraud risk profiles.

^bWe evaluated the U.S. Department of Homeland Security’s SBIR fraud risk assessment conducted by the Countering Weapons of Mass Destruction and Science and Technology subcomponents.

^cWe evaluated the U.S. Department of Health and Human Services’ National Institutes of Health’s Extramural Grant Program fraud risk profile, as SBIR/STTR officials reported information into the documentation.

^dThe misrepresentation during the award life cycle category includes four subcategories, and agencies are given partial credit if fraud risks were not identified in each. See app. IV for the full list of categories.

Elements of a comprehensive assessment. According to the Fraud Risk Framework, comprehensive fraud risk assessments include all key elements—from identification of inherent risk to documentation of the risk profile—as described earlier. In our review of the three participating agencies’ fraud risk assessments and profiles, one included all key elements of a comprehensive fraud risk assessment process, but two agencies’ risk assessment or profile did not.⁷⁴ Specifically, while DHS’ SBIR fraud risk assessment includes managers’ fraud risk tolerance and prioritization determinations, it did not document the program’s fraud risk profile. While HHS’ fraud risk profile for extramural grant programs identified and assessed the likelihood and impact of selected fraud risks, it did not include managers’ fraud risk tolerance and prioritization determinations.

According to HHS officials, the programs’ risk tolerance for the identified SBIR/STTR programs’ fraud risks was not documented because the SBA’s Policy Directive does not require them to do so. While the Policy Directive sets the general requirements for assessing applicant and monitoring awardee fraud, waste, and abuse risks, according to SBA officials, it is not designed as detailed guidance for strategic management of fraud risks in the SBIR/STTR program. For example, while the Policy Directive requires that agencies collaborate with their OIG on developing SBIR fraud detection indicators, it does not provide guidance on using the OIG fraud detection indicators to inform SBIR/STTR program fraud risk assessments. Further, it does not instruct participating agencies to follow GAO’s Fraud Risk Framework key elements for conducting a comprehensive fraud risk assessment.

Strategic fraud risk management—in alignment with the Policy Directive—includes robust identification of inherent fraud risks and a comprehensive fraud risk assessment that includes key elements such as fraud risk tolerance determinations. Without these, agencies may fail to identify and target resources to areas of greatest risk. Further, if fraud risks are not identified, they may not be managed appropriately, or at all.

As noted earlier, SBA provides guidance for participating agencies on preventing program fraud, waste, and abuse risks and implementing related Policy Directive requirements. Without guidance from SBA on how to identify, assess, and manage SBIR/STTR fraud risks, agencies are missing instruction to strategically and

⁷⁴We evaluated the presence of the key elements of a comprehensive fraud risk assessment process. We did not evaluate the quality or appropriateness of agencies’ determinations.

effectively do so. Such guidance would support agency awareness of the need to (1) conduct fraud risk assessments for SBIR/STTR programs that (2) include all elements of a comprehensive assessment, such as by using available information for robust identification of inherent fraud risks and setting a risk tolerance to prioritize cost-effective management of the most significant risks.

Participating Agencies Could Benefit from Improved Data Analytics and Data Quality to Identify Potentially Ineligible Applicants, Awardees, and Other Risks

Participating agencies vary in their use of available federal information to assess applicant eligibility and the risk of potential fraud, waste, or abuse prior to making an SBIR/STTR award. To identify vulnerabilities in these participating agencies' approaches for assessing applicant eligibility and risks, we used various databases to test five selected eligibility requirements associated with awardee information from awards made in fiscal years 2016 through 2021.⁷⁵ Specifically, we performed data testing related to (1) foreign ownership, (2) business size, (3) principal investigators, (4) essentially equivalent work, and (5) research facility addresses. We also conducted analytic tests associated with selected risk factors for fraud, waste, and abuse among the awards and associated awardees in our time frame.

We performed these tests on fiscal years 2016 through 2021 SBIR/STTR awards from SBIR.gov, which contained 38,206 awards associated with about 10,570 awardees.⁷⁶ Collectively, our analytic tests identified 842 of 10,570 awardees that were made to potentially ineligible applicants. These awardees were associated with at least four or more indications of fraud, waste, and abuse risks.⁷⁷ Our results demonstrate the benefits that participating agencies could gain from applying similar analytics. Further, we identified data quality issues in the two key SBA databases for the SBIR/STTR program relevant for agencies' full use of these analytics for managing fraud risk.

Agencies Made Awards to Potentially Ineligible Applicants and Use Various Information Sources to Identify and Assess Applicant Risks

We performed data testing for selected eligibility requirements in five areas: (1) foreign ownership, (2) business size, (3) principal investigators, (4) essentially equivalent work, and (5) research facility addresses (see fig. 13). We performed these tests on the SBIR/STTR awards from SBIR.gov, which contained 38,206 awards

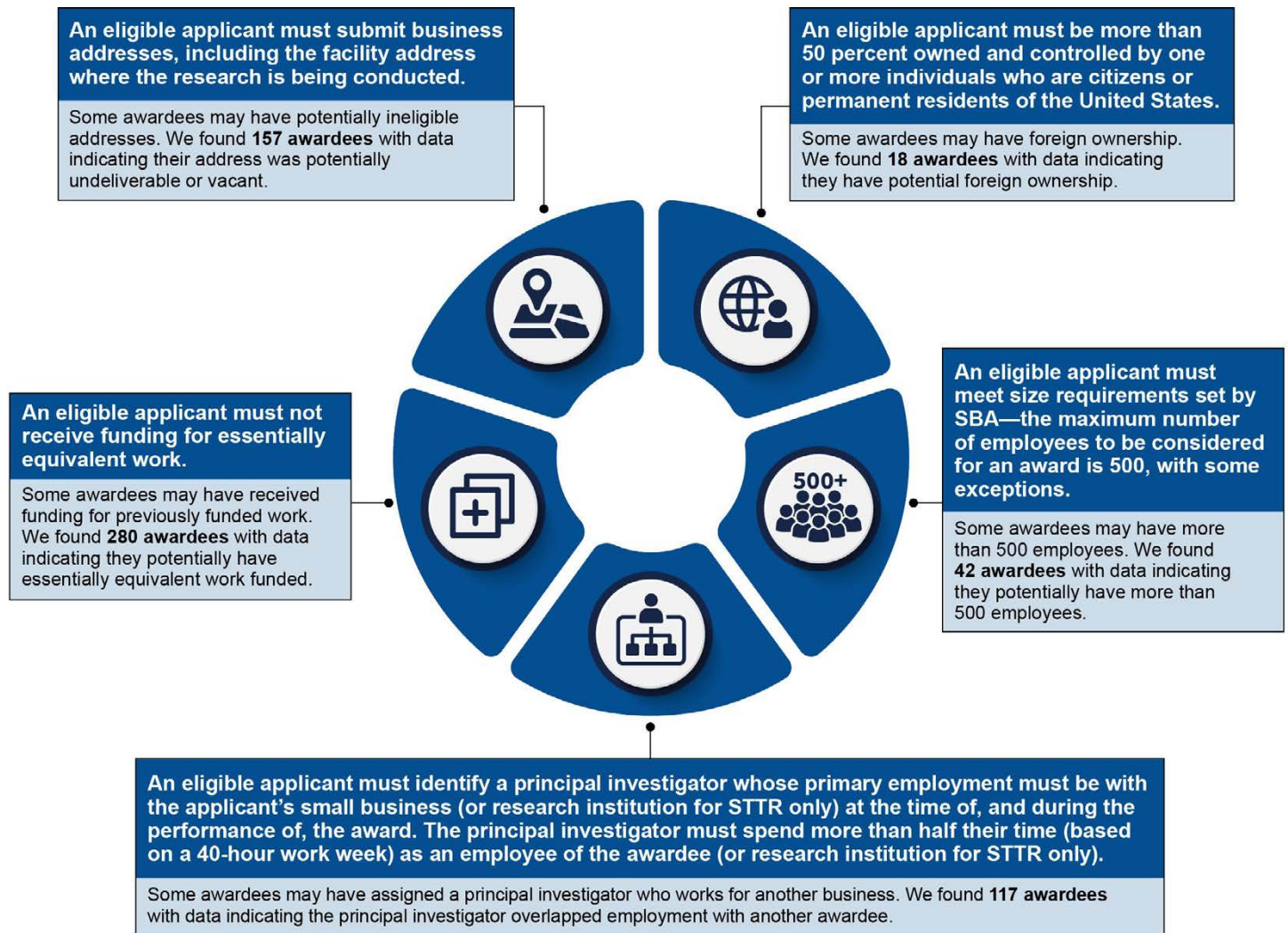
⁷⁵To be eligible for an award, an applicant must meet other requirements in addition to these five. According to the Policy Directive, an applicant is the organizational entity (business) that qualifies as a small business concern and submits a proposal or application for a contract, grant, or cooperative agreement under the SBIR/STTR programs. An awardee is the business that receives a SBIR/STTR award. In this report, we refer to an applicant as a business.

⁷⁶Due to missing and incorrect Dun & Bradstreet Data Universal Numbering System (DUNS number) values, we cleaned SBIR.gov award data to consolidate the awards by individual awardees. We identified 10,570 awardees, but the actual number may be lower or higher.

⁷⁷The Policy Directive defines an awardee as the organizational entity that receives a SBIR/STTR award. In this report, a business is a commercial operation, business, or firm. A business that receives a SBIR/STTR award is identified as an awardee.

associated with about 10,570 awardees.⁷⁸ While the results do not confirm an awardee’s ineligibility, they provide information about weaknesses in control activities and represent areas of heightened risk for fraud, waste, and abuse that may signal the need for further inquiry. Results from our analysis where we found the presence of fraud, waste, or abuse risks will result in referrals to relevant agency OIGs for further investigation.

Figure 13: Analytic Tests and Results for Selected Program Eligibility Requirements



Legend

SBA = U.S. Small Business Administration
 SBIR = Small Business Innovation Research
 STTR = Small Business Technology Transfer

Sources: GAO analysis of U.S. Small Business Administration data; Icon-Studio/stock.adobe.com (icons). | GAO-24-105470

⁷⁸SBIR.gov award data required data cleansing to consolidate the awards by individual awardees due to missing and incorrect DUNS numbers. We identified 10,570 awardees, but the true number may be lower or higher. Agencies might not be able to undertake this type of testing due to data quality limitations we describe later in the report.

Accessible Data for Figure 13: Analytic Tests and Results for Selected Program Eligibility Requirements

An eligible applicant must submit business addresses, including the facility address where the research is being conducted.

Some awardees may have potentially ineligible addresses. We found 157 awardees with data indicating their address was potentially undeliverable or vacant.

An eligible applicant must be more than 50 percent owned and controlled by one or more individuals who are citizens or permanent residents of the United States.

Some awardees may have foreign ownership. We found 18 awardees with data indicating they have potential foreign ownership.

An eligible applicant must meet size requirements set by the SBA—the maximum number of employees to be considered for an award is 500, with some exceptions.

Some awardees may have more than 500 employees. We found 42 awardees with data indicating they potentially have more than 500 employees.

An eligible applicant must identify a principal investigator whose primary employment must be with the applicant’s small business (or research institution for STTR only) at the time of, and during the performance of, the award. The principal investigator must spend more than half their time (based on a 40-hour work week) as an employee of the awardee (or research institution for STTR only).

Some awardees may have assigned a principal investigator who works for another business. We found 117 awardees with data indicating the principal investigator overlapped employment with another awardee.

An eligible applicant must not receive funding for essentially equivalent work.

Some awardees may have received funding for previously funded work. We found 280 awardees with data indicating they potentially have essentially equivalent work funded.

An eligible applicant must submit the facility address where the research is being conducted.

Some awardees may have potentially invalid facilities. We found 51 awardees with data indicating their address listed on an award is a commercial mail receiving agency in 2021.

Legend

SBA = U.S. Small Business Administration

SBIR = Small Business Innovation Research

STTR = Small Business Technology Transfer

Sources: GAO analysis of U.S. Small Business Administration data; Icon-Studio/stock.adobe.com (icons) | GAO-24-105470

To be eligible for awards, SBIR/STTR applicants must complete a business profile and annual representations and certifications in the General Services Administration’s System for Award Management registration, consistent with federal regulations.⁷⁹ For example, applicants self-report whether they are a small business,

⁷⁹The System for Award Management is the primary government repository for prospective federal awardee information and the centralized system for certain contracting, grants, and other assistance-related processes. It includes data collected from prospective federal awardees required for the conduct of business with the government; prospective contractor-submitted annual representations and certifications in accordance with FAR [Federal Acquisition Regulation] subpart 4.12; identification of those parties excluded from receiving federal contracts, subcontracts; and certain types of federal financial and nonfinancial assistance and benefits. During the scope of our review, applicants were required to have a DUNS number. As of April 4, 2022, applicants are required to have a Unique Entity Identifier (Unique Entity ID) number, which is outside the scope of our review.

socially and economically disadvantaged, under indictment, and have any present criminal or civil charges for contracts or subcontracts related to fraud, among other things.⁸⁰ Applicants also use the SBA's Company Registry within SBIR.gov to submit information and self-certify that they will meet the eligibility requirements in their proposal, upon award and throughout the award life cycle.⁸¹ For example, applicants and awardees self-certify that they (and their affiliates) meet SBIR/STTR requirements related to ownership status, business size, and convictions or civil judgments.

In addition to the SBA's Policy Directive, which requires that agencies evaluate the risks of fraud, waste, and abuse in each application, participating agencies told us that they use other regulations to review applicant risks. For example, agency officials said that they follow the Federal Acquisition Regulation (FAR) and Code of Federal Regulations (C.F.R.). These regulations require agencies to assess applicant risk by reviewing government-wide data, including information on eligibility or financial integrity when awarding grants, contracts, and cooperative agreements. For instance, an applicant cannot receive an award while suspended or debarred from federal procurement and nonprocurement transactions, unless the designated agency official determines otherwise.⁸²

Agencies Made Awards to Potentially Ineligible Applicants with Foreign Ownership

To be eligible for a SBIR/STTR award, an applicant must meet certain ownership requirements at the time of award. Specifically, the applicant's business must be more than 50 percent owned and controlled by one or more individuals who are citizens or permanent residents of the United States, among other things.⁸³ In addition, if an applicant has any businesses that are affiliated with the applicant, certain of its affiliates must also meet other foreign ownership eligibility requirements.⁸⁴

⁸⁰Applicants and awardees are required to self-report whether the business, or any of its principals, have been convicted or had a civil judgment rendered against it within the previous 3-year period for the following: (1) commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) contract or subcontract; (2) violation of federal or state antitrust statutes relating to the submission of offers; or (3) commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating federal criminal tax laws, or receiving stolen property.

⁸¹The Company Registry is an element that the business is required to include within its proposal application or as an appendix. We define award life cycle as preaward, during the award, and postaward.

⁸²FAR § 9.405 generally notes that contractors debarred, suspended, or proposed for debarment are excluded from receiving contracts and, if applicable, subcontracts, for a set period, unless the agency head determines that there is a compelling reason to award the contract. 2 C.F.R. parts 180 and 200 contains similar provisions for parties to a grant or cooperative agreement.

⁸³The regulations require that applicants self-certify that they meet the eligibility requirements in 13 C.F.R. § 121.702. Small business concerns may also be owned by an Indian Tribe, Alaska Native Corporations, Native Hawaiian Organizations, or a wholly owned business entity of such tribe; joint ventures that meet certain conditions; and, under certain circumstances, venture capital operating businesses, hedge funds, and private equity businesses.

⁸⁴An affiliate of the small business concern can be a business that controls, or has the power to control, the small business concern. An affiliate can also be a subsidiary, where the small business concern has control of another business. The Extension Act, Pub. L. No. 117-183, 136 Stat. 2180 (2022), amended section 9 of the Small Business Act to require small businesses applying for SBIR/STTR awards to disclose information about the applicant's investment and foreign ties. In response, SBA amended section 9(a) of the Policy Directive and added an appendix to address responsibilities of participating agencies to collect disclosures of information about the applicant's investment and foreign ties, as required by the act. 13 C.F.R. § 121.702(c) defines affiliation for the SBIR/STTR programs. Affiliation, for our data-testing purposes, was determined by identifying potential relationships between the business and the global parent field within the System for Award Management. All businesses that share a global parent are considered affiliates of one another.

All applicants must certify at the time of award that they meet program eligibility requirements, including an applicant's business ownership. In addition, participating agencies must require that an applicant recertify the business' continued eligibility at other points in the award life cycle. For example, agencies will require a recertification if the applicant has been merged with or acquired by another business.

Some Awardees May Have Foreign Ownership



Eligibility requirements: A business must be more than 50 percent owned and controlled by one or more individuals who are citizens or permanent residents of the United States, among other things.

GAO analysis: Of the 10 awardees that self-reported foreign ownership, two of those were also found to have foreign bank accounts.

Sources: GAO analysis of U.S. Small Business Administration data; Icon-Studio/stock.adobe.com (icons); Surapong/stock.adobe.com (background image). | GAO-24-105470

We identified SBIR/STTR awardees that self-reported that they were foreign owned within the System for Award Management or were potentially affiliated with an applicant that self-reported as foreign owned. Six of the 11 participating agencies were associated with awards totaling \$34.3 million to 18 awardees with potential foreign ownership. Specifically, of the 10,570 awardees in our testing,

- 10 directly self-reported as foreign owned. These awardees received a total of \$5.7 million; and
- eight have potential affiliates that self-reported that they were foreign owned.⁸⁵ These awardees received a total of \$28.5 million.

Our analysis of SBIR/STTR charges, settlements, and administrative actions from fiscal years 2016 through 2023 did not identify schemes related to foreign ownership. Regardless, if the awardees identified through data testing did not disclose foreign ownership or relationships within the award process, this may be misrepresentation and merits further review by program management.

Participating agencies used various sources to identify applicant foreign ownership risks, according to agency officials. See table 5.

⁸⁵These potential affiliates of the SBIR/STTR awardees self-reported within the System for Award Management that they were foreign owned. We did not conduct additional research to confirm whether the business and the affiliates were foreign owned.

Table 5: Resources to Identify Applicant Foreign Ownership Risks That Participating Agencies Reported Using

Resources used to identify applicant foreign ownership risks	Agency responses
Government databases	Nine of 11 participating agencies use government databases, such as the System for Award Management, Federal Awardee Performance and Integrity Information System, or SBIR.gov. For example, agency officials stated that they review self-reported representations and certifications for ownership in the System for Award Management prior to award to identify and evaluate applicant risks related to ownership.
Third-party sources	One agency’s subcomponent uses third-party sources, such as Bloomberg’s data subscription service, which provides news; legal content; and complete company financial data, including government contractors and subcontractors, according to an official.
Due diligence processes	Ten of 11 agencies referenced using due diligence processes. ^a For example, these processes include reviewing employee affiliations and foreign ownership (e.g., financial ties and obligations).

Source: GAO analysis of participating agency responses. | GAO-24-105470

^aAll participating agencies, as of September 2022, were to begin implementing new requirements to establish a due diligence program, which includes conducting some type of review to verify an applicant’s foreign-ownership status. In November 2023, we found that agencies plan to use due diligence tools to help vet foreign ownership and foreign financial ties and obligations associated with Small Business Innovation Research and Small Business Technology Transfer applicants and awardees. For example, some agencies may use intra-agency resources—such as counterintelligence or security offices—to help gather and analyze information. In cases where an agency determines that the relationships or commitments of a business pose a national security risk, the agency may choose to deny an award or take other actions consistent with their risk-based approach. According to the U.S. Small Business Administration, the due diligence programs required to be established by the Extension Act are intended to help agencies manage any potential foreign risks associated with awards, in accordance with the established federal research security strategy. [GAO-24-106400](#). We did not assess agencies’ due diligence efforts, as these requirements were promulgated after the scope of our review, which included awards made from fiscal years 2016 through 2021.

Agencies Made Awards to Potentially Ineligible Applicants Exceeding Size Requirements

Some Awardees May Have More Than 500 Employees



Eligibility requirements: A business must meet size requirements set by the U.S. Small Business Administration: A business—together with its affiliates—must not have more than 500 employees, with some exceptions.

GAO analysis: Of the 42 awardees identified, we found 17 that self-reported over 500 employees within the System for Award Management in their award year.

Sources: GAO analysis of U.S. Small Business Administration data; Icon-Studio/stock.adobe.com. | GAO-24-105470

GAO 24 105470 (icons). | [GAO-24-105470](#)

To be eligible for an award, an applicant must meet size requirements set by SBA at the time of the award, wherein the applicant—together with its affiliates—must not have more than 500 employees, with some exceptions.⁸⁶ The SBA’s Policy Directive requires agencies to collect and review the applicant’s size information at the time of award and during the award life cycle. Each phase I and phase II applicant must submit a certification stating that it meets the size requirements of the SBIR/STTR programs.

We identified 42 out of 10,570 awardees that may have more than 500 employees based on information from the System for Award Management and National Directory of New Hires.⁸⁷ Five of 11 participating agencies made these awards, totaling about \$117 million, to awardees that potentially did not meet the program size requirements.

Our analysis of SBIR/STTR charges, settlements, and administrative actions from fiscal years 2016 through 2023 identified three cases associated with awards to awardees allegedly above the size threshold (see text box for an illustrative example).

⁸⁶Business size is based on average employees over the previous pay periods for the preceding 24 calendar months. A business may increase to greater than 500 employees during the performance of the award. See 13 C.F.R. § 121.106 for calculation of employee size and 13 C.F.R. § 121.704 for when the eligibility of a concern is determined.

⁸⁷This includes potential affiliates and reflects information between October 1, 2019, and September 30, 2020. The National Directory of New Hires data available for this analysis coincide with the COVID-19 public health emergency that began in March 2020. It is possible the pandemic impacted the number of employees reported in the National Directory of New Hires in this time frame. The System for Award Management’s average number of employees uses a 12-month average.

A business and two of its officers allegedly misrepresented its status as a small business concern to obtain Small Business Innovation Research (SBIR) awards. A business, its chief executive officer, and its chief financial officer allegedly misrepresented the business’s eligibility to receive SBIR awards by falsely certifying that the business was a small business concern. The business and its officers allegedly made these misrepresentations to the U.S. National Science Foundation (NSF), the National Aeronautics and Space Administration (NASA), and the U.S. Department of Health and Human Services (HHS) both when applying for the awards and throughout the awards’ life cycles. As a result, NSF, NASA, and HHS approved and funded awards that the business would not have otherwise received. The business and its officers agreed to pay the United States \$1.9 million to resolve these allegations.

Source: GAO analysis of U.S. Department of Justice court documents. | GAO-24-105470

Most participating agencies reported using self-reported applicant proposal documentation (including certifications) to identify and evaluate some risks related to false information about business size, as required. Participating agencies also reported using information from government databases and due diligence review processes to evaluate risks associated with business size. See table 6.

Table 6: Resources to Identify Applicant Size Risks That Participating Agencies Reported Using

Resources to identify applicant size risks	Agency responses
U.S. Small Business Administration (SBA) databases or information	Four of 11 agencies use SBA databases or information. For example, the U.S. Department of Agriculture uses SBIR.gov when researching size. Two U.S. Department of Defense (DOD) subcomponents use the SBA’s Dynamic Small Business Search database to review contractors’ business size. ^a According to SBA officials, participating agencies should not rely on SBIR.gov to make eligibility determinations.
System for Award Management	Five of 11 agencies use the System for Award Management. For example, one U.S. Department of Commerce subcomponent checks the System for Award Management to confirm small business status.
Due diligence review processes	Four of 11 agencies use due diligence review processes. For example, one DOD subcomponent’s due diligence risk review report identifies company size based on publicly available information.
None	Some agencies, including a few subcomponents, did not identify additional information sources. For example, U.S. Department of Energy and U.S. Environmental Protection Agency officials told us they use self-certifications and did not identify additional information or actions taken to assess risk associated with entity size.

Source: GAO analysis of participating agency interviews and documentation. | GAO-24-105470

^aAccording to the Dynamic Small Business Search’s web page, contracting officers can use the database as a part of market research and to help determine set-aside or sole-source allocation, or search for contractors for open or upcoming awards.

Agencies Made Awards to Applicants with Potentially Ineligible Principal Investigators

To be eligible for SBIR/STTR awards, principal investigators must certify that they are primarily employed by the applicant.⁸⁸ The SBA’s Policy Directive requires that for phase I and II STTR/STTR awards, the primary employment of the principal investigator must be with the applicant’s small business or research institution (for STTR only) at the time of, and during the performance of, the award. Primary employment is defined as most

⁸⁸The principal investigator is the individual designated by the applicant to provide the scientific and technical direction to a project supported by the funding agreement. The principal investigator will spend more than half their time (based on a 40-hour work week) as an employee of the awardee (or research institution for STTR only). Occasionally, deviations from this requirement may occur and must be requested and approved in writing by the funding agreement officer after consultation with the agency’s SBIR/STTR program manager or coordinator. Regardless, wages from multiple sources raise concern on principal investigator employment.

of one's time based on a 40-hour work week. This requirement precludes full-time employment with another organization. The Policy Directive requires agencies to collect and review principal investigator information at the time of, and during, the award life cycle.

On the basis of our analysis of the awards data, we identified 117 out of 10,570 awardees listing principal investigators whose employment overlapped at least 15 days for two or more separate SBIR/STTR awardees, indicating that they may have been concurrently employed by two awardees. Nine of 11 participating agencies made these awards, totaling \$95 million, to awardees whose principal investigator worked for more than one SBIR/STTR awardee at the same time.

Some Awardees Potentially Shared a Principal Investigator



Eligibility requirements: Principal investigators must certify that they are primarily employed by the applicant—defined as spending the majority of one's time with that employer based on a 40-hour work week.

GAO analysis: Among the 117 awardees with principal investigators working for more than one Small Business Innovation Research/Small Business Technology Transfer (SBIR/STTR) awardee at the same time, we identified four principal investigators who have awards for two separate businesses that overlap for 2 years or more.

Sources: GAO analysis of U.S. Small Business Administration data; Icon-Studio/stock.adobe.com (icons); Surapong/stock.adobe.com (background image). | GAO-24-105470

Further, in a separate test based on analysis of wage data and fiscal year 2020 awards, we identified 661 awardees with a principal investigator receiving wages from more than one business in that year.⁸⁹ Ten of 11 participating agencies made these awards, totaling nearly \$487 million, to awardees whose principal investigator received wages from more than one business in that year.

Of these awardees,

- 14 had a principal investigator with wages reported from four or more businesses, totaling about \$10 million;
- 88 had a principal investigator with wages reported from three businesses, totaling about \$58 million; and

⁸⁹The National Directory of New Hires reports wage data on a quarterly basis. It is possible that individuals identified in these tests worked for multiple businesses in the same quarter but not necessarily at the same time.

- 570 had a principal investigator with wages from two businesses, totaling about \$419 million.⁹⁰

Our analysis of SBIR/STTR charges, settlements, and administrative actions from fiscal years 2016 through 2023 identified principal investigator-related concerns. See text box for an illustrative example.

A business misrepresented the primary employment of its principal investigator for multiple Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) awards. A business falsely represented that the individual it listed as the principal investigator for multiple SBIR and STTR grant awards was primarily employed by the business. Specifically, the business represented that the individual was eligible to serve as the principal investigator in proposals, payment requests, and final reports regarding four SBIR and STTR grants awarded by the U.S. National Science Foundation and U.S. Environmental Protection Agency. When making these representations, the business knew that the individual was primarily employed by another business. The business pleaded guilty to two counts of false statements and, among other things, was sentenced to 5 years of probation and ordered to pay restitution of over \$800,000.

Source: GAO analysis of U.S. District Court documents. | GAO-24-105470

In addition to the fraud schemes identified, we also identified an instance of an agency taking an administrative action against a business that designated an independent contractor as principal investigator on an HHS National Institutes of Health SBIR grant. This individual was ineligible to serve as the principal investigator for these awards because the individual was not an employee of the business. Because of this and other failures by the business to comply with award requirements, HHS National Institutes of Health disallowed certain costs the business had charged to the SBIR award.

Participating agencies reported using various government sources, applicant proposal documentation, and internet searches to identify and evaluate risks related to principal investigators' employment and eligibility. See table 7.

Table 7: Resources to Identify Applicant Principal Investigator Risks That Participating Agencies Reported Using

Resources to identify applicant principal investigator risks	Agency responses
Small Business Innovation Research/Small Business Technology Transfer (SBIR/STTR) and federal agency databases	Four of 11 agencies use other SBIR and STTR and federal agency databases. For example, the U.S. National Science Foundation uses the Bureau of Labor Statistics to match education and experience data with the applicant information as a part of their review. The U.S. Department of Education uses the U.S. Department of the Treasury's Do Not Pay System to assess such risks. ^a According to U.S. Small Business Administration (SBA) officials, participating agencies should not rely on SBIR.gov to make eligibility determinations.
Internet searches	Four of 11 agencies conduct internet searches to identify false information, such as principal investigator affiliation. For example, the U.S. Department of Commerce's subcomponents conduct internet searches to identify principal investigator affiliation, whether a business exists, and to confirm that principal investigators are employed by the business.
Applicant's proposal documentation	Six of 11 agencies reported using the applicant's proposal documentation. Such documentation included resumes, certifications, financial disclosure forms, and pay stubs.

Source: GAO analysis of participating agency interviews and documentation. | GAO-24-105470

⁹⁰In these instances, it would not be uncommon for a principal investigator for STTR awards to have wages from two sources, since the principal investigator's employment may be the research institution, as well as the awardee's business. We did not review the source of principal investigators' wages.

^aThe Treasury's Do Not Pay Working System was developed to enable federal agencies to reduce improper payments by checking various databases before making payments or awards to identify ineligible awardees and to prevent fraud or errors from being made. Through the Do Not Pay initiative, agencies can use the Social Security Administration's Death Master File (public version), the Treasury Offset Program Debt Check, the U.S. Department of Health and Human Service's List of Excluded Individuals and Entities, and the General Services Administration's System for Award Management Exclusion Records, among other data sources, to assist in verifying eligibility. However, the Do Not Pay system does not contain information needed to check various principal investigators' employment risks, such as employment with multiple businesses.

Applicants are not required to submit a principal investigator's information in the proposal, but this information is required once the applicant receives an award. Past work identified if a principal investigator has awards that overlap in time, the agency requires the applicant to submit a form documenting current and pending support to the applicant to determine how much effort the principal investigator is proposing in any given time frame.⁹¹ In addition, an OIG may initiate an investigation into an award, if it has information that multiple, simultaneous awards identified the same principal investigator, which can indicate insufficient time to actively work on all of them.⁹²

Agencies Made Awards to Applicants for Potentially Equivalent Work

SBIR/STTR applicants often submit duplicate or similar proposals to more than one soliciting agency, when those agencies make announcements or solicitations. According to the Policy Directive, essentially equivalent work must not be funded in the SBIR/STTR or other federal agency programs, unless an exception to this rule applies.

Essentially equivalent work is defined in the Policy Directive as work that is

- substantially the same research, which is proposed for funding in more than one contract proposal or grant application submitted to the same federal agency, or submitted to two or more different federal agencies for review and funding consideration; or
- work where a specific research objective and the research design for accomplishing the objective are the same or closely related to another proposal or award, regardless of the funding source.

Agencies are required to develop policies and procedures to avoid funding essentially equivalent work already funded by the same or another agency, which could include searching SBIR.gov prior to award for the applicant, key individuals, and similar abstracts.⁹³

⁹¹In June 2021, we found that agencies used differing approaches to implement the Policy Directive requirements related to fraud, waste, and abuse. Of the 21 recommendations we made in June 2021, three recommendations remain open for two DOD subcomponents that participate in the SBIR/STTR programs, as of May 2024. The remaining 18 recommendations have been implemented by the participating agencies. [GAO-21-413](#).

⁹²[GAO-21-413](#).

⁹³An abstract is a summary of the SBIR/STTR research project.

Some Awardees Potentially Received Awards for Work Already Funded



Eligibility requirements: Applicant must not receive award funds for essentially equivalent work in the Small Business Innovation Research/Small Business Technology Transfer (SBIR/STTR) or other federal agency programs, unless an exception to this rule applies.

GAO analysis: We identified 280 out of the 10,570 awardees with potentially equivalent work based on text analysis that identified unique word duplication within 23,135 awardee abstracts.

Sources: GAO analysis of U.S. Small Business Administration data; Icon-Studio/stock.adobe.com (icons). | GAO-24-105470

On the basis of our text analysis of the abstracts in the awards data that identified unique word duplication, we identified 280 out of 10,570 awardees with potentially equivalent work.⁹⁴ Ten of 11 participating agencies made these awards, totaling about \$445 million, to awardees for potentially equivalent work. If the awardees identified through our data testing did not disclose similar proposals throughout the awards process, this may be misrepresentation for eligibility and merits further review.

Our analysis of SBIR/STTR charges, settlements, and administrative actions from fiscal years 2016 through 2023 identified four schemes involving awards to applicants with potentially equivalent work (see text box for an illustrative example).

A couple did not disclose essentially equivalent work on three U.S. Department of Energy (DOE) Small Business Technology Transfer (STTR) grant applications. On three occasions, a university professor and his wife applied for DOE STTR grants on behalf of a business they founded and controlled. The applications sought funding to research, develop, and commercialize a specialized pump used in analytical chemistry. On the basis of these applications, DOE awarded the business a total of \$2.1 million in STTR funds. However, on applications for each of the DOE grants, the couple omitted that the professor had previously received a U.S. Department of Health and Human Services' National Institutes of Health grant to perform essentially equivalent work on the pump. The professor pleaded guilty to using false documents and was sentenced to 27 months in prison, 2 years of supervised release, a \$10,000 fine. The professor's wife pleaded guilty to making a false statement and was sentenced to 14 months in prison, 2 years of supervised release, and a \$10,000 fine. The couple was also ordered to pay \$2.1 million in restitution to DOE.

Source: GAO analysis of U.S. District Court documents. | GAO-24-105470

Most of the participating agencies reported using various databases and tools to identify and evaluate applicants for potentially equivalent work. Most agencies also reported using internal staff and conducting outreach to other SBIR/STTR agencies to assess equivalent work risks. See table 8.

⁹⁴Of the 38,206 awards in scope identified on SBIR.gov, we excluded 9,289 awards when a business had only one phase I or phase II award. An additional 5,782 awards were removed due to their abstracts having fewer than 60 unique words. These were deemed to have too few words for an accurate review of potentially duplicative work. Of the excluded awards in our scope, 179 had fewer than 50 characters, such as "NA" and "TBD."

Table 8: Resources to Identify Applicant Equivalent Work Risks That Participating Agencies Reported Using

Resources to identify applicant equivalent work risks	Agency responses
SBIR.gov	Five of 11 agencies use SBIR.gov to assess equivalent work risks. For example, according to U.S. Department of Education officials, when proposals are recommended for funding, officials conduct a more in-depth review for fraud, waste, and abuse indicators, including searching SBIR.gov for prior awards to avoid essentially equivalent work. According to U.S. Small Business Administration officials, participating agencies should not rely solely on SBIR.gov to make eligibility determinations.
Government and third-party databases and software	Three of 11 agencies use government and third-party databases and software. For example, a U.S. Department of Energy (DOE) subcomponent uses a system called CRUNCHBASE to see if the proposed research has been funded by a government agency. ^a
Internal databases	Four of 11 agencies use internal databases. For example, the four U.S. Department of Health and Human Services (HHS) subcomponents use an internal database to avoid funding duplicative awards. The U.S. Department of Agriculture (USDA) searches its Current Research Information System site to check for essentially equivalent work. ^b
Text analysis tools and software	Four of 11 agencies use text analysis tools and software. For example, a U.S. Department of Defense (DOD) subcomponent agency reported that the proposals selected for award are reviewed using the DocSim search tool, which compares the proposal abstracts against previously awarded proposals across the federal government. ^c The National Aeronautics and Space Administration uses software that can search for specific textual terms and gives a score for relevance and potential duplication.
Program and other internal staff	Seven of 11 agencies use program and other internal staff. For example, five participating agencies, including one HHS and four DOD subcomponents, use internal subject matter experts to review and assess potential equivalent work risks. One DOD subcomponent, however, is not resourced to vet individual proposals to determine if proposed work has already been selected for funding and relies on the knowledge of technology chiefs and subject-matter experts to identify potentially equivalent work risks.
Outreach to other agencies	Four of 11 agencies outreach to other agencies to avoid duplicate funding risks. For example, the U.S. Department of Education has an informal process to contact other participating agencies about their most recent awards to not award duplicative funding to an applicant.

Source: GAO analysis of participating agencies interviews and documentation. | GAO-24-105470

Note: Table includes one or more participating agencies and subcomponents responses; thus, the examples will exceed 11.

^aAccording to DOE SBIR/STTR officials, the CRUNCHBASE database provides information of the sources of funding that various businesses have received, including venture capital or other government funding.

^bAccording to the Current Research Information System site (<https://cris.nifa.usda.gov/>), the Current Research Information System provides documentation and reporting for ongoing agricultural; food science; human nutrition; and forestry research, education, and extension activities for USDA.

^cDocSim is software that compiles and compares information, according to officials.

Agencies Made Awards to Applicants with Potentially Ineligible Addresses, but Full Extent of Risk Is Unknown

Some Awardees May Have Potentially Invalid Facilities



Eligibility requirements: Applicants are required to submit the physical facility location where the research is being conducted, as well as any other mailing and business address. Applicants are required to certify that they will, or did, perform the work on the award at their facilities with their employees, unless otherwise indicated.

GAO analysis: We found 78 awardees with vacant addresses and 79 awardees with invalid addresses, according to United States Postal Service data.

Sources: GAO analysis of U.S. Small Business Administration data; Icon-Studio/stock.adobe.com (icons). | GAO-24-105470

To be eligible for an SBIR/STTR award, applicants must submit a detailed description and location of the physical facility where the research is being conducted. Applicants must certify that the work is being performed at their facilities within the United States, unless otherwise indicated in their applications and approved in the funding agreement. Though the applicant may provide multiple addresses, only one address per award is entered into SBIR.gov once an award is granted.

Eight of 11 participating agencies—which are responsible for entering awardee information into SBIR.gov—told us that the address listed on the website may not reflect the facility address where the work is being performed. Moreover, most agencies noted that a business could have several locations and could possibly leverage those to conduct the research.

Using the awardee address listed on SBIR.gov, we identified 157 out of 10,570 awardees with potentially ineligible addresses that were undeliverable or vacant, according to United States Postal Service data.⁹⁵ All participating agencies made these awards, totaling about \$157 million, to awardees with potentially ineligible addresses.⁹⁶ Specifically, we identified:

- 79 awardees with undeliverable addresses and

⁹⁵SBIR.gov does not provide information on facility address, either as its own data field or by indicating if the business certified multiple addresses. As a result, we were unable to perform analyses specifically on facility addresses and were not able to determine the number of additional awardees with potentially ineligible facilities. It is possible that some of the awardees identified in our analyses had the same business and facilities address.

⁹⁶In January 2023, we analyzed fiscal years 2016 through 2021 awardee addresses in SBIR.gov, using the United States Postal Service Address Matching System. We analyzed all awardees in our scope for undeliverable addresses. We focused on fiscal year 2021 awardees only to identify vacant addresses to get as close to the award date as possible. It is possible awardees changed locations after their award date ended.

- 78 awardees with vacant addresses.

Additionally, we found 146 awardees with addresses that were commercial mail-receiving agencies, a third-party agency that receives and handles mail for a client.⁹⁷

To review our address results further, we selected 12 awardees associated with 17 addresses for further investigation. We used publicly available information on the internet to research and select these awardees. For example, we selected one awardee with a commercial mail-receiving agency address for further review because the awardee listed an updated address on other awards that was residential and associated with additional businesses and potential foreign influences.

GAO criminal investigators conducted site visits to these 17 selected addresses.⁹⁸ During these site visits, we assessed whether the awardee was located at the given address. Specifically, we found

- one government facility without business presence,
- one vacant lot,
- one address that appears to not exist,
- five addresses without confirmation of a business presence,
- two mailboxes affiliated with businesses located in shared office suites without a physical presence,
- one residential home,
- three shared office suites that appeared to be occupied by the businesses, and
- three addresses confirmed as independent office suites.

A couple misrepresented the location of work in proposals for National Aeronautics and Space Administration (NASA) Small Business Innovation Research (SBIR) awards. A university professor and his wife misrepresented the facilities where they would complete work under NASA SBIR awards. Specifically, the individuals submitted proposals stating that they would complete the research at a business they owned and subcontract some of the work to the university that employed the professor. In fact, the business had no facilities, and the research was performed solely by students and others working in a university laboratory. Each individual was convicted of six counts of wire fraud. The professor was sentenced to a year and a day in prison and a \$3,000 fine. The professor's wife was sentenced to 3 months in prison and a \$1,000 fine. The couple was also ordered to pay \$72,000 in restitution to NASA.

Our analysis of SBIR/STTR charges, settlements, and administrative actions from fiscal years 2016 through 2023 further demonstrated the importance of knowing the facility address. Specifically, our analysis identified seven SBIR/STTR fraud schemes that involved misrepresentation of the facilities. For example, in one

⁹⁷A business's use of a commercial mail-receiving agency may not disqualify an applicant from the SBIR/STTR program. However, the physical facility must be conducive for the proposed research that is being conducted, and a commercial mail-receiving agency may not be feasible for the proposed research. For example, a commercial mail-receiving agency may be a virtual office—that is, a company advertising mailbox, or a telephone answering service—and is not conducive for laboratory or technical research. A commercial mail-receiving agency may also be a dedicated workspace that is conducive for the proposed research. Vacant addresses refer to a business that is no longer at the location provided. The United States Postal Service would flag a location as vacant if it used to deliver mail there and has not delivered mail there in more than 90 days. An invalid address is when an address is not recognized by the United States Postal Service, was incorrectly entered, or was missing a street number.

⁹⁸Site visits were conducted July through December 2023. Awards that were identified for investigative review were restricted to those received in fiscal year 2021 to mitigate the amount of time between the awarded date and our investigative date. It is possible that those businesses no longer exist or have since moved from the locations visited.

scheme, awardees attested that SBIR/STTR projects would be completed in the United States, when, in fact, the work was performed in other countries. See the text box for another illustrative example.

Source: GAO analysis of U.S. Department of Justice and U.S. District Court documents. | GAO-24-105470

Neither the Policy Directive nor the statute require participating agencies to verify the validity of applicant addresses, including the facility address where the research is to be conducted.⁹⁹ Most agencies do not verify the addresses provided by the applicant and rely solely on the applicant’s self-certification in the proposals. Some agencies told us they take steps to verify addresses, though this is not required. See table 9.

Table 9: Resources to Identify Applicant Facility Address Risks That Participating Agencies Reported Using

Resources to identify applicant facility address risks	Agency responses
System for Award Management	Five of 11 agencies verify that the address in the System for Award Management matches the applicant’s address in the proposal.
Internet searches	Four of 11 agencies and subcomponents use other sources, including conducting internet searches, to verify address and facility information. For example, the U.S. Environmental Protection Agency (EPA) and the National Aeronautics and Space Administration conduct internet searches to verify facility addresses; EPA also confirms it is not a residential address.
Site visits	Two of 11 participating agencies conduct site visits. Some agencies cited challenges to do so. For example, the U.S. Department of Homeland Security (DHS) does not have the ability and resources to monitor the location of the employees of the small businesses. DHS officials further noted that, depending on the nature of the work and the feasibility, there are some contracts for which travel to the business’s facility or in-person events are conducted. Additionally, two agencies requested in their fiscal year 2024 work plan to the U.S. Small Business Administration (SBA) to use Small Business Innovation Research/Small Business Technology Transfer funding for fraud, waste, and abuse prevention efforts, including conducting site visits. For example, the U.S. Department of Energy has requested \$10,000 in additional funding to conduct planned site visits in fiscal year 2024. The U.S. Department of Health and Human Services’ National Institutes of Health has requested \$50,000 to hire a contractor to conduct site visits. ^a

Source: GAO analysis of SBA and participating agency interviews and documentation. | GAO-24-105470

^aAccording to the Policy Directive, participating agencies may use up to 3 percent of its budget for one or more specific activities, including oversight and fraud, waste, and abuse prevention. Agencies must submit a work plan to SBA at least 30 calendar days prior to the start of each fiscal year for which the pilot program is in operation.

As described earlier in this report, since September 2022, participating agencies have been required to implement new due diligence efforts to assess applicant security risks. For example, in May 2023, SBA updated its Policy Directive to require applicants to identify foreign ownership or affiliation. In some agency efforts, agencies request applicants to submit additional documentation. For example, one HHS subcomponent stated that its due diligence guidance indicates that a copy of an active lease or similar agreement be requested; however, the subcomponent does not verify addresses provided. Similarly, the NSF’s due diligence

⁹⁹The SBIR and STTR Extension Act of 2022 required that participating agencies implement a due diligence program to assess security risks. Agencies are required to assess, using a risk-based approach, as appropriate, the cybersecurity practices, patent analysis, employee analysis, and foreign ownership of a small business concern seeking an award, including the financial ties and obligations, such as the equity and debt obligations of the small business concern and the employees of the small business concern, to a foreign country, foreign person, or foreign entity. The act does not specifically require agencies to verify the validity of a business’s address nor facility address where the research is being conducted.

efforts require applicants to identify all locations where work is to be conducted during the project. According to NSF officials, since about 2016, NSF requires all potential awardees to disclose all research locations. Officials also require applicants to complete a “Primary Place of Performance” document, which is the location where the largest share of the work is to be done. For locations not owned by the applicant, NSF requests lease or equivalent documentation guaranteeing access. NSF officials do not directly verify the locations of work performed during the project.

Federal Internal Control Standards state that managers should use quality information to achieve the entity’s objectives.¹⁰⁰ To do this, managers may identify information requirements; obtain relevant data from reliable internal and external sources; and process data into information that is appropriate, current, complete, accurate, accessible, and provided on a timely basis. Additionally, according to Fraud Risk Framework leading practices, physical inspections, site visits, or making contact with program enrollees for additional information can be used to help prevent and detect potential fraud.¹⁰¹

As our analyses show, verifying all awardee business addresses, including facility addresses, can identify potentially ineligible applicants with invalid addresses. Additionally, conducting site visits can further prevent and detect potential fraud, waste, and abuse by ensuring that awardees are providing accurate information on their certifications. Although some agencies take some steps, such as reviewing the System for Award Management to validate an applicant’s address, agencies are only checking that the address matches. Most agencies rely on the applicant self-certifying that the address is valid, which may not be the case. For example, we identified one awardee that listed a commercial mail-receiving agency’s mailbox as its research facility address, which was accepted by the agency. This awardee currently has a 2023 phase II SBIR award and is using the mailbox as its facility address. By not verifying applicant business addresses, including facilities addresses, participating agencies are missing opportunities to ensure that awardee addresses are accurate and meet research needs.

¹⁰⁰[GAO-14-704G](#).

¹⁰¹[GAO-15-593SP](#).

Our Data Tests Identified Numerous Fraud, Waste, and Abuse Risks, but Data Quality Limitations May Hinder Participating Agencies' Ability to Identify Such Risks

Analytic Tests Identified Awardees Associated with Potential Fraud, Waste, and Abuse Risks

Fraud Risk Framework Component 3

Design and implement an antifraud strategy with control activities



Source: GAO. | GAO-24-105470

Participating agencies use various methods to identify individual applicant and awardee risks for potential fraud, waste, or abuse. Some leverage analytic testing—such as text mining to compare applicant proposals with information in publication and patent databases—to strategically identify SBIR/STTR fraud, waste, or abuse risks to target resources for additional reviews. A leading practice from the Fraud Risk Framework encourages agencies to conduct data analytics activities to prevent and detect fraud. For example, agencies can consider program rules and known, or previously encountered, fraud schemes to design analytic tests. Additionally, analytic activities can include mining and matching internal and external data to verify applicant information and identify inconsistencies and previously unknown relationships within the data.¹⁰²

We developed 27 analytic tests of specific SBIR/STTR program eligibility requirements mentioned earlier and risks, such as identifying awardees who may have shared bank information to identify the presence of potential fraud, waste, or abuse risks within the programs (see table 12 in app. I).¹⁰³ We analyzed the SBIR/STTR Policy Directive guidelines, the 11 participating agencies' OIG SBIR fraud detection indicators, and previous fraud schemes to create these tests. We aligned the tests with the GAO-identified fraud, waste, and abuse risk categories. Our results identified at least four or more indications of fraud, waste, and abuse risk for 842 of

¹⁰²According to the Fraud Risk Framework, conducting data matching to verify key information, including self-reported data and information necessary to determine eligibility, can prevent and detect fraud. Data mining analyzes data for relationships that have not previously been discovered. Data mining can identify suspicious activity or transactions, including anomalies, outliers, and other red flags in the data. [GAO-15-593SP](#).

¹⁰³Our 27 tests covered 21 GAO-identified fraud, waste, and abuse categories. We were not able to create tests for all categories, such as bid-rigging and subcontractors, due to limitations in available data. We analyzed the SBIR/STTR Policy Directive guidelines, OIG SBIR fraud detection indicators, and previous fraud schemes to create these tests and aligned them with the GAO-identified fraud, waste, and abuse risk categories. We examined risks by matching data on awardees found in SBIR.gov awards data against the SBA's Company Registry, the System for Award Management, and other available databases. Tests were designed to prevent and detect fraud at various stages of the award life cycle.

10,570 awardees in fiscal years 2016 through 2021.¹⁰⁴ Although an awardee may be identified in multiple tests, the presence of such indicators does not confirm fraud, waste, or abuse but can provide information on prioritizing awards and awardees for additional review by program managers.

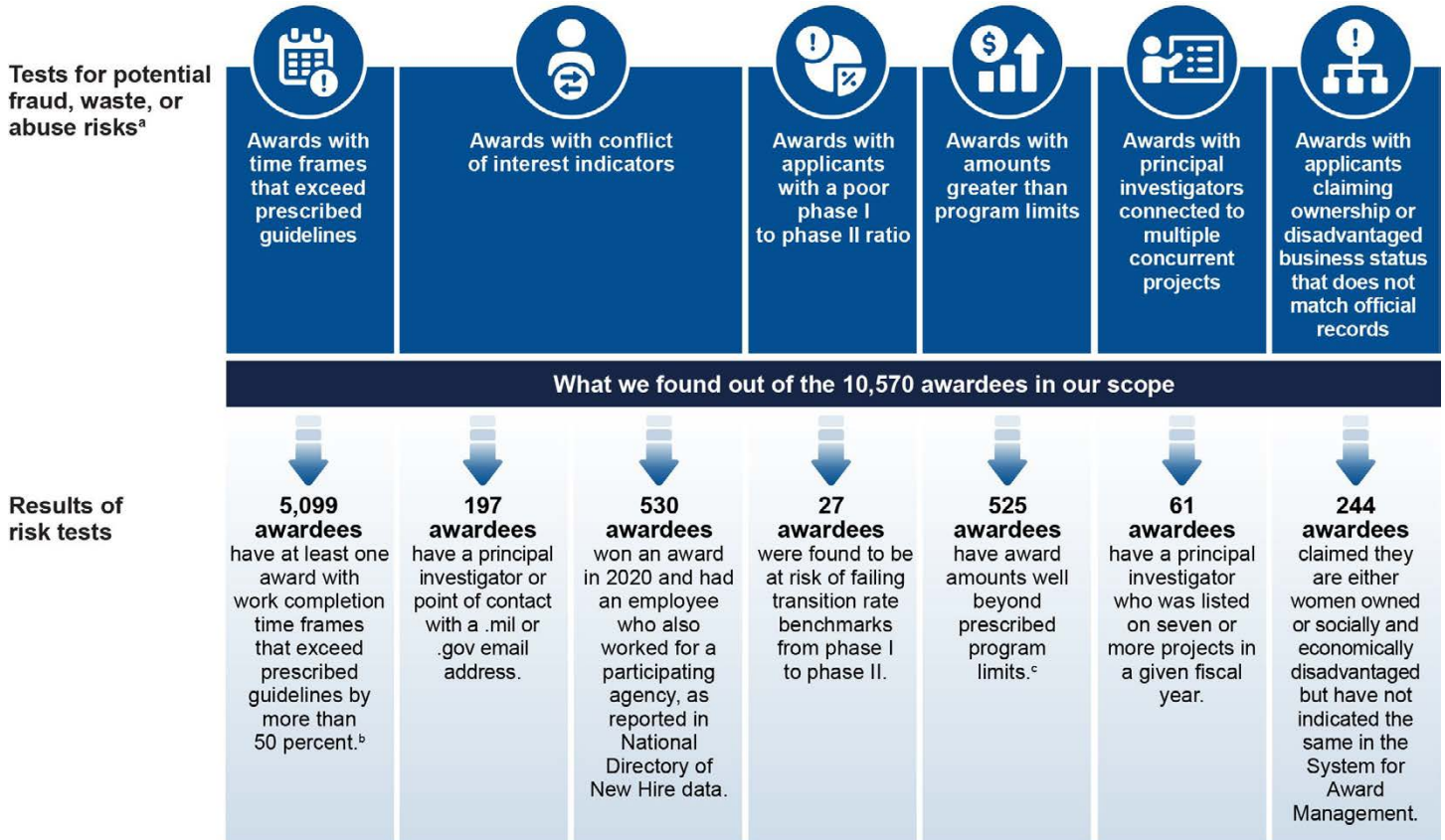
Our tests related to Policy Directive guidelines focused on several fraud, waste, and abuse risk categories, such as conflict of interest and misrepresentation during the award life cycle. For example, SBA cautions that awards made to a business owned by, or employing, current or previous federal government employees may create conflicts of interest.¹⁰⁵ To identify potential conflicts of interest, we mined the SBIR.gov award data and found 197 awardees with a principal investigator or point of contact that had a .mil or .gov email address, indicating a potential relationship with the federal government.

Similarly, a SBIR/STTR program goal is to foster and encourage participation by minority and disadvantaged businesses in technological innovation. To identify instances of potential misrepresentation of these data, we conducted data matching to the System for Award Management and found 244 awardees that had conflicting information related to their status, indicating potential misrepresentation or error by the awardee. Figure 14 shows selected results for other tests performed based on Policy Directive guidelines.

¹⁰⁴The Policy Directive defines an awardee as the organizational entity business that receives a SBIR/STTR award. In this report, a business is a commercial operation, company, or firm. A business that receives a SBIR/STTR award is identified as an awardee.

¹⁰⁵According to the Policy Directive, this may be a violation of FAR part 3 and the Ethics in Government Act of 1978. Each participating agency should refer to the standards of conduct review procedures currently in effect for its agency to ensure that such conflicts do not arise.

Figure 14: Analytic Tests of Selected Policy Directive Guidelines and Results for Awardees with Potential Fraud, Waste, or Abuse Risks



Sources: GAO analysis of U.S. Small Business Administration data; Icons-Studio/stock.adobe.com (icons). | GAO-24-105470

Accessible Data for Figure 14: Analytic Tests of Selected Policy Directive Guidelines and Results for Awardees with Potential Fraud, Waste, or Abuse Risks

Test for potential fraud, waste, or abuse risks ^a	Results of risk tests (What we found out of the 10,570 awardees in our scope)
Awards with time frames that exceed prescribed guidelines	5,099 awardees have at least one award with work completion time frames that exceed prescribed guidelines by more than 50 percent. ^b
Awards with conflict of interest indicators	197 awardees have a principal investigator or point of contact with a .mil or .gov email address.
Awards with applicants with a poor phase I to phase II ratio	530 awardees won an award in 2020 and had an employee who also worked for a participating agency, as reported in National Directory of New Hire data.
Awards with amounts greater than program limits	27 awardees of failing transition rate benchmarks from phase I to phase II.
Awards with principal investigators connected to multiple concurrent projects	525 awardees have award amounts well beyond prescribed program limits. ^c
Awards with applicants claiming ownership or disadvantaged business status that does not match official records	61 awardees have a principal investigator who was listed on seven or more projects in a given fiscal year.
	244 awardees claimed they are either women owned or socially and economically disadvantaged but have not indicated the same in the System for Award Management.

Test for potential fraud, waste, or abuse risks ^a	Results of risk tests (What we found out of the 10,570 awardees in our scope)
Awards with principal investigator connected to multiple concurrent projects	61 awardees have a principal investigator who was listed on 7 or more projects in a given fiscal year.
Awards with applicants claiming ownership or disadvantaged business status that does not match official records	244 awardees claimed they are either women owned or socially and economically disadvantaged but have not indicated the same in the System for Award Management.

Sources: GAO analysis of U.S. Small Business Administration data; Icons-Studio/stock.adobe.com (icons). | GAO-24-105470

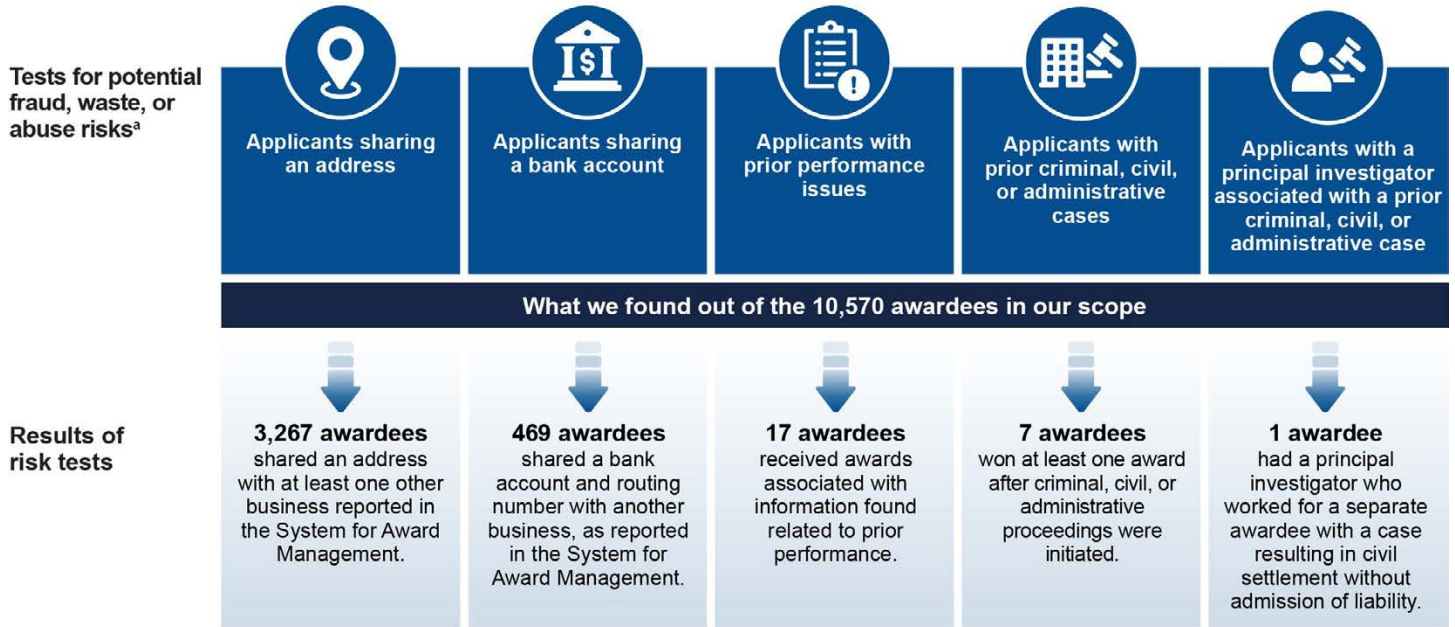
^aFraud involves obtaining something of value through willful misrepresentation (e.g., materially false statements of fact based on actual knowledge, deliberate ignorance, or reckless disregard of falsity). Whether an act is, in fact, fraud is a determination to be made through the judicial or other adjudicative system and is beyond management’s professional responsibility for assessing risk. Waste is the act of using or expending resources carelessly, extravagantly, or to no purpose. Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary operational practice, given the facts and circumstances. Although waste and abuse do not necessarily involve fraud or illegal acts, they may be an indication of potential fraud or illegal acts and may still affect the achievement of defined objectives. The presence of such an indicator does not confirm fraud, waste, or abuse.

^bThe Policy Directive states that a phase I award period of performance normally should not exceed 6 months for the Small Business Innovation Research program or 1 year for the Small Business Technology Transfer program. However, agencies may provide a longer performance period, where appropriate, for a particular project. A phase II award period of performance is subject to negotiation between the awardee and the issuing participating agency. The duration of a phase II award period normally should not exceed 2 years. However, agencies may provide a longer performance period, where appropriate, for a particular project. We tested to identify awards that have a length that is 50 percent greater than the normally prescribed lengths. Our testing coincides with the COVID-19 public health emergency that began in January 2020. It is possible the pandemic impacted the length of some awards.

^cAs of October 2022, agencies may issue a phase I award (including modifications) up to \$295,924 and a phase II award (including modifications) up to \$1,972,828 without seeking U.S. Small Business Administration approval. Any award above those levels requires a waiver. Our testing identified any award in scope where the awarded amount was higher than these values by about 50 percent: \$450,000 for a phase I award and \$3 million for a phase II award.

Similarly, our tests based on OIG SBIR fraud detection indicators and our analysis of fraud schemes in SBIR/STTR allowed us to identify other fraud, waste, and abuse risk categories. For instance, OIG fraud detection indicators point to having shared addresses or bank accounts as an indication of potentially affiliated firms. By conducting data matching, we identified 3,267 awardees that shared an address with at least one other business and 469 awardees who shared a bank account and routing number with another business within the System of Award Management data, indicating a potential affiliation risk. Figure 15 shows selected test results related to OIG SBIR fraud detection indicators and previous fraud schemes in SBIR/STTR.

Figure 15: Analytic Tests of Selected Office of Inspector General Fraud Detection Indicators and Fraud Schemes and Results for Awardees with Potential Fraud, Waste, or Abuse Risks



Sources: GAO analysis of U.S. Small Business Administration data; Icons-Studio/stock.adobe.com (icons). | GAO-24-105470

Accessible Data for Figure 15: Analytic Tests of Selected Office of Inspector General Fraud Detection Indicators and Fraud Schemes and Results for Awardees with Potential Fraud, Waste, or Abuse Risks

Test for potential fraud, waste, or abuse risks ^a	Results of risk tests (What we found out of the 10,570 awardees in our scope)
Applicants sharing an address	3,267 awardees shared an address with at least one other business reported in the System for Award Management.
Applicants sharing a bank account	469 awardees shared a bank account and routing number with another business, as reported in the System for Award Management.
Applicants with prior performance issues	17 awardees received awards associated with information found related to prior performance.
Applicants with prior criminal, civil, or administrative cases	7 awardees won at least one award after criminal, civil, or administrative proceedings were initiated.
Applicants with a principal investigator associated with a prior criminal, civil, or administrative case	1 awardee had a principal investigator who worked for a separate awardee with a case resulting in civil settlement without admission of liability.

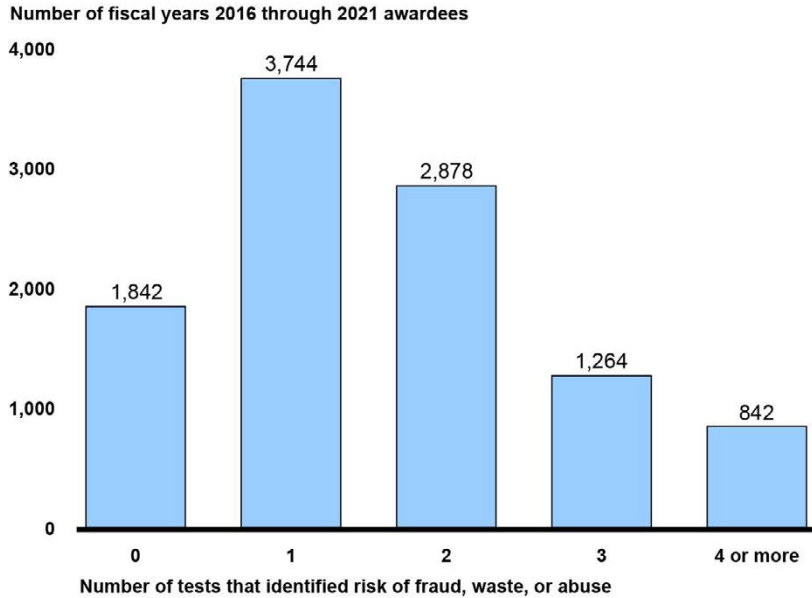
Sources: GAO analysis of U.S. Small Business Administration data; Icons-Studio/stock.adobe.com (icons). | GAO-24-105470

^aFraud involves obtaining something of value through willful misrepresentation (e.g., materially false statements of fact based on actual knowledge, deliberate ignorance, or reckless disregard of falsity). Whether an act is, in fact, fraud is a determination to be made through the judicial or other adjudicative system and is beyond management's professional responsibility for assessing risk. Waste is the act of using or expending resources carelessly, extravagantly, or to no purpose. Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary operational practice, given the facts and circumstances. Although waste and abuse do not necessarily involve fraud or illegal acts, they may be an indication of potential fraud or illegal acts and may still affect the achievement of defined objectives. The presence of such an indicator does not confirm fraud, waste, or abuse.

Combining the results of individual fraud, waste, and abuse risks can further identify awardees that may require additional review for program managers. We combined the results of all 27 analytic tests and found that about 8 percent (842 of 10,570) of awardees from fiscal years 2016 through 2021 were identified in four or

more tests. Figure 16 shows the number of awardees that were identified on different tests. Some awardees were identified on as many as 11 or 12 separate tests. These awardees may pose a higher risk to the SBIR/STTR program. We plan to make referrals for awardees with multiple fraud, waste, and abuse risk indicators to relevant OIGs, as appropriate.

Figure 16: Awardees by Number of Fraud, Waste, or Abuse Risk Indicators Identified in Analytic Tests of Small Business Innovation Research and Small Business Technology Transfer Awards, Fiscal Years 2016 through 2021



Source: GAO analysis of U.S. Small Business Administration data. | GAO-24-105470

Accessible Data for Figure 16: Awardees by Number of Fraud, Waste, or Abuse Risk Indicators Identified in Analytic Tests of Small Business Innovation Research and Small Business Technology Transfer Awards, Fiscal Years 2016 through 2021

Number of tests that identified risk of fraud, waste, or abuse	Number of fiscal years 2016 through 2021 awardees
0	1842
1	3744
2	2878
3	1264
4 or more	842

Source: GAO analysis of U.S. Small Business Administration data. | GAO-24-105470

Data Quality Limitations May Hinder Participating Agencies' Ability to Identify Fraud, Waste, and Abuse Risks

The Small Business Act, as amended, required SBA to develop the Company Registry and SBIR.gov awards databases to reduce vulnerabilities of the SBIR/STTR programs to fraud, waste, and abuse.¹⁰⁶ According to SBA officials, SBA developed and introduced the Company Registry in fiscal years 2013 and 2014. The Company Registry is generally used by businesses to register their information with agencies to participate in the SBIR/STTR programs. Once the applicant receives a SBIR/STTR award, the participating agency must enter the awardee information in SBIR.gov at least quarterly. SBA is then responsible for reviewing awards data in SBIR.gov and reporting the information annually to Congress.

We identified data quality issues in the SBA's Company Registry and the SBIR.gov awards database that may impact efficient identification of fraud, waste, and abuse risks through analytics or other mechanisms perform by participating agencies. Specifically, we found missing, incomplete, and invalid awardee information in key fields in both databases. See table 10.

Table 10: Data Quality Limitations Identified in Our Analysis of the U.S. Small Business Administration's Company Registry

Type of limitation	Company Registry requirements	What we found
Duplicate company records	The Company Registry should not have duplicate business information to ensure that awards are properly associated with the correct company for essentially equivalent work detection and performance benchmark requirements. ^a	We identified 12 records with duplicate information in the Company Registry data. These records shared the same Unique Entity Identifier (Unique Entity ID) ^b values, and most had similar names in the Company Name field, such as small variations in naming, such as "Co." instead of "Company."
Missing data in mandatory fields	The Company Registry should have complete information in required fields to ensure that participating agencies have accurate data to review.	We found nearly 450 of 13,749 awardees with missing values for the number of employees, a required field. We also found awardees with missing social and economic business indicators, such as women-owned and disadvantaged business status.
Inaccurate data values	The Company Registry should have accurate information to ensure that participating agencies have accurate information to reference.	We identified instances where the information was captured but likely inaccurate. For instance, in addition to missing values in the number of employees field, we identified about 300 of 13,749 awardees that listed zero employees. ^c The Policy Directive requires information to be updated no more than 6 months prior to the date of a proposal submission. While some businesses may have accurate information with zero employees for their first (and potentially only) award, those that continue to win awards may not be updating their information, as needed. ^d

Source: GAO analysis of U.S. Small Business Administration data. | GAO-24-105470

¹⁰⁶The Small Business Act, as amended, also included a provision for GAO to review the effectiveness of the databases described in section 9(k) of the Small Business Act (15 U.S.C. § 638(k)) in reducing vulnerabilities of the SBIR/STTR programs to fraud, waste, and abuse, particularly with respect to federal agencies funding duplicative proposals and business concerns falsifying information in proposals.

^aBusinesses with multiple Small Business Innovation Research and Small Business Technology Transfer (SBIR/STTR) awards must meet minimum performance benchmark requirements to be eligible to apply for new awards. The performance benchmark requirements address the extent to which an awardee progresses a project from phase I to phase II and the extent to which an awardee progresses a project from phase II toward commercialization.

^bAs of April 2022, the Unique Entity ID is the primary means of entity identification for federal awards government-wide and is the official identifier for doing business with the U.S. government.

^cIt is unclear to GAO if these are missing values, errors, or values that were unavailable as of our data pull.

^dAccording to U.S. National Science Foundation officials, applicants are required to register in the Company Registry prior to submitting a phase I proposal, and new applicants may not hire their first employee until just prior to the issuance of an award. Officials further noted that having at least one employee on the small business payroll at the time of the SBIR/STTR application is not a program requirement.

Within the SBIR.gov awards database, we identified data quality issues associated with unique identifiers, consistency of information within the Company Registry, and completeness of abstract information. Incomplete, missing, and inaccurate data can hinder the effectiveness of research and analytics, such as data matching. See table 11.

Table 11: Data Quality Limitations Identified in Our Analysis of the U.S. Small Business Administration’s SBIR.gov Awards Database

Type of limitation	What we found
Missing and multiple Data Universal Numbering System (DUNS)	We identified 1,025 awards with blank or zero-filled DUNS numbers. ^a We identified 218 of 10,570 awardees with multiple DUNS numbers or variations across multiple awards. For awards in the time frame of our analysis, DUNS numbers were used as a unique nine-digit identification number to identify awardees. ^b
Consistency of information across U.S. Small Business Administration (SBA) databases	We were required to take steps to match awardee information in the SBA’s SBIR.gov awards database, Company Registry, and the System for Award Management data to ensure that awardee identifying information was accurate and to mitigate missing and incorrect DUNS numbers in SBIR.gov (see above). Though this process, we identified awardee variations in the SBIR.gov awards data, which reduced the ability to perform data analysis. Specifically, it caused us to reduce the number of awardees from 11,405 to our scope of 10,570 unique awardees. For example, we identified one awardee in SBIR.gov with an in-scope award where the awardee’s business name associated with the award did not correspond to the underlying data in SBIR.gov, such as the DUNS number, address, email domains, and the awardee name placed within the abstract. Through our supplemental data linking, we matched this award to the correct awardee to remedy the error and conduct our testing.
Completeness of abstracts	Among the 38,206 awards made from fiscal years 2016 through 2021, we identified 1,908 that had abstracts with fewer than 42 total words. ^c Of these, 179 had fewer than 50 total characters and include abstracts with incomplete phrases, such as “TBD,” “XXX,” and “JBHJHJU.” We identified an additional 1,097 awards that may not include the full abstract. ^d These abstracts contained fewer than 200 words and did not contain selected punctuation, such as periods, closed parentheses, or greater than signs, which may indicate the end of a statement within the abstract.

Source: GAO analysis of U.S. Small Business Administration data. | GAO-24-105470

^aThe majority of awards with missing or zero-filled DUNS numbers were from 2016 and 2017. SBA has implemented controls to improve data quality and, from 2018 onward, there were fewer than 25 blank or defaulted DUNS values each year.

^bThe DUNS number is a unique nine-digit identifier for businesses provided by Dun & Bradstreet. Although the DUNS number is a valuable field for assuring more reliable data checks and matching compared with business name, it was not a mandatory field within the awards data. On April 4, 2022, the federal government transitioned from using the DUNS number to the Unique Entity Identifier (Unique Entity ID). The Unique Entity ID, which replaced DUNS numbers in 2022, is required for new applicants, as of April 2024.

^cWe selected 42 words that represented the fifth percentile of total words across the 38,206 abstracts in our awards data. Participating agencies may redact award abstracts for security reasons.

^dParticipating agencies are required to develop policies and procedures to avoid funding essentially equivalent work already funded by the same, or another, agency, which may include searching SBIR.gov prior to granting an award for similar abstracts, among other things. For this analysis, we

reviewed all awards made in fiscal years 2016 through 2021 to identify all abstracts with potential data quality issues. Given that awardees can have multiple awards, we reported this analysis according to awards. We reviewed award abstracts in our scope and calculated that the median number of words per abstract was 211 words. For all awards below 200 words, we identified if the abstract was missing selected ending punctuation, suggesting that the abstract was cut off or incomplete.

For both SBIR.gov awards data and the Company Registry, SBA stated that it reviews and requests corrections for related data from participating agencies for accuracy and completeness. For example, SBA explained that the Company Registry primarily reflects business-reported information, but participating agencies may also create an “on-the-fly” applicant record, if the agency cannot locate an applicant in the database. According to SBA, “on-the-fly” business creation helps agencies facilitate the timely receipt of award and annual reporting information.

SBA acknowledged that the practice of using “on-the-fly” creations in the Company Registry has resulted in instances where business information is duplicated, and necessary data fields are incomplete or inaccurate. SBA officials stated that they correct these errors annually when performing benchmarking analysis.¹⁰⁷ According to SBA officials, SBA only provides limited validation of the Company Registry because much of the self-reported data may not be easily validated.

Further, SBA stated that it has enhanced its linkages to the System for Award Management to help agencies verify some applicant-reported information, such as information related to business type.¹⁰⁸ However, the enhanced linkages do not help improve other key fields useful for verifying applicant-reported information and identifying ineligible awardee risks, such as those related to foreign ownership and business size, among others. Relatedly, while SBA places no limits on the abstract length, it does require that the abstract be more than zero characters, according to the data dictionary. We identified no guidance to participating agencies on ensuring that sufficient information is collected in the abstract to identify essentially equivalent work. Further, SBA officials stated that they will generally not make changes to the underlying data in SBIR.gov, even if they find a potential issue, as the agency is the authoritative source for information.

Federal Internal Control Standards direct managers to use quality information to achieve the entity’s objectives.¹⁰⁹ Quality information is appropriate, current, complete, accurate, accessible, and provided on a timely basis. These standards also direct managers to communicate the necessary quality information both internally and externally. Furthermore, GAO’s Fraud Risk Framework directs agencies to design and implement control activities—such as data analytics—for effective fraud risk management.¹¹⁰ These analytics could include data matching to verify key information, such as self-reported data, to effectively prevent and detect instances of potential fraud.

Without complete and accurate applicant and awardee data within Company Registry and SBIR.gov—including ownership, unique identifiers, business size, abstracts, and other information—participating agencies are

¹⁰⁷Annually, SBA performs benchmarking calculations to ensure that SBIR/STTR phase I applicants that have won multiple, prior SBIR/STTR awards are progressing toward commercialization. The phase I-to-phase-II transition rate benchmark applies when a small business has received 21 or more phase I awards during the past 5 fiscal years, excluding the most recently completed fiscal year. It requires the small business to average a ratio of phase II-to-phase-I awards of at least 0.25, meaning that the business must average one phase II for every four phase I awards received during the measurement period.

¹⁰⁸According to SBA, it has successfully linked 88 percent of registered businesses to SAM.gov for fiscal years 2017 through 2020 data.

¹⁰⁹[GAO-14-704G](#).

¹¹⁰[GAO-15-593SP](#).

limited in their ability to effectively identify eligibility risks at award. Some agencies reported that using SBIR.gov for risk identification was challenging because updates to applicant information are delayed, and the SBIR.gov awards data do not contain sufficient information to make the determination. The allowance of missing or incomplete Company Registry information makes agencies' review of data from SBIR.gov potentially unreliable and may also indicate that applicants are not updating their information in a timely manner, as required by the Policy Directive.

Further, incorrect and incomplete data can limit participating agencies' efforts to leverage data analytics to identify potential fraud, waste, and abuse risks associated with awards and applicants to comply with due diligence efforts. For example, incomplete abstract information limits the utility of performing analyses to identify essentially equivalent work. Abstracts that have limited words or typos restrict participating agencies from effectively searching for essentially equivalent work.

Conclusions

SBA and participating agencies apply a variety of tools to combat fraud in the SBIR/STTR programs. For example, the SBA's website of prosecuted instances of fraud, monthly program manager meetings, antifraud training, and the fraud risk assessments undertaken by some participating agencies are all positive elements of antifraud efforts. Nevertheless, we found limitations in how SBA and agencies are applying the tools, and our work demonstrates opportunities to further protect the SBIR and STTR programs from fraud.

The SBA's website of SBIR/STTR convictions and findings of civil liability is designed to serve as a deterrent to potential fraudsters. However, information gaps related to the SBA's searches and agencies' reporting of cases limit the SBA's website's utility as a deterrent against fraud. Applying more comprehensive search terms, or legal research tools to identify fraud-related convictions and findings of civil liability, would better position SBA to address these gaps. In addition, leveraging monthly program manager discussions with participating agencies to ensure timely contributions to the website can help SBA ensure that agencies are meeting the 15-day requirement to report such cases to SBA.

Antifraud training is a key control for fraud prevention. While most participating agencies have processes in place to ensure that program officials, applicants, and awardees receive fraud, waste, and abuse training, as required, two did not. Specifically, DOD subcomponents did not train program officials, and USDA did not train applicants. Ensuring that program officials and applicants receive required training supports fraud, waste, and abuse prevention goals. Further, the SBA's annual survey to agencies offers opportunities for SBA to identify and address gaps in agencies' compliance in meeting these training requirements.

Fraud risk assessments are foundational to robust antifraud efforts for the SBIR/STTR programs and support the fraud, waste, and abuse prevention goals of the SBA's Policy Directive. Such assessments are a leading practice from GAO's Fraud Risk Framework and part of a strategic approach to fraud prevention, as required by the Policy Directive. Participating agencies have taken a variety of approaches in assessing program risks, but these were often limited with respect to assessing SBIR/STTR-specific fraud risks. In support of the Policy Directive goals for fraud, waste, and abuse, SBA is positioned to issue guidance reinforcing participating agencies' fraud risk assessment requirements for their SBIR/STTR programs. Such guidance would support agency awareness of the need to conduct fraud risk assessments and use available information on fraud risks for a robust assessment, among other elements of a comprehensive assessment.

Accurate and complete data enable participating agencies to verify applicant and awardee information—a key control for assuring that ineligible entities do not receive SBIR/STTR awards. Incomplete and inaccurate applicant and awardee data within the Company Registry and SBIR.gov limit participating agencies' ability to effectively identify eligibility risks at award and potential fraud, waste, and abuse risks associated with awards and applicants. SBA generally does not make changes to underlying data in these systems, even if errors are identified, which can make the use of these data potentially unreliable. However, correcting errors and ensuring that key fields, such as business size and address, are accurate would better position participating agencies to identify ineligible applicants and purported research facilities that are not fit for research purposes. SBA is positioned to provide guidance to agencies for ensuring that complete and accurate information is collected for abstracts and addresses to support these efforts. Further, the SBA's actions to validate and correct data in two of its key sources of information relevant to SBIR/STTR awards would support agencies' use of these data for preventing fraud, waste, and abuse.

Recommendations for Executive Action

We are making the following eight recommendations, including six to SBA, one to DOD, and one to USDA.

The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation expands the methods and sources used to identify fraud-related convictions and findings of civil liability to list in the SBA's database, such as through alerts from legal research resources. (Recommendation 1)

The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation leverages its oversight mechanisms to identify, share, and report fraud-related convictions and findings of civil liability to SBIR.gov and address participating agencies' challenges in understanding and meeting the 15-day reporting requirement. (Recommendation 2)

The Secretary of the U.S. Department of Agriculture should ensure that the Director of the National Institute of Food and Agriculture ensures that USDA SBIR/STTR applicants receive fraud, waste, and abuse training. (Recommendation 3)

The Secretary of Defense should ensure that the DOD Office of the Under Secretary of Defense for Research and Engineering SBIR/STTR Program ensures that DOD SBIR/STTR subcomponent program officials receive fraud, waste, and abuse training. (Recommendation 4)

The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation leverages its existing oversight mechanisms to ensure the accuracy of agencies' survey responses to required fraud, waste, and abuse training and, to the full extent of the SBA's legal authority, shares SBIR/STTR fraud risk information and resources for conducting fraud risk assessments. (Recommendation 5)

The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation, to the full extent of the SBA's legal authority, provides guidance to participating agencies to conduct comprehensive SBIR/STTR program fraud risk assessments, including all key elements, in support of the Policy Directive's fraud, waste, and abuse prevention requirements and consistent with Fraud Risk Framework leading practices. (Recommendation 6)

The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation improves SBIR.gov data quality by updating guidance to require that abstracts are sufficiently complete and that applicant and awardee addresses are verified to support program eligibility determinations. (Recommendation 7)

The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation validates existing information in the SBIR/STTR databases, specifically the Company Registry and SBIR.gov, to identify and correct deficiencies, as appropriate. (Recommendation 8)

Agency Comments and Our Evaluation

We provided a draft of this report to SBA and the 11 participating agencies—Commerce, DHS, DOD, DOE, DOT, Education, EPA, HHS, NASA, NSF, and USDA, as well as their OIGs, for review and comment. Two agencies—SBA and USDA—provided written comments, which are reproduced in appendixes V and VI. Four agencies—Commerce, DHS, SBA, and USDA—provided technical comments, which we incorporated, as appropriate. Eight agencies—DOD, DOE, DOT, Education, EPA, HHS, NASA, and NSF—and the 12 agencies' OIGs had no technical or written comments.

In their comments, SBA and DOD concurred with our recommendations, while USDA generally concurred.

SBA concurred with our six recommendations. In its comments, SBA highlighted recent efforts in which it has (1) improved the data quality within SBIR.gov; (2) instituted processes for participating agencies' implementation of the SBIR/STTR Policy Directive minimum fraud, waste, and abuse requirements; (3) established a repetitive, and consistent, process to list fraud-related convictions and findings of civil liability on SBIR.gov; and (4) initiated discussions around newly resolved fraud cases and frequent fraud schemes during the SBA-led monthly SBIR/STTR program managers' meetings. However, SBA further noted that, as the report demonstrates, opportunities exist to do more, and is committed to taking appropriate actions within the confines of its legal authority and resources to further strengthen protections against fraud and reduce potential vulnerabilities.

DOD concurred, by email from the Director of the Defense SBIR/STTR Program Office for the Office of the Under Secretary of Defense for Research and Engineering, with our recommendation to ensure that DOD SBIR/STTR subcomponent program officials receive fraud, waste, and abuse training.

USDA generally concurred with our recommendation to ensure that USDA SBIR/STTR applicants receive fraud, waste, and abuse training. In its comments, USDA stated that the National Institute of Food and Agriculture is planning to incorporate fraud, waste, and abuse training into technical webinars provided to SBIR/STTR applicants.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, and Transportation; the Administrators of the SBA, EPA, and NASA; the Director of NSF; and other interested parties.

In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

Letter

If you or your staff have any questions about this report, please contact me at (202) 512-6722 or SheaR@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 VII.

A handwritten signature in black ink that reads "Rebecca Shea". The signature is written in a cursive, flowing style.

Rebecca Shea
Director
Forensic Audits and Investigative Service

List of Committees

The Honorable Jeanne Shaheen
Chair
The Honorable Joni Ernst
Ranking Member
Committee on Small Business and Entrepreneurship
United States Senate

The Honorable Frank D. Lucas
Chairman
The Honorable Zoe Lofgren
Ranking Member
Committee on Science, Space, and Technology
House of Representatives

The Honorable Roger Williams
Chairman
The Honorable Nydia M. Velázquez
Ranking Member
Committee on Small Business
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The Small Business Act, as amended, includes a provision for GAO to review every 4 years what the participating agencies and agency Offices of Inspector General (OIG) are doing to prevent; identify; respond to; and reduce fraud, waste, and abuse in the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs.¹ Our prior reports were issued in June 2021, April 2017, and November 2012.²

This fourth report (1) describes SBIR/STTR fraud schemes for fiscal years 2016 through 2023, participants, and impacts; (2) evaluates the extent to which selected U.S. Small Business Administration (SBA) and participating agency antifraud activities align with program fraud, waste, and abuse prevention requirements and leading practices; (3) evaluates the extent to which agencies assessed fraud risks in alignment with leading practices; and (4) evaluates the extent to which applicant and award data from fiscal years 2016 through 2021 indicate vulnerabilities to fraud, waste, and abuse and identifies opportunities for participating agencies and SBA to leverage data analytics.

For all objectives, we reviewed relevant laws; regulations; prior court cases; and guidance, including the SBIR.gov website and the SBA's Policy Directive. We also interviewed program officials from participating agencies and SBA to gain further understanding on how the program operates and any steps reported by the agencies to mitigate potential fraud, waste, and abuse.³ We also received written responses from the co-chairs of the SBIR Investigations Working Group to describe investigative efforts to date; use of information to inform fraud, waste, and abuse investigative efforts; and any challenges experienced.

For our first objective, to understand SBIR/STTR fraud schemes, participants, and impacts, we analyzed 60 publicly reported criminal, civil, and administrative actions initiated or resolved during fiscal years 2016 through 2023 and closed by the end of fiscal year 2023. We selected fiscal years 2016 through 2023 to align with our data testing of awards made during fiscal years 2016 through 2021 and to capture the most recent information available as of our mandated reporting in fiscal year 2024. To identify criminal, civil, and administrative actions, we obtained U.S. Department of Justice (DOJ) press releases through a subscription to Westlaw and used other available sources, such as the SBIR.gov and Law360 websites.⁴ We included search terms, such as "Small Business Technology Transfer," and acronyms like STTR. We reviewed these search results for

¹15 U.S.C. § 638b(b). Responsibility for investigating fraud, waste, and abuse in SBIR and STTR programs is typically found within the participating agencies' OIGs. However, in the three Department of Defense (DOD) military departments of the Army, Navy, and Air Force, investigative responsibilities are instead located in the Army Criminal Investigation Command, Naval Criminal Investigative Service, and Air Force Office of Special Investigations. We refer to them collectively as the OIGs and military investigative offices.

²GAO's provision includes reviewing the effectiveness of the risk management strategies of each federal agency that participates in the SBIR or STTR program in identifying areas of the programs that are at high risk for fraud and the success of each federal agency that participates in the SBIR or STTR program in reducing fraud, waste, and abuse in the programs of the federal agency, among other things. Previous reports include GAO, *Small Business Innovation Research: Agencies Need to Fully Implement Requirements for Managing Fraud, Waste, and Abuse*, [GAO-21-413](#) (Washington, D.C.: June 30, 2021); *Small Business Research Programs: Additional Actions Needed to Implement Fraud, Waste, and Abuse Prevention Requirements*, [GAO-17-337](#) (Washington, D.C.: Apr. 15, 2017); and *Small Business Research Programs: Agencies Are Implementing New Fraud, Waste, and Abuse Requirements*, [GAO-13-70R](#) (Washington, D.C.: Nov. 15, 2012).

³Participating agencies' program officials include any staff or personnel that have a role in managing and coordinating the SBIR/STTR programs.

⁴Westlaw and Law360 are legal news services.

relevancy to our audit objective and scope to identify actions for additional review. For the actions we identified for review, we searched the System for Award Management for additional, related administrative actions, if any. We also obtained relevant court documents from Public Access to Court Electronic Records and requested documents, as necessary, from participating agencies.⁵

These documents contained, among other things, information about charged individuals and businesses and judgment and settlement amounts. Using this information, we conducted thematic analyses based on the GAO Conceptual Fraud Model to understand commonalities of actions related to SBIR/STTR programs.⁶ We analyzed information from the actions to identify fraud schemes and analyzed and identified their characteristics and impacts on SBIR and STTR. A single fraud scheme may relate to one or more actions. We selected fraud schemes to use as illustrative examples of how fraud occurred. These illustrative examples are not generalizable to other schemes.

Our analysis is limited to schemes we identified based on closed criminal, civil, and administrative actions that were reported publicly in the sources listed above. For the purposes of our analysis, we considered criminal and civil actions as closed when they reached conclusion through a guilty plea, settlement, dismissed charges, or a verdict at trial. We considered actions as ongoing when they had not reached a conclusion as of September 30, 2023. Some ongoing actions may have since reached conclusions but are not reflected in our analysis.

To examine reported financial impacts associated with SBIR/STTR fraud schemes, we analyzed restitution, cash and noncash forfeitures, and fines associated with criminal convictions. Our results may include restitution, cash and noncash forfeitures, and fines that were court ordered but not necessarily paid. We also analyzed settlement amounts associated with civil settlements with and without admissions of liability. These figures do not account for all the financial impacts of adjudicated SBIR/STTR fraud schemes, such as detection, investigation, and prosecution costs; the costs of negotiating civil settlements and administrative agreements; or the costs of SBIR/STTR funds going to ineligible awardees. Further, the full extent of fraud is difficult to measure because some fraud schemes may remain undetected by the government, and others may not yet or ever be adjudicated.

Finally, to describe nonfinancial impacts of SBIR/STTR fraud schemes, we developed a framework that identified nonfinancial ways in which fraud against SBIR and STTR can manifest itself. We primarily relied on areas of impact identified in the GAO Conceptual Fraud Model and the International Public Section Fraud Forum's *Guide to Understanding the Total Impact of Fraud*.⁷ Using our review of the areas of impact identified in GAO's Conceptual Fraud Model and the forum's guide, and considering the relevance of impact areas in the context of the SBIR/STTR programs, we selected six areas of nonfinancial impact to examine further in our analysis. For each area of nonfinancial impact, we developed definitions relevant to the SBIR/STTR context

⁵Public Access to Court Electronic Records is a service of the federal judiciary that enables the public to search online for case information from U.S. District, Bankruptcy, and Appellate courts. Federal court records available through this system include case information (such as names of parties, proceedings, and documents filed), as well as information on case status.

⁶The model is organized as an ontology, which provides an explicit description of categories of federal fraud, their characteristics, and the relationships among them. GAO, *GAO Fraud Ontology Version 1.0* (Washington, D.C.: Jan. 10, 2022), https://gaoinnovations.gov/antifraud_resource/howfraudworks.

⁷International Public Sector Fraud Forum, *Guide to Understanding the Total Impact of Fraud* (February 2020). The forum was established in 2017 by government officials from Australia, Canada, New Zealand, the United Kingdom, and the United States. The goal of the forum is to use shared knowledge to reduce the risk and harm of fraud and corruption in the public sector across the world.

and informed by GAO's Conceptual Fraud Model and the International Public Sector Fraud Forum's guide. For each area of impact, we developed statements of impact based on our analysis of SBIR/STTR fraud schemes. The areas of impact we identified, and our statements of impact, may not encompass all nonfinancial impacts of SBIR/STTR fraud schemes.

For the second objective, we assessed the efforts of SBA and the 11 participating agencies to manage fraud risks against the SBA's 2020 Policy Directive and leading practices in GAO's *Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework), as appropriate. We included all subcomponents issuing SBIR/STTR awards from fiscal years 2016 through 2021 for the five participating agencies with multiple subcomponents that participate in the SBIR/STTR programs—the U.S. Department of Commerce, DOD, the U.S. Department of Energy (DOE), the U.S. Department of Homeland Security (DHS), and the U.S. Department of Health and Human Services (HHS). As a result, we included 23 agency subcomponents in the scope of our review. We assessed SBA's oversight efforts against component 1 leading practices and its guidance (2020 Policy Directive) against leading practices in components 1 through 4 of GAO's Fraud Risk Framework to determine the extent to which the guidance addressed the leading practices (see app. III). Further, we interviewed SBIR/STTR program officials from the 11 participating agencies and their OIGs regarding their efforts to improve training and develop SBIR fraud detection indicators and took actions to address GAO's open recommendations.⁸

For the third objective, we interviewed SBA officials to discuss their fraud, waste, and prevention guidance. We also interviewed officials from the 11 participating agencies to describe how they identify, assess, and manage program fraud risks. Specifically, we interviewed agency program officials in 2022 and executed additional follow-up in March and April 2023 to determine whether they conducted or contributed to SBIR/STTR-specific fraud risk assessments.

We used Fraud Risk Framework component 2 leading practice related to planning regular fraud risk assessments to determine which participating agencies and subcomponents were relevant to our fraud risk assessment evaluation. We determined that, as of April 2023, three participating agencies—(1) DOE, (2) DHS, and (3) HHS, which included documentation from five subcomponents across these agencies—were relevant for additional review.⁹

We evaluated applicable fraud risk profiles and assessments against component 2 leading practices of the Fraud Risk Framework to determine whether participating agencies developed comprehensive fraud risk assessments that identified, analyzed, and responded to inherent fraud risks.¹⁰ Specifically, we evaluated the applicable fraud risk profiles and assessments to determine whether they contained key elements of the fraud risk assessment process under component 2. These key elements are (1) identifying inherent fraud risks affecting the program, (2) assessing the likelihood and impact of inherent fraud risks, (3) determining fraud risk

⁸Of the 21 recommendations we made in June 2021, three recommendations remain open for two DOD subcomponents that participate in the SBIR/STTR programs, as of May 2024. [GAO-21-413](#).

⁹We evaluated the most recent subcomponent documentation, as of April 2023, according to agency SBIR/STTR officials from the U.S. Department of Energy's Advanced Research Projects Agency – Energy and Office of Science fraud risk profiles; the U.S. Department of Health and Human Services' National Institutes of Health's Extramural Grant Program fraud risk profile; and the U.S. Department of Homeland Security's Countering Weapons of Mass Destruction and Science and Technology fraud risk assessment.

¹⁰As discussed in the Fraud Risk Framework, a fraud risk profile of the basis of an overall antifraud strategy that informs the design and implementation of specific fraud control activities should also include managers' risk tolerance and prioritization, among other things. GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015).

tolerance, (4) examining suitability of existing fraud controls and prioritizing residual fraud risks, and (5) documenting the program's fraud risk profile. We also evaluated the extent to which the fraud risk profiles and assessments demonstrated the use of available stakeholder fraud risk information, specifically, OIG fraud detection indicators.¹¹

To determine the extent to which the fraud risk profiles and assessments identified and assessed inherent SBIR/STTR fraud risks, we used a two-reviewer methodology. Specifically, the two reviewers independently evaluated the five subcomponents' fraud risk profile and assessment to identify all fraud-related information, including all instances where one or more of the following terms are used: "fraud," "waste," and "abuse," or where the agency identified fraud scheme and fraud risk, among other things. Each reviewer then determined which GAO-identified category the information addressed and compared the independent data collection instruments to identify and reconcile any inconsistencies and validate the results. The reviewers then used the identified fraud-related information to determine whether it addressed the 21 SBIR/STTR fraud, waste, and abuse categories and demonstrated the subcomponents' use of related OIG fraud detection indicators, where available (see app. IV).

For the fourth objective, we interviewed SBA officials to determine how mandated SBIR/STTR awards data are managed and interviewed officials from the 11 participating agencies to describe how they identify, assess, and manage applicant and awardee fraud risks. We also analyzed the extent to which SBA and agencies' practices align with relevant leading practices in GAO's Fraud Risk Framework, as well as principles in the *Standards for Internal Control in the Federal Government* (Federal Internal Control Standards).

We matched participating agencies' fiscal years 2016 through 2021 SBIR/STTR program awards data to government contracting and grant performance, wage, exclusions, and other data to identify potential fraud, waste, and abuse, as well as to assess data reliability. We selected this scope of awards, given that it was the most complete set of more than 5 years of awards data at the time of our review. We used 6 years of awards data to perform SBIR/STTR benchmarking calculations.¹²

Using data analysis, we selected 12 awardees associated with 17 addresses for further investigative review. GAO criminal investigators performed site visits to the addresses to verify their accuracy and whether the facility at the address could physically support the research described in the awardee's application. These addresses were selected to highlight examples of potentially ineligible addresses. Results from our analysis and investigation where we found the presence of fraud, waste, or abuse risks will result in referrals to relevant agency OIGs for further investigation.

Our data work focused on all phase I and phase II awards and awardees from fiscal years 2016 through 2021. The awards in our scope are publicly available from SBIR.gov for download. The data are maintained by SBA and are regularly updated with new awards and updates to previously uploaded awards. We pulled our data

¹¹The Policy Directive requires that participating agencies collaborate with their OIGs on developing SBIR fraud detection indicators. Fraud detection indicators range from specific fraud risks—such as "bait-and-switch" schemes, in which contractors propose an experienced researcher as the principal investigator and then use a less-qualified, lower-cost employee to serve in that role—to general indicators of potential fraud, such as significant levels of foreign ownership.

¹²The phase I-to-phase-II transition rate benchmark only applies when a small business has received 21 or more phase I awards during the past 5 fiscal years, excluding the most recently completed fiscal year. It requires the small business to average a ratio of phase II-to-phase-I awards of at least 0.25, meaning that the business must average one phase II for every four phase I awards received during the measurement period.

from the SBIR.gov awards website on January 4, 2023. We did not use commercialization data to phase III awards, as well as the awards made under this program in our analysis.

We primarily designed 27 selected analytical tests to search for potential fraud, waste, and abuse through a review of fraud risks identified by the 11 participating agencies' OIGs. As part of the 10 minimum requirements to combat fraud, waste, and abuse, each agency OIG created a list of fraud detection indicators related to the SBIR/STTR programs. We reviewed the indicators to determine their feasibility for testing with available data, complexity required to create a test, and timing required to create the test. Once we determined that a fraud, waste, or abuse risk would be viable for testing, we designed custom analytics to identify potential fraud, waste, and abuse leading practices in the Fraud Risk Framework.¹³ Analytics were also designed based on review of the Policy Directive, SBIR.gov, and discussions with our investigators. A relevant leading practice from the Fraud Risk Framework encourages agencies to conduct data analytics activities to prevent and detect fraud. For example, agencies can consider program rules and known or previously encountered fraud schemes to design analytic tests. Where able, agencies can combine data across programs and from separate databases to facilitate analytics and to verify applicant information. Additionally, agencies can conduct data mining to identify inconsistencies and other anomalies within the data.

Data Quality and Validation

We took steps to review data reliability, as well as to ensure the accuracy of the SBIR.gov awards data, as well as other-sourced information used for testing and to standardize the data, where necessary. All data were reviewed to ensure that fields were imported correctly, as well as contained the appropriate information for testing. Any limitations on the data were documented and determined to not cause a material impact to test for potential fraud, waste, and abuse.

To create the designed tests related to potential fraud, waste, and abuse in the SBIR/STTR programs, we obtained awards data available publicly. The data are maintained by SBA and updated constantly to incorporate new awards and to update previously uploaded awards. We filtered down to only the years in scope for our testing, fiscal years 2016 through 2021. We reconciled the awards data to the SBIR/STTR annual reports created by SBA to ensure the accuracy of our data pull and filtering to awards in scope. No unexplainable variances were noted when reconciling the data.

We also obtained the Company Registry data from SBA, which contained awardees from fiscal year 2012 onward, which were provided on November 30, 2022. The Company Registry was used to standardize the groupings (by name and Dun & Bradstreet Data Universal Numbering System (DUNS number)) within the awards data. We used, in addition to data maintained by SBA, data sources to perform the tests described below.

- To review applicant registration information and compare award characteristics, we obtained monthly System for Award Management data, which contained data from January 2016 through August 2021.¹⁴

¹³GAO-15-593SP.

¹⁴The General Services Administration's System for Award Management is the central registration point for businesses seeking contracts with the federal government. The System for Award Management also contains information on contractors that have been excluded from receiving federal contracts, such as due to suspensions and debarments.

- To review employee counts, as well as to compare principal investigator wage data, we used 1 year of national quarterly wage data from HHS's National Directory of New Hires for the period ending September 30, 2020. The National Directory of New Hires is a national database of wage and employment information. The National Directory of New Hires is maintained and used by HHS for the assistance of state child support agencies in locating parents and enforcing child support orders. These data may not be available to participating agencies for use.
- To review potential suspensions and debarments to awardees, we obtained:
 - the General Services Administration's System for Award Management exclusions file, as of August 2021;
 - the General Services Administration's Federal Awardee Performance Integrity Information System,¹⁵ as of September 12, 2022;
 - the U.S. Department of Commerce's Consolidated Screening List,¹⁶ as of September 12, 2022; and
 - the World Bank's Listing of Ineligible Firms and Individuals,¹⁷ as of September 12, 2022.

We reviewed the quality of all data to ensure that it was appropriate for our tests. We identified quality concerns in the data, such as typos, missing information, or potentially duplicative businesses, but these were not of material significance enough to prevent our analysis.

For our analysis identifying potential fraud, waste, and abuse, we performed multiple steps and procedures:

- We submitted the address listed for each award into the United States Postal Service's Address Matching System to identify delivery information for each award. This test was designed to identify potentially ineligible addresses, such as commercial mail-receiving agencies that might suggest a potential for fraud. We considered the results of the United States Postal Service's Address Matching System for further investigation. Businesses (SBIR/STTR awardees) considered for further investigation were limited to those with awards in fiscal year 2021, which were the latest awards in our scope.
- We matched awards data to the SBA's Company Registry to ensure that we were able to group the awards to the appropriate awardees. We used a multipart waterfall matching technique to match between the awards data and registry data to ensure accuracy. We matched data on a combination of the DUNS number, business name, and ZIP code between the two files. Matching between the two data sets allowed us to standardize the DUNS identifier for each award, as well as the business name on the award. We then matched the matched data to System for Award Management data in a similar

¹⁵The Federal Awardee Performance and Integrity Information System data were downloaded from FAPIIS.gov in September 2022. In December 2022, the Federal Awardee Performance and Integrity Information System was transitioned to SAM.gov and was renamed to responsibility/qualification.

¹⁶The Consolidated Screening List is a list of parties for which the U.S. government maintains restrictions on certain exports, reexports, or transfers of items and consolidates multiple export screening lists of the U.S. Departments of Commerce, State, and the Treasury.

¹⁷The World Bank Listing of Ineligible Firms and Individuals is a listing of ineligible businesses and individuals with a sanction imposed as a result of (1) an administrative process conducted by the World Bank that permitted the accused businesses and individuals to respond to the allegations; or (2) cross-debarment, in accordance with the Agreement for Mutual Enforcement of Debarment Decisions made effective by the World Bank, Asian Development Bank, European Bank for Reconstruction and Development, Inter-American Development Bank, and African Development Bank.

manner by a combination of the DUNS number, business name, and ZIP code using a waterfall technique. We did this to further validate and group the data, provide the Employer Identification Number for future matching, and to standardize the DUNS number and business names for grouping of awards to awardees.

- Once we grouped the awards by business, we performed various tests to identify potential fraud, waste, and abuse. See table 12 for a description of the 27 analytic tests performed, limitations of the testing, and fraud risk categories covered by the test.

Table 12: Analytic Tests Designed and Performed to Identify Potential Fraud, Waste, or Abuse Risks in Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs

Test performed	Description	Fraud, waste, or abuse risk categories
Agency employees also identified as award winners	The Policy Directive cautions that awards made to applicants owned by, or employing, current or previous federal government employees may create conflicts of interest. We used the National Directory of New Hires quarterly wage data to identify individuals employed by both participating agencies and award winners.	Conflict of interest Misrepresentation during the award life cycle ^a
Award outliers	SBIR/STTR programs have funding thresholds for phase I and phase II awards, \$295,924 and \$1,972,828, respectively. ^b We analyzed for awards that exceeded these thresholds by more than 50 percent.	Agency oversight Number or type of awards Program compliance
Awards to employee ratio	Participating agencies' Offices of Inspector General (OIG) identified businesses with an improbable number of awards for the number of employees as a SBIR OIG fraud detection indicator. We reviewed the National Directory of New Hires quarterly wage data and calculated the ratio of awards to employees.	Number or type of awards
Benchmarking recalculations	The Policy Directive provides guidance on the phase II transition rate that sets a minimum required rate of progress from phase I to phase II over a specified period. ^c We analyzed for awardees that did not meet this benchmark.	Number or type of awards Poor performance Program compliance
Business address	The Policy Directive states that during the performance of award, the research and development will be performed at the awardee's facilities by the awardee's employees. We used the United States Postal Service Address Matching System to identify awards where the address listed was potentially ineligible.	Misrepresentation during the award life cycle Research facilities Shell company

Appendix I: Objectives, Scope, and Methodology

Test performed	Description	Fraud, waste, or abuse risk categories
Business size	A SBIR/STTR awardee, together with its affiliates, must not have more than 500 employees, with some exceptions, at the time of award. ^d We used the National Directory of New Hires wage quarterly data to calculate the average number of employees across the 1 year of data available. We also used the System for Award Management to identify awardees with more than 500 employees as reported in the data as of the award year.	Affiliated firms Misrepresentation during the award life cycle
Business's socially and economically disadvantaged status	One purpose of the SBIR/STTR programs is to foster and encourage participation by socially and economically disadvantaged businesses, and by women-owned businesses, in technological innovation. We analyzed for awardees with inconsistencies in self-reported characteristics award data and the System for Award Management.	Misrepresentation during the award life cycle
Email aliases	Prior GAO work has identified email aliases, the creation of various email addresses that route to a single address, as a potential fraud risk. We analyzed for email variations within the point of contact and principal investigators.	Principal investigator Shell company
Essentially equivalent work (duplicative awards)	The Policy Directive states that SBIR/STTR applicants often submit duplicate or similar proposals to more than one soliciting agency when the announcement or solicitation appears to involve similar topics or requirements. However, essentially equivalent work must not be funded in the SBIR/STTR or other federal agency programs. We analyzed for awards with a high percentage of shared unique words between abstracts.	Essentially equivalent work Misrepresentation during the award life cycle
Foreign ownership	SBIR or STTR awards typically must be more than 50 percent owned or controlled by citizens or permanent residents of the United States. ^e We analyzed for awardees and affiliates with self-reported foreign ownership as listed in the System for Award Management.	Affiliated firms Foreign ownership Misrepresentation during the award life cycle
Frequent award winners across multiple agencies	Participating agencies' OIGs identified businesses with many awards across multiple agencies as a SBIR fraud detection indicator. We analyzed for awardees that were in the 95th percentile of number awards received across multiple agencies within our scope from fiscal years 2016 through 2021.	Conflict of Interest Number or type of awards

Appendix I: Objectives, Scope, and Methodology

Test performed	Description	Fraud, waste, or abuse risk categories
Frequent award winners within a single agency	Participating agencies' OIGs identified businesses with many awards across a single agency as a SBIR fraud detection indicator. We analyzed for awardees that were in the 95th percentile of number awards received from a single agency within our scope from fiscal years 2016 through 2021.	Conflict of Interest Number or type of awards
Government or military email	The Policy Directive cautions that awards made to businesses owned by, or employing, current or previous federal government employees may create conflicts of interest. We analyzed for government and military email identifiers in the point of contact and principal investigators.	Conflict of Interest Misrepresentation during the award life cycle Principal investigator
Highest awarded awardees within an agency	Participating agencies' OIGs identified businesses with many awards across a single agency as a SBIR fraud detection indicator. We analyzed for awardees who were in the 99th percentile of award money received from a single agency within our scope from fiscal years 2016 through 2021.	Conflict of Interest Number or type of awards
Length of award	The Policy Directive states that a phase I award's period of performance normally should not exceed 6 months for SBIR or 1 year for STTR. A phase II's period of performance normally should not exceed 2 years. However, agencies may provide longer performance periods, where appropriate, for a particular project. We analyzed for awards that had a length that was 50 percent greater than the normally prescribed lengths. ^f	Agency oversight Program compliance
Limited liability company	A shell company often uses nonpublicly traded corporations or limited liability companies that have no physical presence beyond a mailing address and that generate little-to-no independent economic value and help conceal the company's true ownership. We analyzed for awardees who self-reported as a limited liability company or used "LLC" in their name. ^g	Shell company
Phase I-to-phase-II modified benchmarking	Participating agencies' OIGs identified businesses with many phase I awards but limited phase II awards as an SBIR OIG fraud detection indicator. We analyzed for awardees at risk of not meeting benchmarking requirements (see benchmarking recalculations test above). ^h	Number or type of awards Poor performance Program compliance

Appendix I: Objectives, Scope, and Methodology

Test performed	Description	Fraud, waste, or abuse risk categories
Principal investigators associated with a prior court case	The Policy Directive states that the U.S. Small Business Administration’s (SBA) SBIR/STTR program database will include a list of any individual or small business concern that has received an SBIR/STTR award and that has been convicted of a fraud-related crime involving SBIR/STTR funds or found civilly liable for a fraud-related violation involving SBIR/STTR funds, of which SBA has been made aware. We analyzed for principal investigators associated with a prior court case listed on awards with a separate awardee.	Principal investigator
Principal investigator on multiple projects	Participating agencies’ OIGs identified businesses with many awards to the same principal investigator as an SBIR OIG fraud detection indicator. Our test analyzed for principal investigators who had seven or more awards with a single awardee in an award year.	Principal investigator
Principal investigator working for another business	The Policy Directive states that for both phase I and phase II, the primary employment of the principal investigator must be with the business at the time of the award and during the conduct of the proposed project. ¹ Our test used the National Directory of New Hires to identify principal investigators who may be working for other businesses or institutions.	Misrepresentation during the award life cycle Principal investigator
Principal investigator working for multiple SBIR/STTR awardees simultaneously	The Policy Directive states that for both phase I and phase II, the primary employment of the principal investigator must be with the business at the time of award and during the conduct of the proposed project. We analyzed the data for principal investigators who are found on multiple SBIR/STTR awardees in an award year.	Affiliated firms Misrepresentation during the award life cycle Principal investigator
Prior court cases	The Policy Directive states that the SBA’s SBIR/STTR program database will include a list of any individual or small business concern that has received an SBIR/STTR award and that has been convicted of a fraud-related crime involving SBIR/STTR funds or found civilly liable for a fraud-related violation involving SBIR/STTR funds, of which SBA has been made aware. We analyzed for any awardees with prior court cases that received awards after the reported court initiation date.	Poor performance
Prior court cases affiliations	Participating agencies’ OIGs identified businesses with previous lawsuits for fraud as a SBIR OIG fraud detection indicator. We analyzed for potential affiliates of awardees with prior court cases.	Affiliated firms Poor performance

Appendix I: Objectives, Scope, and Methodology

Test performed	Description	Fraud, waste, or abuse risk categories
Shared addresses	Participating agencies' OIGs identified businesses with a shared address with another business or residence as a SBIR OIG fraud detection indicator. We analyzed if more than one business could be found at the same physical address listed within the System for Award Management for SBIR/STTR awardees.	Affiliated firms Research facilities Shell company
Shared bank information	Participating agencies' OIGs identified businesses with joint bank accounts as a SBIR OIG fraud detection indicator. We analyzed for awardees who shared bank account and routing information with at least one other business.	Affiliated firms Shell company
Suspensions and debarments	Participating agencies' OIGs identified businesses with a poor history of managing federal awards as a SBIR OIG fraud detection indicator. We analyzed for SBIR/STTR awardees, points of contact, and principal investigators found in four data sources related to suspensions and debarments: the Federal Awardee Performance and Integrity Information System, System for Award Management Exclusions, World Bank Listing of Ineligible Firms and Individuals, and the Consolidated Screening List.	Excluded parties Poor performance Principal investigator
Venture capital operating company ownership	The SBIR/STTR programs allow for participation of businesses that have venture capital operating company ownership. When the venture capital operating company has greater than a 50 percent ownership in the business, there are limitations to the involvement of those businesses. We analyzed for self-reported venture capital operating company ownership in awardees that may be ineligible.	Agency oversight Business ownership Misrepresentation during the award life cycle

Sources: GAO analysis of Office of Inspector General fraud detection indicators and the U.S. Small Business Administration's Policy Directive; Icons-Studio/stock.adobe.com (icons). | GAO-24-105470

^aFor the purposes of this report, an award life cycle includes preaward, during the award, and postaward.

^bAs of October 2023, agencies may issue a phase I award (including modifications) up to \$306,872 and a phase II award (including modifications) up to \$2,045,816, without seeking SBA approval. According to SBA officials, any award above these levels requires a waiver, and such awards are flagged as a part of the SBIR.gov award upload process. Our testing used limits set as of October 2022.

^cThe SBIR and STTR Extension Act of 2022 ("Extension Act"), Pub. L. No. 117–183, 136 Stat. 2180 (2022), amended the application of benchmarks for more experienced firms as of April 2023. The phase I-to-phase-II transition rate benchmark only applies when a company has received 21 or more phase I awards during the past 5 fiscal years, excluding the most recently completed fiscal year. It requires the company to average a ratio of phase II-to-phase-I awards of at least 0.25, meaning that they must average one phase II for every four phase I awards received during the measurement period. This update for more experienced businesses that have won 51 or more phase I awards during the past 5 fiscal years, excluding the most recently completed fiscal year, was not applied to our testing.

^dRegulations require that awardees self-certify that they meet the eligibility requirements at the time of the award. Business size is based on average employees over the previous 24 pay periods. See 13 C.F.R. § 121.106 for calculation of employee size and 13 C.F.R. § 121.704 for when the eligibility of a concern is determined. Small business concerns and entities are affiliates of each other when one controls, or has the power to control, the other, or a third party or parties' controls, or has the power to control, both. It does not matter whether control is exercised, so long as the power to control exists. Affiliation for our data testing purposes was determined by identifying potential relationships between the business and the global parent field within the System for Award Management. All businesses that share a global parent are considered affiliates of one another.

^ePer small business regulations, an eligible applicant must be a small business concern that is more than 50 percent owned and controlled by one or more individuals who are citizens or permanent residents of the United States. 13 C.F.R. § 121.702. Small business concerns may also be owned by an

Appendix I: Objectives, Scope, and Methodology

Indian Tribe, Alaska Native Corporations, Native Hawaiian Organizations, or a wholly owned business entity of such tribe, corporation, or organization; joint ventures that meet certain conditions; and, under certain circumstances, venture capital operating companies, hedge funds, and private equity firms.

^fParticipating agencies may implement policies to extend the time lines to mitigate disruptions between phase I and phase II awards. When taken together with the results of additional tests, such as the principal investigator employment tests, these awardees could present a higher risk of potential fraud, waste, and abuse.

^gA shell company often uses nonpublicly traded corporations or limited liability companies that have no physical presence beyond a mailing address and that generate little-to-no independent economic value and help conceal the company's true ownership. We identified awardees who self-reported as a limited liability company or used "LLC" in their name. When taken together with the results of additional tests, such as address tests, these awardees could present a higher risk of potential fraud, waste, and abuse.

^hAccording to SBA officials, SBA provides a copy of businesses that fail benchmarking requirements to all participating agencies as part of their performance benchmark process. When taken together with the results of additional tests, such as the principal investigator employment and length of award tests, these awardees could present a higher risk of potential fraud, waste, and abuse.

ⁱThis test identified whether a principal investigator received wages from multiple businesses. A principal investigator's primary employment must be more than half of their time with the small business concern. It is possible that the principal investigator is employed by another business at the same time, but not primarily employed.

Results of our analyses may include awardees and awards as having an indicator(s) of potential fraud, waste, or abuse but may have committed no faults and are false positives. Timing, data limitations, and known disclosures unavailable for our analysis, among other reasons, may all contribute to these awards and awardees having no faults in the SBIR/STTR programs. The results of our analyses should not be interpreted as proof of fraud. Additional review, investigation, and adjudication would be needed to determine if, and the extent to which, fraud, waste, and abuse exist in the programs. Our analyses should be viewed as a starting point to focus future review and investigations and to identify potential connections that may exist between various potential fraud indicators and the awardees and awards.

To ensure consistency throughout our coding process of potential fraud, waste, and abuse tests, we used a two-person independent coding approach. Our coding process involved reviewing the relevant materials to create an initial list of tests to be performed, coding those tests, then performing walk-throughs with technical specialists and stakeholders to discuss in real time which tests required further review and adjustment and which should be removed from testing. Once tests were agreed upon, the code used to create them was independently reviewed by a technical specialist outside of the specific project team.

We conducted this performance audit from October 2021 through September 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted our related investigative work from in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

Appendix II: Analysis of Nonfinancial Impacts of Fraud Schemes

We identified various types of nonfinancial impacts of Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) fraud based on our analysis of 37 SBIR/STTR fraud schemes and areas of impact described in the GAO Conceptual Fraud Model and the International Public Section Fraud Forum’s *Guide to Understanding the Total Impact of Fraud*.¹ Our analysis identified nonfinancial impacts of SBIR/STTR fraud schemes on businesses, individuals, and the federal government. As described in the body of the report, fraud schemes impact program goals and those involved in the schemes. Other impacts are described below.

Stakeholder Impact

Investigation and, where applicable, prosecution of SBIR/STTR fraud schemes demanded the resources of law enforcement agencies and the U.S. Department of Justice (DOJ). For example, our analysis identified 30 agencies—including the Offices of Inspector General (OIG) from the U.S. Small Business Administration (SBA) and participating agencies, United States Attorney’s Offices, and others—that contributed to SBIR/STTR fraud investigations. Further, we found that attorneys in 28 of 94 federal districts filed criminal or civil charges or entered civil settlements (including civil settlements without admissions of liability) related to these schemes. Administrative proceedings also demanded resources from participating agencies’ suspension and debarment officials. Specifically, our analysis identified five agencies that took administrative actions against scheme participants.

Health and Security Impact

SBIR/STTR fraud schemes can impact public health and national security by depriving participating agencies with responsibilities in these areas (e.g., U.S. Departments of Health and Human Services (HHS) and Defense (DOD)) of necessary research and development. They can also endanger national security when scheme participants obtain sensitive information and share that information with others for their own gain. For example, in one scheme, a fraudster shared sensitive information obtained through a DOD Missile Defense Agency SBIR contract with a subcontractor in Venezuela without authorization and failed to complete work under the contract within promised time frames.

Reputational Impact

Fraud against government programs can erode trust in government entities—confidence in their ability to manage taxpayer dollars, prevent fraud, and pursue justice—raising questions about the current integrity and future viability of the programs. For example, fraud in the SBIR/STTR programs can lead to public perception that program funds are easy to obtain fraudulently and make the programs targets for further and future exploitation. Relatedly, a DOJ official publicly stated that fraud in the SBIR/STTR award processes can

¹GAO, *GAO Fraud Ontology Version 1.0* (Washington, D.C.: Jan. 10, 2022), https://gaoinnovations.gov/antifraud_resource/howfraudworks; and International Public Sector Fraud Forum, *Guide to Understanding the Total Impact of Fraud* (February 2020).

undermine confidence that federal funding for research and innovation will continue. Further, SBIR/STTR fraud may affect the reputations of all awardees—including those that have not participated in fraud—potentially discouraging investors, research partners, and others from collaborating with awardees.

Impact on Victim

SBIR/STTR fraud schemes may victimize entities and individuals in various ways. Awardee businesses may suffer reputational and financial harm when their employees commit fraud, including legal and other costs associated with responding to law enforcement inquiries. STTR fraud schemes can similarly cause reputational and financial harm to partner research institutions—such as nonprofit colleges or universities—when, for example, fraudsters misrepresent the extent to which these entities performed work under the award and received award funds. In one scheme, fraudsters falsely represented that their business would perform at least 40 percent of the work under a U.S. Department of Energy (DOE) STTR award, in accordance with award conditions. In reality, work was primarily performed at a partner university. The fraudsters also submitted to DOE altered invoices, credit card statements, and canceled check images overstating the award funds they paid the partner university.


Finally, SBIR/STTR fraud schemes may victimize individuals through the unauthorized use of identity information and misrepresentation of labor costs. For example, in one scheme, fraudsters used the names and biographic information of legitimate researchers whom they did not employ to strengthen their proposals for SBIR/STTR awards from the U.S. National Science Foundation (NSF), DOE, and the U.S. Department of Agriculture. In another scheme, a fraudster allegedly paid foreign graduate students working on an Army SBIR project substantially less than the hourly labor rate quoted in contract proposals.

Appendix III: Comparison of GAO Fraud Risk Framework Leading Practices with the Policy Directive

In 2020, the U.S. Small Business Administration (SBA) updated its Policy Directive, which is SBA’s guidance to agencies administering the SBIR/STTR programs.¹ We identified the SBA’s fraud risk management requirements referenced in the SBIR/STTR Policy Directive, including the 10 minimum fraud, waste, and abuse requirements, and compared them with GAO’s *Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework). In addition to the 10 minimum requirements, we reviewed the remainder of the Policy Directive to assess whether any relevant guidance addressed Fraud Risk Framework requirements. In this appendix, we refer to the remainder of the Policy Directive as “other Policy Directive guidance.” See figures 17 through 20 below.

¹SBA issued revised guidance for the SBIR/STTR programs in August 2012 that included new requirements designed to help agencies identify and prevent potential fraud, waste, and abuse in the programs—changes that SBA developed in consultation with participating agencies and a working group of inspectors general. The Policy Directive has since been updated in February 2014, May 2019, October 2020 and, most recently, in May 2023. The May 2023 Policy Directive update did not change fraud, waste, and abuse requirements and does not apply to the awards within our review.

Figure 17: Comparison of Fraud Risk Framework Leading Practices for Creating a Culture and Structure to Manage Fraud Risks (Component 1) and Policy Directive Guidance

 Framework for Managing Fraud Risks in Federal Programs leading practices for creating a culture and structure to manage fraud risks (component 1)	Addressed by the U.S. Small Business Administration's Policy Directive 10 minimum fraud, waste, and abuse requirements	Addressed by other Policy Directive guidance
1.1.1 Demonstrate a senior-level commitment to integrity and combating fraud.	<input checked="" type="radio"/>	<input checked="" type="radio"/>
1.1.2 Involve all levels of the agency in setting an antifraud tone that permeates the organizational culture.	<input checked="" type="radio"/>	<input checked="" type="radio"/>
1.2.1 Designate an entity to design and oversee fraud risk management activities.	<input type="radio"/>	<input checked="" type="radio"/>
1.2.2 Designate an entity to design and oversee fraud risk management activities that <ul style="list-style-type: none"> • understands the program and its operations, as well as the fraud risks and controls throughout the program; • has defined responsibilities and the necessary authority across the program; • has a direct reporting line to senior-level managers within the agency; and • is located within the agency and not the Office of Inspector General, so the latter can retain its independence to serve its oversight role. In carrying out its role, the antifraud entity, among other things <ul style="list-style-type: none"> • serves as the repository of knowledge on fraud risks and controls; • manages the fraud risk-assessment process; • leads or assists with trainings and other fraud-awareness activities; and • coordinates antifraud initiatives across the program. 	<input type="radio"/>	<input checked="" type="radio"/>

Policy Directive addresses identified leading practices

Yes
 Partially
 No

Source: GAO analysis of U.S. Small Business Administration information. | GAO-24-105470


Appendix III: Comparison of GAO Fraud Risk Framework Leading Practices with the Policy Directive

Accessible Data for Figure 17: Comparison of Fraud Risk Framework Leading Practices for Creating a Culture and Structure to Manage Fraud Risks (Component 1) and Policy Directive Guidance

Framework for Managing Fraud Risks in Federal Programs leading practices for creating a culture and structure to manage fraud risks (component 1)	Addressed by the U.S. Small Business Administration’s Policy Directive 10 minimum fraud, waste, and abuse requirements	Addressed by other Policy Directive guidance
1.1.1 : Demonstrate a senior-level commitment to integrity and combating fraud.	Partially	Partially
1.1.2: Involve all levels of the agency in setting an antifraud tone that permeates the organizational culture.	Yes	Yes
1.2.1: Designate an entity to design and oversee fraud risk management activities.	No	Yes
1.2.2: Designate an entity to design and oversee fraud risk management activities that	No	Partially
<ul style="list-style-type: none"> • understands the program and its operations, as well as the fraud risks and controls throughout the program; • has defined responsibilities and the necessary authority across the program; and • has a direct reporting line to senior-level managers within the agency • is located within the agency and not the Office of Inspector General, so the latter can retain its independence to serve its oversight role. 		
In carrying out its role, the antifraud entity, among other things		
<ul style="list-style-type: none"> • serves as the repository of knowledge on fraud risks and controls; • manages the fraud risk-assessment process; • leads or assists with trainings and other fraud-awareness activities; and • coordinates antifraud initiatives across the program. 		

Source: GAO analysis of U.S. Small Business Administration information. | GAO-24-105470

Figure 18: Comparison of Fraud Risk Framework Leading Practices for Planning and Conducting Fraud Risk Assessments (Component 2) and Policy Directive Guidance

 Framework for Managing Fraud Risks in Federal Programs leading practices for planning and conducting fraud risk assessments (component 2)	Addressed by the U.S. Small Business Administration's Policy Directive 10 minimum fraud, waste, and abuse requirements	Addressed by other Policy Directive guidance
2.1.1 Tailor the fraud risk assessment to the program.	○	◐
2.1.2 Plan to conduct fraud risk assessments at regular intervals and when there are changes to the program or operating environment, as assessing fraud risks is an iterative process.	○	○
2.1.3 Identify specific tools, methods, and sources for gathering information about fraud risks, including data on fraud schemes and trends from monitoring and detection activities.	○	○
2.1.4 Involve relevant stakeholders in the assessment process, including individuals responsible for the design and implementation of fraud controls.	○	○
2.2.1 Identify inherent fraud risks affecting the program.	○	○
2.2.2 Assess the likelihood and impact of inherent fraud risks. <ul style="list-style-type: none"> • Involve qualified specialists, such as statisticians and subject-matter experts, to contribute expertise and guidance when employing techniques like analyzing statistically valid samples to estimate fraud losses and frequency. • Consider the nonfinancial impact of fraud risks, including impact on reputation and compliance with laws, regulations, and standards. 	○	○
2.2.3 Determine fraud risk tolerance.	○	○
2.2.4 Examine the suitability of existing fraud controls and prioritize residual fraud risks.	○	○
2.2.5 Document the program's fraud risk profile.	○	○

Policy Directive addresses identified leading practices

Yes
 Partially
 No

Source: GAO analysis of U.S. Small Business Administration information. | GAO-24-105470

Accessible Data for Figure 18: Comparison of Fraud Risk Framework Leading Practices for Planning and Conducting Fraud Risk Assessments (Component 2) and Policy Directive Guidance


Framework for Managing Fraud Risks in Federal Programs leading practices for planning and conducting fraud risk assessments (component 2)	Addressed by the U.S. Small Business Administration's Policy Directive 10 minimum fraud, waste, and abuse requirements	Addressed by other Policy Directive guidance
2.1.1: Plan to conduct fraud risk assessments at regular intervals and when there are changes to the program or operating environment, as assessing fraud risks is an iterative process.	No	Partially
2.1.2: Plan to conduct fraud risk assessments at regular intervals and when there are changes to the program or operating environment, as assessing fraud risks is an iterative process.	No	No

Appendix III: Comparison of GAO Fraud Risk Framework Leading Practices with the Policy Directive

Framework for Managing Fraud Risks in Federal Programs leading practices for planning and conducting fraud risk assessments (component 2)	Addressed by the U.S. Small Business Administration's Policy Directive 10 minimum fraud, waste, and abuse requirements	Addressed by other Policy Directive guidance
2.1.3: Identify specific tools, methods, and sources for gathering information about fraud risks, including data on fraud schemes and trends from monitoring and detection activities.	No	No
2.1.4: Involve relevant stakeholders in the assessment process, including individuals responsible for the design and implementation of fraud controls.	No	No
2.2.1: Identify inherent fraud risks affecting the program.	No	No
2.2.2: Assess the likelihood and impact of inherent fraud risks. Involve qualified specialists, such as statisticians and subject-matter experts, to contribute expertise and guidance when employing techniques like analyzing statistically valid samples to estimate fraud losses and frequency. Consider the nonfinancial impact of fraud risks, including impact on reputation and compliance with laws, regulations, and standards.	No	No

Source: GAO analysis of U.S. Small Business Administration information. | GAO-24-105470

Figure 19: Comparison of Fraud Risk Framework Leading Practices for Designing and Implementing an Antifraud Strategy with Control Activities (Component 3) and Policy Directive Guidance

 Framework for Managing Fraud Risks in Federal Programs leading practices for designing and implementing an antifraud strategy with control activities (component 3)	Addressed by the U.S. Small Business Administration's Policy Directive 10 minimum fraud, waste, and abuse requirements	Addressed by other Policy Directive guidance
3.1.1 Use the fraud risk profile to help decide how to allocate resources to respond to residual fraud risks.	<input type="radio"/>	<input type="radio"/>
3.1.2 Develop, document, and communicate an antifraud strategy to employees and stakeholders that describes the program's activities for preventing, detecting, and responding to fraud, as well as monitoring and evaluation.	<input type="radio"/>	<input checked="" type="radio"/>
3.1.3 Establish roles and responsibilities of those involved in fraud risk management activities, such as the antifraud entity and external parties responsible for fraud controls, and communicate the role of the Office of Inspector General (OIG) to investigate potential fraud.	<input checked="" type="radio"/>	<input checked="" type="radio"/>
3.1.4 Create timelines for implementing fraud risk management activities, as appropriate, including monitoring and evaluations.	<input type="radio"/>	<input type="radio"/>
3.1.5 Demonstrate links to the highest internal and external residual fraud risks outlined in the fraud risk profile.	<input type="radio"/>	<input type="radio"/>
3.1.6 Link antifraud efforts to other risk management activities, if any.	<input checked="" type="radio"/>	<input checked="" type="radio"/>
3.2.1 Focus on fraud prevention over detection and response to avoid a "pay-and-chase" model, to the extent possible.	<input checked="" type="radio"/>	<input checked="" type="radio"/>
3.2.2 Consider the benefits and costs of control activities to address identified residual risks.	<input type="radio"/>	<input checked="" type="radio"/>
3.2.3 Design and implement the following control activities to prevent and detect fraud: data-analytics activities, fraud-awareness initiatives, reporting mechanisms, and employee-integrity initiatives.	<input checked="" type="radio"/>	<input type="radio"/>
3.3.1 Develop a plan outlining how the program will respond to identified instances of fraud and ensure the response is prompt and consistently applied.	<input type="radio"/>	<input checked="" type="radio"/>
3.3.2 Refer instances of potential fraud to the OIG or other appropriate parties, such as law-enforcement entities or the Department of Justice, for further investigation.	<input checked="" type="radio"/>	<input type="radio"/>
3.4.1 Establish collaborative relationships with internal and external stakeholders, including other offices within the agency; federal, state, and local agencies; private-sector partners; law-enforcement entities; and entities responsible for control activities to, among other things, share information on fraud risks and emerging fraud schemes, and share lessons learned related to fraud control activities.	<input checked="" type="radio"/>	<input checked="" type="radio"/>
3.4.2 Collaborate and communicate with the OIG to improve understanding of fraud risks and align efforts to address fraud.	<input checked="" type="radio"/>	<input checked="" type="radio"/>
3.4.3 Create incentives for employees to manage risks and report fraud, including creating performance metrics that assess fraud risk management efforts and employee integrity, particularly for managers; and balancing fraud-specific performance metrics with other metrics related to employees' duties.	<input type="radio"/>	<input checked="" type="radio"/>
3.4.4 Provide guidance and other support and create incentives to help external parties, including contractors, effectively carry out fraud risk management activities.	<input checked="" type="radio"/>	<input type="radio"/>

Policy Directive addresses identified leading practices

Yes Partially No

Source: GAO analysis of U.S. Small Business Administration information. | GAO-24-105470


Appendix III: Comparison of GAO Fraud Risk Framework Leading Practices with the Policy Directive

Accessible Data for Figure 19: Comparison of Fraud Risk Framework Leading Practices for Designing and Implementing an Antifraud Strategy with Control Activities (Component 3) and Policy Directive Guidance

<i>Framework for Managing Fraud Risks in Federal Programs</i> leading practices for designing and implementing an antifraud strategy with control activities (component 3)	Addressed by the U.S. Small Business Administration's Policy Directive 10 minimum fraud, waste, and abuse requirements	Addressed by other Policy Directive guidance
3.1.1: Use the fraud risk profile to help decide how to allocate resources to respond to residual fraud risks.	No	No
3.1.2: Develop, document, and communicate an antifraud strategy to employees and stakeholders that describes the program's activities for preventing, detecting, and responding to fraud, as well as monitoring and evaluation.	No	Yes
3.1.3: Establish roles and responsibilities of those involved in fraud risk management activities, such as the antifraud entity and external parties responsible for fraud controls, and communicate the role of the Office of Inspector General (OIG) to investigate potential fraud.	Yes	Yes
3.1.4: Create timelines for implementing fraud risk management activities, as appropriate, including monitoring and evaluations.	No	No
3.1.5: Demonstrate links to the highest internal and external residual fraud risks outlined in the fraud risk profile.	No	No
3.1.6: Link antifraud efforts to other risk management activities, if any.	Yes	Yes
3.2.1: Focus on fraud prevention over detection and response to avoid a "pay-and-chase" model, to the extent possible.	Yes	Yes
3.2.2: Consider the benefits and costs of control activities to address identified residual risks.	No	Yes
3.2.3: Design and implement the following control activities to prevent and detect fraud: data-analytics activities, fraud-awareness initiatives, reporting mechanisms, and employee-integrity initiatives.	Yes	No
3.3.1: Develop a plan outlining how the program will respond to identified instances of fraud and ensure the response is prompt and consistently applied.	No	Yes
3.3.2: Refer instances of potential fraud to the OIG or other appropriate parties, such as law-enforcement entities or the Department of Justice, for further investigation.	Yes	No
3.4.1: Establish collaborative relationships with internal and external stakeholders, including other offices within the agency; federal, state, and local agencies; private-sector partners; law-enforcement entities; and entities responsible for control activities to, among other things: share information on fraud risks and emerging fraud schemes, and share lessons learned related to fraud control activities.	Yes	Yes
3.4.2: Collaborate and communicate with the OIG to improve understanding of fraud risks and align efforts to address fraud.	Yes	Yes
3.4.3: Create incentives for employees to manage risks and report fraud, including creating performance metrics that assess fraud risk management efforts and employee integrity, particularly for managers; and balancing fraud-specific performance metrics with other metrics related to employees' duties.	No	Yes
3.4.4: Provide guidance and other support and create incentives to help external parties, including contractors, effectively carry out fraud risk management activities.	Yes	No

Source: GAO analysis of U.S. Small Business Administration information. | GAO-24-105470

Figure 20: Comparison of Fraud Risk Framework Leading Practices for Monitoring, Evaluating, and Adapting Fraud Risk Management Activities (Component 4) and Policy Directive Guidance

 Framework for Managing Fraud Risks in Federal Programs leading practices for monitoring, evaluating, and adapting fraud risk management activities (component 4)	Addressed by the U.S. Small Business Administration's Policy Directive 10 minimum fraud, waste, and abuse requirements	Addressed by other Policy Directive guidance
4.1.1 Monitor and evaluate the effectiveness of preventive activities, including fraud risk assessments and the antifraud strategy, as well as controls to detect fraud and response efforts.	○	●
4.1.2 Collect and analyze data, including data from reporting mechanisms and instances of detected fraud, for real-time monitoring of fraud trends and identification of potential control deficiencies.	●	○
4.1.3 Employ a risk-based approach to monitoring by taking into account internal and external factors that can influence the control environment, such as organizational changes and emerging risks.	●	○
4.1.4 Engage stakeholders responsible for specific fraud risk management activities in the monitoring and evaluation process.	○	○
4.2.1 Measure outcomes, in addition to outputs, of fraud risk management activities.	○	○
4.2.2 In the absence of sufficient data, assess how well managers follow recommended "leading practices" for designing fraud risk management activities.	○	○
4.3.1 Use the results of monitoring and evaluations to improve the design and implementation of fraud risk management activities.	○	○
4.3.2 Use analysis of identified instances of fraud and fraud trends to improve fraud risk management activities, including prioritizing and taking corrective actions, as well as enhancing fraud-awareness trainings.	○	○
4.3.3 Use results of investigations and prosecutions to enhance fraud prevention and detection.	●	○
4.3.4 Communicate results of monitoring and evaluations, including corrective actions taken, if any, to relevant stakeholders.	○	○

Policy Directive addresses identified leading practices

Yes
 Partially
 No

Source: GAO analysis of U.S. Small Business Administration information. | GAO-24-105470

Accessible Data for Figure 20: Comparison of Fraud Risk Framework Leading Practices for Monitoring, Evaluating, and Adapting Fraud Risk Management Activities (Component 4) and Policy Directive Guidance

Framework for Managing Fraud Risks in Federal Programs leading practices for monitoring, evaluating, and adapting fraud risk management activities (component 4)	Addressed by the U.S. Small Business Administration's Policy Directive 10 minimum fraud, waste, and abuse requirements	Addressed by other Policy Directive guidance
4.1.1: Monitor and evaluate the effectiveness of preventive activities, including fraud risk assessments and the antifraud strategy, as well as controls to detect fraud and response efforts.	No	Yes

Appendix III: Comparison of GAO Fraud Risk Framework Leading Practices with the Policy Directive

Framework for Managing Fraud Risks in Federal Programs leading practices for monitoring, evaluating, and adapting fraud risk management activities (component 4)	Addressed by the U.S. Small Business Administration's Policy Directive 10 minimum fraud, waste, and abuse requirements	Addressed by other Policy Directive guidance
4.1.2: Collect and analyze data, including data from reporting mechanisms and instances of detected fraud, for real-time monitoring of fraud trends and identification of potential control deficiencies.	Yes	No
4.1.3: Employ a risk-based approach to monitoring by taking into account internal and external factors that can influence the control environment, such as organizational changes and emerging risks.	Yes	No
4.1.4: Engage stakeholders responsible for specific fraud risk management activities in the monitoring and evaluation process.	No	No
4.2.1: Measure outcomes, in addition to outputs, of fraud risk management activities.	No	No
4.2.2: In the absence of sufficient data, assess how well managers follow recommended "leading practices" for designing fraud risk management activities.	No	No
4.3.1: Use the results of monitoring and evaluations to improve the design and implementation of fraud risk management activities.	No	No
4.3.2: Use analysis of identified instances of fraud and fraud trends to improve fraud risk management activities, including prioritizing and taking corrective actions, as well as enhancing fraud-awareness trainings.	No	No
4.3.3: Use results of investigations and prosecutions to enhance fraud prevention and detection.	Yes	No
4.3.4: Communicate results of monitoring and evaluations, including corrective actions taken, if any, to relevant stakeholders.	No	No

Source: GAO analysis of U.S. Small Business Administration information. | GAO-24-105470

Appendix IV: Fraud, Waste, or Abuse Risk Categories, Descriptions, and Examples

We used participating agency Office of Inspector General (OIG) Small Business Innovation and Research (SBIR) and Small Business Technology Transfer (STTR) fraud detection indicators, the U.S. Small Business Administration’s (SBA) Policy Directive, and discussions with internal stakeholders to develop 21 fraud, waste, or abuse risk categories and subcategories. We used these categories to inform our evaluation of participating agencies’ fraud risk assessments and our data testing, as described in appendix I. See table 13 for the fraud, waste, and abuse categories, descriptions, and examples.

The fraud, waste, or abuse risk categories we identified may not include all potential fraud, waste, or abuse risk categories that may impact the program; however, the categories represent those that were identified in our review. An identified fraud, waste, or abuse risk category does not necessarily mean there has been a judicially determined finding of fraud in all instances. Rather, we identify risks generally, since they can ultimately lead to cases of fraud.¹

In addition to fraud, other forms of misconduct can occur, such as waste and abuse.² Waste and abuse do not necessarily involve fraud or illegal acts; however, they may be an indication of potential fraud.³ For example, misuse of applicants’ personal or financial information, such as selling applicant information to contractors, may indicate abuse, potential fraud, or other illegal activity. See appendix I for the data testing we conducted.

Table 13: Fraud, Waste, or Abuse Risk Categories, Descriptions, and Examples

Categories	Description	Examples
Agency oversight	Agency does not properly assess the progress and feasibility of an applicant throughout the award life cycle.	The agency technical point of contact lacks the ability to properly assess progress. The agency technical expert lacks oversight to properly assess research progress and reports.

¹Fraud and fraud risk are distinct concepts. Fraud—obtaining something of value through willful misrepresentation—is challenging to detect because of its deceptive nature. Fraud risk (which is a function of likelihood and impact) exists when people 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. Whether an act is, in fact, fraud is a determination to be made through the judicial or other adjudicative system.

²Waste is the act of using or expending resources carelessly, extravagantly, or to no purpose. Abuse involves behavior that is deficient or improper, when compared with behavior that a prudent person would consider reasonable and necessary operational practice, given the facts and circumstances. This includes the misuse of authority or position for personal gain or for the benefit of another. GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

³[GAO-14-704G](#).

Appendix IV: Fraud, Waste, or Abuse Risk Categories, Descriptions, and Examples

Categories	Description	Examples
Affiliated business	An affiliated business relationship is not reported by the applicant or identified by the agency during the award life cycle.	An applicant does not report an affiliated business relationship in proposal documentation or designated government database, which may make the applicant ineligible for awards. An applicant reports affiliated business relationships, and an agency does not consider the effect on award eligibility, such as the small business 500 employee count threshold.
Applicant employees: Nepotism	Applicant has an unreasonable preference for individuals or institutions.	An applicant has family members on the payroll. An applicant demands to include certain individuals or institutions in their award process.
Applicant employees: Workplace environment	Applicant's workplace is not conducive to being able to complete the research.	An applicant shows evidence of allowing employee misconduct. An applicant has high employee turnover.
Bid-rigging	Applicant(s) conspires with another business to influence the purchase of goods or services to avoid competitive bidding controls.	The applicant submits unusual bid patterns for research. The applicant requests losing bidders to be subcontractors.
Bribery and kickbacks: Bribery	Applicant or agency offers, gives, receives, or solicits something of value as payment to influence an official act.	An agency contracting employee insists on a particular applicant to receive an award. The applicant contract changes without justification.
Bribery and kickbacks: Kickbacks	Applicant and agency officials coordinate to direct awards to the applicant in exchange for something of value related to the award.	An agency contracting employee insists on a particular applicant to receive an award. An applicant has a prior reputation related to gifts or kickbacks.
Business ownership	Applicant does not disclose a condition related to business ownership, or the agency does not identify a condition related to ownership during the award life cycle.	An applicant does not disclose that a business or person with ownership is on an excluded parties list or was not identified by the agency as being on an excluded parties list. An applicant does not meet ownership requirements or was not identified by the agency as not meeting ownership requirements.
Conflict of interest	Applicant has undisclosed financial or personal relationship related to a Small Business Innovation Research (SBIR) or Small Business Technology Transfer (STTR) award. Or the agency does not identify a financial or personal relationship related to the SBIR or STTR programs.	Government personnel are involved within the proposal. An applicant does not report personal or business relationships with agency officials.

Appendix IV: Fraud, Waste, or Abuse Risk Categories, Descriptions, and Examples

Categories	Description	Examples
Essentially equivalent work	SBIR or STTR work that is per the U.S. Small Business Administration's (SBA) Policy Directive, "substantially the same research" either submitted by an applicant or unidentified by an agency during the application and award process.	An applicant knowingly accepts a new SBIR/STTR award for research that is "substantially the same" as prior or ongoing research. An agency does not identify if substantially similar research has been funded previously by itself or another agency, regardless of the applicant.
Excluded parties	Applicant does not disclose ineligibility due to suspension or debarments. Or the agency did not identify or enforce suspensions or debarments throughout the award life cycle.	The applicant has prior court cases.
Financial responsibility	Applicant does not have adequate financial resources to perform research or the ability to obtain them. Or the agency does not properly evaluate financial risks posed by applicant.	The applicant lacks financial stability. An applicant displays poor quality management systems.
Foreign ownership	Applicant does not disclose foreign ownership, or the agency does not identify and consider foreign ownership, during the award life cycle.	An applicant does not report business or person with foreign ownership in proposal documentation or designated government database, which may make it ineligible for awards. An applicant discloses foreign relationships, but the agency does not consider effect on award eligibility.
Inappropriate billing	Awardee obtains payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases. Or the agency does not identify issues related to billing.	The awardee provides invoices in round dollars. The awardee misrepresents the use of expended funds.
Misrepresentation during the award life cycle: Eligibility	Applicant knowingly does not disclose information related to eligibility. Or the agency does not verify or enforce the requirement that an applicant meet all eligibility requirements during the award life cycle.	The applicant maintains eligibility requirements just below specific thresholds. The agency does not identify that an applicant employee size is over the program limit during the award life cycle.
Misrepresentation during the award life cycle: Proposal	Applicant knowingly provides false or misleading information in proposal documentation. Or the agency does not identify false or misleading information during the award life cycle.	An applicant provides false letters of support during the award life cycle. An applicant plagiarizes research during the award life cycle.
Misrepresentation during the award life cycle: Program information	Applicant knowingly excludes required information during the award life cycle. Or the agency does not enforce the requirement for necessary documentation.	The applicant provides incomplete financial disclosure statements. The applicant requests extensions to produce certifications.
Misrepresentation during the award life cycle: Reporting	Applicant knowingly provides false or misleading information in reporting. Or the agency does not identify false or misleading information during the award life cycle.	An applicant has no failures in reported test records.

Appendix IV: Fraud, Waste, or Abuse Risk Categories, Descriptions, and Examples

Categories	Description	Examples
Number or type of awards	Applicant receives a higher number of awards or has awards that exceed normal program limits without a required waiver, as appropriate.	An applicant does not meet performance benchmark requirements and continues to receive awards from an agency. An applicant has many awards that are longer than the normal award performance period.
Poor performance	Applicant has a history of not meeting research expectations. Or the agency does not identify and consider prior performance.	The applicant misrepresents research performed. The applicant has a discrepancy between the proposed research versus the actual research performed.
Principal investigator	Principal investigator does not meet employment requirements, or the agency does not identify and consider principal investigator eligibility during the award life cycle.	An applicant does not disclose that the primary employment of the principal investigator is to another business. The agency does not consider that the principal investigator is listed on multiple awards.
Program compliance	Applicant does not meet requirements of the SBIR or STTR programs. Or the agency does not enforce program requirements on applicants during the award life cycle.	The applicant misrepresents their compliance in the SBIR/STTR programs. The agency has lax enforcement of award requirements to applicants.
Product substitution	Awardee provides the agency with product that does not meet funding agreements. Or the agency does not verify that the product meets funding agreement requirements.	The applicant provides “new” products that appear “used.” The applicant provides materials in unusual or generic packaging.
Research facilities	Applicant falsely reports the facility location where the research is performed or the facilities are not adequate for the research. Or the agency does not verify that applicant facilities are adequate to meet award needs throughout the award life cycle.	An applicant’s facilities are not adequate for the proposed research. An applicant lists a location to conduct research that is not feasible, such as a post office box.
Shell company	Applicant shows a lack of physical presence and generates little-to-no independent economic value to help conceal the business’s true ownership. Or the agency does not verify the applicant’s credentials throughout the award life cycle.	The applicant has limited-to-no presence on the internet. The agency does not recognize that the applicant has no real U.S. presence.
Subcontract	Awardee misrepresents a relationship with subcontractors or the agency does not identify subcontracting concerns as appropriate, during the award life cycle.	The applicant moves employees from the prime business to the subcontractor. The agency does not identify an invalid subcontractor.

Sources: GAO analysis of Office of Inspector General fraud detection indicators; and the U.S. Small Business Administration’s Policy Directive; Icons-Studio/stock.adobe.com (icons). | GAO-24-105470

Appendix V: Comments from the U.S. Small Business Administration



August 13, 2024

Rebecca Shea
Director
Forensic Audits and Investigative Service
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Rebecca Shea:

Thank you for providing the U. S. Small Business Administration (SBA) with a copy of the Government Accountability Office (GAO) draft report titled “Opportunities Exist for SBA and Agencies to Reduce Vulnerability to Fraud, Waste, and Abuse”, GAO-24-105470.

The GAO report covers an award period between 2016 and 2022, and as the report noted in multiple sections and through several footnotes, during more recent years the SBA has: (1) improved the data quality within SBIR.gov; (2) instituted processes for participating agencies’ implementation of the SBIR/STTR Policy Directive minimum fraud, waste, and abuse requirements; (3) established a repetitive, and consistent process to list fraud-related convictions and findings of civil liability on SBIR.gov; and (4) initiated discussions around newly resolved fraud cases and frequent fraud schemes during the SBA-led monthly SBIR/STTR program manager’s meetings.

Nonetheless, as the draft report demonstrates, opportunities exist to do more, and SBA is committed to taking appropriate actions within the confines of our legal authority and resources to further strengthen protections against fraud and reduce potential vulnerabilities.

Recommendation 1: The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation expands the methods and sources used to identify fraud-related convictions and findings of civil liability to list in the SBA’s database, such as through alerts from legal research resources.

SBA Response: Concur.

Recommendation 2: The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation leverages its oversight mechanisms to identify, share, and report fraud-related convictions and findings of civil liability to SBIR.gov and address participating agencies’ challenges in understanding and meeting the 15-day reporting requirement.

SBA Response: Concur.

Recommendation 3: The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation leverages its existing oversight mechanisms to ensure the accuracy of agencies survey responses to required fraud, waste, and abuse training and, to the full extent of the SBA's legal authority, shares SBIR/STTR fraud risk information and resources for conducting fraud risk assessments.

SBA Response: Concur.

Recommendation 4: The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation, to the full extent of the SBA's legal authority, provides guidance to participating agencies to conduct comprehensive SBIR/STTR program fraud risk assessments, including all key elements, in support of the Policy Directive's fraud, waste, and abuse prevention requirements and consistent with *Fraud Risk Framework* leading practices.

SBA Response: Concur.

Recommendation 5: The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation improves SBIR.gov data quality by updating guidance to require that abstracts are sufficiently complete, and that applicant and awardee addresses are verified to support program eligibility determinations.

SBA Response: Concur.

Recommendation 6: The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation validates existing information in the SBIR/STTR databases, specifically the Company Registry and SBIR.gov, to identify and correct deficiencies, as appropriate.

SBA Response: Concur.

Thank you for the opportunity to comment on this draft report.

Sincerely,

**ERICK PAGE-
LITTLEFORD**

Digitally signed by ERICK
PAGE-LITTLEFORD
Date: 2024.08.12 16:04:07
-04'00'

Erick Page-Littleford
Director, Small Business Innovation Research and Technology Transfer (SBIRTT)
Office of Investment & Innovation
U.S. Small Business Administration

Accessible Text for Appendix V: Comments from the U.S. Small Business Administration

August 13, 2024

Rebecca Shea
Director
Forensic Audits and Investigative Service
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Rebecca Shea:

Thank you for providing the U. S. Small Business Administration (SBA) with a copy of the Government Accountability Office (GAO) draft report titled “Opportunities Exist for SBA and Agencies to Reduce Vulnerability to Fraud, Waste, and Abuse”, GAO-24-105470.

The GAO report covers an award period between 2016 and 2022, and as the report noted in multiple sections and through several footnotes, during more recent years the SBA has: (1) improved the data quality within SBIR.gov; (2) instituted processes for participating agencies’ implementation of the SBIR/STTR Policy Directive minimum fraud, waste, and abuse requirements; (3) established a repetitive, and consistent process to list fraud-related convictions and findings of civil liability on SBIR.gov; and (4) initiated discussions around newly resolved fraud cases and frequent fraud schemes during the SBA-led monthly SBIR/STTR program manager’s meetings.

Nonetheless, as the draft report demonstrates, opportunities exist to do more, and SBA is committed to taking appropriate actions within the confines of our legal authority and resources to further strengthen protections against fraud and reduce potential vulnerabilities.

Recommendation 1: The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation expands the methods and sources used to identify fraud-related convictions and findings of civil liability to list in the SBA’s database, such as through alerts from legal research resources.

SBA Response: Concur.

Recommendation 2: The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation leverages its oversight mechanisms to identify, share, and report fraud-related convictions and findings of civil liability to SBIR.gov and address participating agencies’ challenges in understanding and meeting the 15- day reporting requirement.

SBA Response: Concur.

Recommendation 3: The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation leverages its existing oversight mechanisms to ensure the accuracy of agencies survey responses to required fraud, waste, and abuse training and, to the full extent of the SBA's legal authority, shares SBIR/STTR fraud risk information and resources for conducting fraud risk assessments.

SBA Response: Concur.

Recommendation 4: The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation, to the full extent of the SBA's legal authority, provides guidance to participating agencies to conduct comprehensive SBIR/STTR program fraud risk assessments, including all key elements, in support of the Policy Directive's fraud, waste, and abuse prevention requirements and consistent with Fraud Risk Framework leading practices.

SBA Response: Concur.

Recommendation 5: The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation improves SBIR.gov data quality by updating guidance to require that abstracts are sufficiently complete, and that applicant and awardee addresses are verified to support program eligibility determinations.

SBA Response: Concur.

Recommendation 6: The Administrator of SBA should ensure that the Associate Administrator for the Office of Investment and Innovation validates existing information in the SBIR/STTR databases, specifically the Company Registry and SBIR.gov, to identify and correct deficiencies, as appropriate.

SBA Response: Concur.

Thank you for the opportunity to comment on this draft report.

Sincerely,

ERICK PAGE-LITTLEFORD

Digitally signed by ERICK PAGE-LITTLEFORD

Date: 2024.08.12 16:04:07-04'00'

Erick Page-Littleford
Director, Small Business Innovation Research and Technology Transfer (SBIRTT)
Office of Investment & Innovation
U.S. Small Business Administration

Appendix VI: Comments from the U.S. Department of Agriculture



August 7, 2024

Rebecca Shea
Director, Forensic Audits and Investigative Service
U.S. Government Accountability Office
441 G St., NW
Washington, DC 20548

Dear Ms. Shea:

The U.S. Department of Agriculture (USDA) appreciates the opportunity to review and comment on the U.S. Government Accountability Office's (GAO) official draft report titled, *Small Business Research Programs: Opportunities Exist for SBA and Agencies to Reduce Vulnerabilities to Fraud, Waste, and Abuse* (GAO-24-105470). GAO made 8 recommendations in the draft report, including one recommendation to USDA.

Recommendation 3 stated: "The Secretary of the U.S. Department of Agriculture should ensure that the Director of the National Institute of Food and Agriculture ensures that USDA SBIR/STTR applicants receive fraud, waste, and abuse training."

USDA generally concurs with this recommendation. In response to the recommendation, the National Institute of Food and Agriculture is planning to incorporate fraud, waste, and abuse training into the technical webinars provided to SBIR/STTR applicants.

USDA would also like to offer two technical comments on the official draft report for your consideration. The technical comments are being provided separately from this letter via the attachment.

Sincerely,

DIONNE TOOMBS
Digitally signed by DIONNE TOOMBS
Date: 2024.08.02 11:48:35 -04'00'

Dr. Manjit K. Misra
Director
National Institute of Food and Agriculture
U.S. Department of Agriculture

Attachment: USDA Technical Comments for GAO Draft Report 105470 SBIR Fraud Risk

1400 Independence Avenue, SW, MS 2201 | Washington, DC | 20250-2201

USDA IS AN EQUAL OPPORTUNITY PROVIDER, EMPLOYER, AND LENDER

Accessible Text for Appendix VI: Comments from the U.S. Department of Agriculture

August 7, 2024

Rebecca Shea
Director, Forensic Audits and Investigative Service
U.S. Government Accountability Office
441 G St., NW
Washington, DC 20548

Dear Ms. Shea:

The U.S. Department of Agriculture (USDA) appreciates the opportunity to review and comment on the U.S. Government Accountability Office's (GAO) official draft report titled, *Small Business Research Programs: Opportunities Exist for SBA and Agencies to Reduce Vulnerabilities to Fraud, Waste, and Abuse* (GAO-24-105470). GAO made 8 recommendations in the draft report, including one recommendation to USDA.

Recommendation 3 stated: "The Secretary of the U.S. Department of Agriculture should ensure that the Director of the National Institute of Food and Agriculture ensures that USDA SBIR/STTR applicants receive fraud, waste, and abuse training."

USDA generally concurs with this recommendation. In response to the recommendation, the National Institute of Food and Agriculture is planning to incorporate fraud, waste, and abuse training into the technical webinars provided to SBIR/STTR applicants.

USDA would also like to offer two technical comments on the official draft report for your consideration. The technical comments are being provided separately from this letter via the attachment.

Sincerely,

Dr. Manjit K. Misra
Director
National Institute of Food and Agriculture
U.S. Department of Agriculture

Attachment: USDA Technical Comments for GAO Draft Report 105470 SBIR Fraud Risk

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

Rebecca Shea at (202) 512-6722 or SheaR@gao.gov

Staff Acknowledgments

In addition to the contact named above, Tonita Gillich (Assistant Director), Mariana Calderón (Assistant Director), Georgette Hagans (Analyst in Charge), Jennifer Felder, Daniel Adorno, Garrick Donnelly, and Nicole Mackowski made key contributions to this report. In addition, Dean Campbell, Dustin Cohan, Brendan Culley, Celina Davidson, Sara Daleski, George Depaoli, Leia Dickerson, Colin Fallon, Barbara Lewis, Rona Mendelsohn, Maria McMullen, Katherine Moody Wong, James Murphy, Amanda Parker, and Steven Putansu contributed to the report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

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

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Sarah Kaczmarek, Acting Managing Director, KaczmarekS@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

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