



April 2023

# FRAUD RISK MANAGEMENT

## Key Areas for Federal Agency and Congressional Action

Accessible Version

# GAO Highlights

Highlights of [GAO-23-106567](#), a report to congressional committees

## Why GAO Did This Study

Fraud poses a significant risk to the integrity of federal programs and erodes public trust in government. The increased flow of federal funds associated with the COVID-19 pandemic has increased opportunities for fraud. While the extent of fraud associated with COVID-19 relief programs has not yet been fully determined, available information indicates substantial levels of fraud and potential fraud occurred. For example, in December 2022, GAO reported that estimated fraud in DOL's Unemployment Insurance programs during the pandemic totaled over \$60 billion.

To help federal program managers strategically manage their fraud risks during both normal operations and emergencies, GAO published the Fraud Risk Framework in July 2015. It provides a comprehensive set of leading practices that serve as a guide for agency managers to use when developing efforts to combat fraud. Since 2015, GAO has issued over 70 reports with numerous recommendations to help federal agencies manage their fraud risks.

This report highlights areas where GAO's prior work has shown that federal agencies and Congress can take action to help ensure effective fraud risk management.

## What GAO Recommends

From July 2015 through December 2022, GAO made 142 recommendations to over 40 agency or program offices related to one or more of the five key areas. As of January 2023, 74 of the recommendations had not been fully implemented.

View [GAO-23-106567](#). For more information, contact Seto J. Bagdoyan at (202) 512-6722 or [BagdoyanS@gao.gov](mailto:BagdoyanS@gao.gov).

April 2023

## FRAUD RISK MANAGEMENT

### Key Areas for Federal Agency and Congressional Action

## What GAO Found

GAO's prior work has highlighted five areas in which federal agencies need to take additional actions to help ensure they are effectively managing fraud risks, consistent with leading practices in GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework).

### Federal Agencies Need to Improve Fraud Risk Management Efforts in Five Areas



Source: GAO (information and icons). | GAO-23-106567

GAO has recently made several recommendations to, for example, the Department of Labor (DOL) to improve fraud risk management in the Unemployment Insurance programs, including recommendations to assess fraud risks and to design and implement an antifraud strategy. DOL has begun taking steps to implement these recommendations, but its work remains incomplete. Completing these efforts would help DOL manage Unemployment Insurance fraud risks more effectively.

GAO's prior work has also identified actions that Congress can take to strengthen fraud risk management practices across the government.

- Reinstating the requirement for agencies to report on their antifraud controls and fraud risk management efforts in agency financial reports.** In March 2022, GAO recommended that Congress amend the Payment Integrity Information Act of 2019 to reinstate certain reporting requirements. Requiring agencies to report annually on their antifraud controls and fraud risk management efforts will help facilitate congressional oversight and focus agency attention on strategic fraud risk management—both during normal operations and in emergencies—and help align their efforts with leading practices.
- Establishing a permanent analytics center of excellence to aid the oversight community in identifying improper payments and fraud.** Inspectors General did not have access to a government-wide analytical capability to help identify fraud until more than a year after agencies began distributing relief funds. Without permanent government-wide analytics capabilities to assist the oversight community, agencies will have limited resources to apply to nonpandemic programs to ensure robust financial stewardship, as well as to better prepare for applying fundamental financial and fraud risk management practices to future emergency funding.

---

# Contents

---

GAO Highlights		ii
	<b>Why GAO Did This Study</b>	ii
	<b>What GAO Recommends</b>	ii
	<b>What GAO Found</b>	ii
Letter		1
	Background	4
	Key Areas for Improving Fraud Risk Management	12
Appendix I: Matters for Congressional Consideration		31
Appendix II: GAO Contact and Staff Acknowledgments		33
	GAO Contact	33
	Staff Acknowledgments	33
Figures		
	Federal Agencies Need to Improve Fraud Risk Management Efforts in Five Areas	ii
	Figure 1: The Fraud Risk Framework and Selected Leading Practices	5
	Text of Figure 1: The Fraud Risk Framework and Selected Leading Practices	5
	Figure 2: Legislation and Guidance Related to Fraud Risk Management	8
	Text of Figure 2: Legislation and Guidance Related to Fraud Risk Management	9
	Figure 3: Case Study Illustrating Aircraft-Related Criminal Activity Risks	21
	Text of Figure 3: Case Study Illustrating Aircraft-Related Criminal Activity Risks	21
	Figure 4: Examples of Fraud Risks and Possible Schemes Targeting Government and Private Businesses and Individuals during Emergencies	24
	Text of Figure 4: Examples of Fraud Risks and Possible Schemes Targeting Government and Private Businesses and Individuals during Emergencies	25

---

---

## Abbreviations

CFO	chief financial officer
CMS	Centers for Medicare & Medicaid Services
DOE	Department of Energy
DOL	Department of Labor
EXIM	Export-Import Bank of the United States
FAA	Federal Aviation Administration
Fraud Risk Framework	<i>A Framework for Managing Fraud Risks in Federal Programs</i>
FRDAA	Fraud Reduction and Data Analytics Act of 2015
Green Book	<i>Standards for Internal Control in the Federal Government</i>
OHS	Office of Head Start
OMB	Office of Management and Budget
PACE	Pandemic Analytics Center of Excellence
PIIA	Payment Integrity Information Act of 2019
PPP	Paycheck Protection Program
PRAC	Pandemic Response Accountability Committee
SBA	Small Business Administration
SSA	Social Security Administration
UI	Unemployment Insurance
USCIS	U.S. Citizenship and Immigration Services

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.



April 13, 2023

The Honorable Gary C. Peters  
Chairman  
The Honorable Rand Paul, M.D.  
Ranking Member  
Committee on Homeland Security and Governmental Affairs  
United States Senate

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

Fraud poses a significant risk to the integrity of federal programs and erodes public trust in government.<sup>1</sup> It contributes to financial and nonfinancial risks that waste taxpayer dollars, threaten national security, or put consumers at risk. Additionally, fraud—which involves obtaining something of value through willful misrepresentation—continues to add to the improper payments made by the government.<sup>2</sup>

The public health crisis, economic instability, and increased flow of federal funds associated with the COVID-19 pandemic have expanded opportunities for fraud. The extent of fraud associated with COVID-19 relief programs has not yet been fully determined. However, available measures and estimates indicate substantial levels of fraud and potential fraud occurred. For example, in December 2022, we reported that

---

<sup>1</sup>Whether an act is fraudulent is determined through the judicial or other adjudicative system and is beyond management’s professional responsibility for assessing risk. GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

<sup>2</sup>An improper payment is defined as any payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements. It includes any payment to an ineligible recipient, any payment for an ineligible good or service, any duplicate payment, any payment for a good or service not received (except for such payments where authorized by law), and any payment that does not account for credit for applicable discounts. While not all improper payments are the result of fraud, all payments made as a result of fraudulent activities are considered to be improper payments.

extrapolating the lower bound of the Department of Labor’s (DOL) estimated national fraud rate for the regular Unemployment Insurance (UI) program for performance year 2021—which covers July 1, 2020 through June 30, 2021—to total spending across all UI programs during the pandemic would suggest over \$60 billion in fraudulent UI payments.<sup>3</sup> Further, based on findings from our prior work and other audits, we added three programs that account for a large portion of COVID-19 funding to our High-Risk List in March 2021 and June 2022, namely

- the Small Business Administration’s (SBA) emergency loans for small businesses issued under the Paycheck Protection Program (PPP),
- SBA’s COVID-19 Economic Injury Disaster Loan program, and
- DOL’s UI program.

Managers of federal programs may perceive a conflict between their priorities to fulfill the program’s mission, such as quickly and efficiently disbursing funds or providing services to beneficiaries, and taking actions to safeguard taxpayer dollars from improper use. However, proactively managing fraud risks can help facilitate the program’s mission and strategic goals by ensuring that taxpayer dollars and government services serve their intended purposes.

The heightened fraud risks and prevalence of fraud in various relief programs during the COVID-19 pandemic underscore the imperative for federal agencies to manage fraud risks strategically. To help federal program managers strategically manage their fraud risks during both normal operations and emergencies, we published *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework) in July 2015.<sup>4</sup> In June 2016, the Fraud Reduction and Data Analytics Act of 2015 (FRDAA) required the Office of Management and Budget (OMB) to establish guidelines for federal agencies to create controls to identify and assess fraud risks and to design and implement antifraud control activities. The act further required OMB to incorporate the leading

---

<sup>3</sup>GAO, *Unemployment Insurance: Data Indicate Substantial Levels of Fraud during the Pandemic; DOL Should Implement an Antifraud Strategy*, [GAO-23-105523](#) (Washington, D.C.: Dec. 22, 2022). It should be noted that such an extrapolation may be substantially understated and has inherent limitations and should be interpreted with caution.

<sup>4</sup>GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015).

---

practices from the Fraud Risk Framework in the guidelines.<sup>5</sup> In March 2020, the Payment Integrity Information Act of 2019 (PIIA) repealed FRDAA but maintained the requirement for OMB to provide guidance to agencies in implementing the Fraud Risk Framework.<sup>6</sup>

Since we issued the Fraud Risk Framework in July 2015, we have issued over 70 reports with recommendations to federal agencies to align their efforts to manage fraud risks with leading practices from the Fraud Risk Framework or the fraud risk principle of *Standards for Internal Control in the Federal Government* (Green Book).<sup>7</sup>

We prepared this report under the authority of the Comptroller General to conduct work to assist Congress with its oversight responsibilities. This report highlights areas where our prior work has shown that federal agencies and Congress can improve fraud risk management efforts.

To address our objective, we identified GAO reports issued from July 2015 through December 2022 that assessed agency efforts against one or more leading practices from the Fraud Risk Framework or the Green Book's fraud risk principle. We reviewed these reports to identify recommendations made to align agency efforts with these criteria. We determined the status of relevant recommendations as of January 2023. We analyzed the content of the recommendations to identify broad areas in which federal agency actions to manage fraud risks could be improved. We also reviewed the reports for examples of federal agencies meeting leading practices from the Fraud Risk Framework.

In addition to recommendations to various agencies, we identified recommendations to OMB and Matters for Congressional Consideration that could help improve federal fraud risk management efforts.

This report is based upon work we previously conducted 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

---

<sup>5</sup>Pub. L. No. 114-186, 130 Stat. 546 (2016).

<sup>6</sup>The Payment Integrity Information Act of 2019 requires 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.

<sup>7</sup>Principle 8 states that management should consider the potential for fraud when identifying, analyzing, and responding to risks. [GAO-14-704G](#).

---

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

---

## Background

---

### Fraud Risk Framework

The objective of fraud risk management is to help ensure program integrity by continuously and strategically mitigating both the likelihood and effects of fraud. When fraud risks can be identified and mitigated, fraud may be less likely to occur.<sup>8</sup> Although the occurrence of fraud indicates there is a fraud risk, a fraud risk can exist even if actual fraud has not yet occurred or been identified. Effectively managing fraud risk helps to ensure that federal programs' services fulfill their intended purpose, funds are spent effectively, and assets are safeguarded. Executive branch agency managers are responsible for managing fraud risks and implementing practices for combating those risks.

As discussed previously, in July 2015, we issued the Fraud Risk Framework to serve as a guide for agency managers—during normal operations, as well as during emergencies—when developing or enhancing efforts to combat fraud in a strategic, risk-based way.<sup>9</sup> The Fraud Risk Framework is also aligned with Principle 8 (“Assess Fraud Risk”) of the Green Book. As depicted below in figure 1, the Fraud Risk Framework describes leading practices within four components: commit, assess, design and implement, and evaluate and adapt.

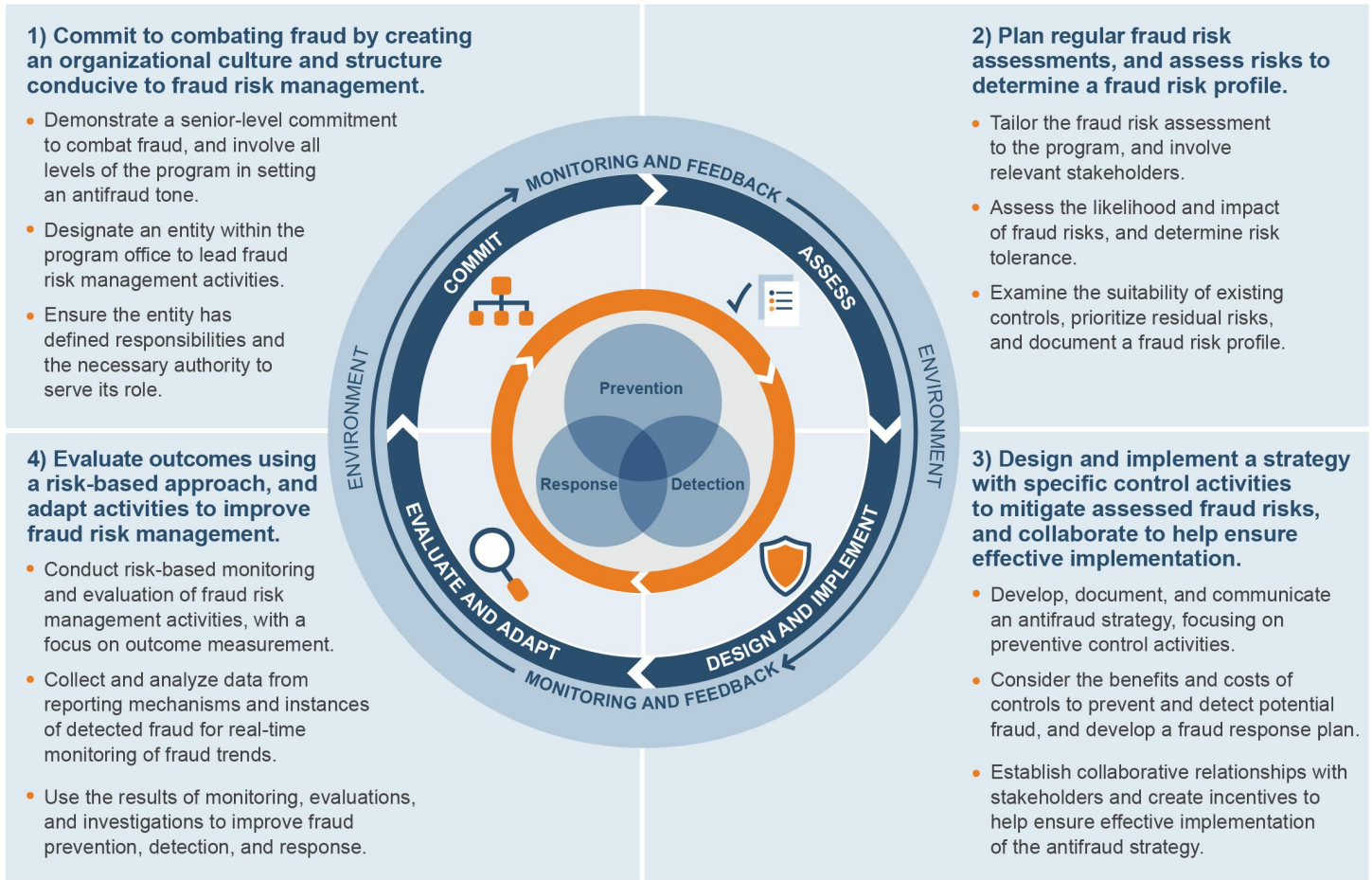
---

<sup>8</sup>Fraud and “fraud risk” are distinct concepts. *Fraud*—obtaining something of value through willful misrepresentation—is a determination to be made through the judicial or other adjudicative system, and that determination is beyond management’s professional responsibility. *Fraud risk* exists when individuals have an opportunity to engage in fraudulent activity, have an incentive or are under pressure to commit fraud, or are able to rationalize committing fraud.

<sup>9</sup>[GAO-15-593SP](#).



**Figure 1: The Fraud Risk Framework and Selected Leading Practices**



Source: GAO (information and icons). | GAO-23-106567

**Text of Figure 1: The Fraud Risk Framework and Selected Leading Practices**

- 1) Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
  - a) Demonstrate a senior-level commitment to combat fraud, and involve all levels of the program in setting an antifraud tone.
  - b) Designate an entity within the program office to lead fraud risk management activities.
  - c) Ensure the entity has defined responsibilities and the necessary authority to serve its role.

- 2) Plan regular fraud risk assessments, and assess risks to determine a fraud risk profile.
  - a) Tailor the fraud risk assessment to the program, and involve relevant stakeholders.
  - b) Assess the likelihood and impact of fraud risks, and determine risk tolerance.
  - c) Examine the suitability of existing controls, prioritize residual risks, and document a fraud risk profile.
- 3) Design and implement a strategy with specific control activities to mitigate assessed fraud risks, and collaborate to help ensure effective implementation.
  - a) Develop, document, and communicate an antifraud strategy, focusing on preventive control activities.
  - b) Consider the benefits and costs of controls to prevent and detect potential fraud, and develop a fraud response plan.
  - c) Establish collaborative relationships with stakeholders and create incentives to help ensure effective implementation of the antifraud strategy.
- 4) Evaluate outcomes using a risk-based approach, and adapt activities to improve fraud risk management.
  - a) Conduct risk-based monitoring and evaluation of fraud risk management activities, with a focus on outcome measurement.
  - b) Collect and analyze data from reporting mechanisms and instances of detected fraud for real-time monitoring of fraud trends.
  - c) Use the results of monitoring, evaluations, and investigations to improve fraud prevention, detection, and response.

Source: GAO. | GAO-23-106567

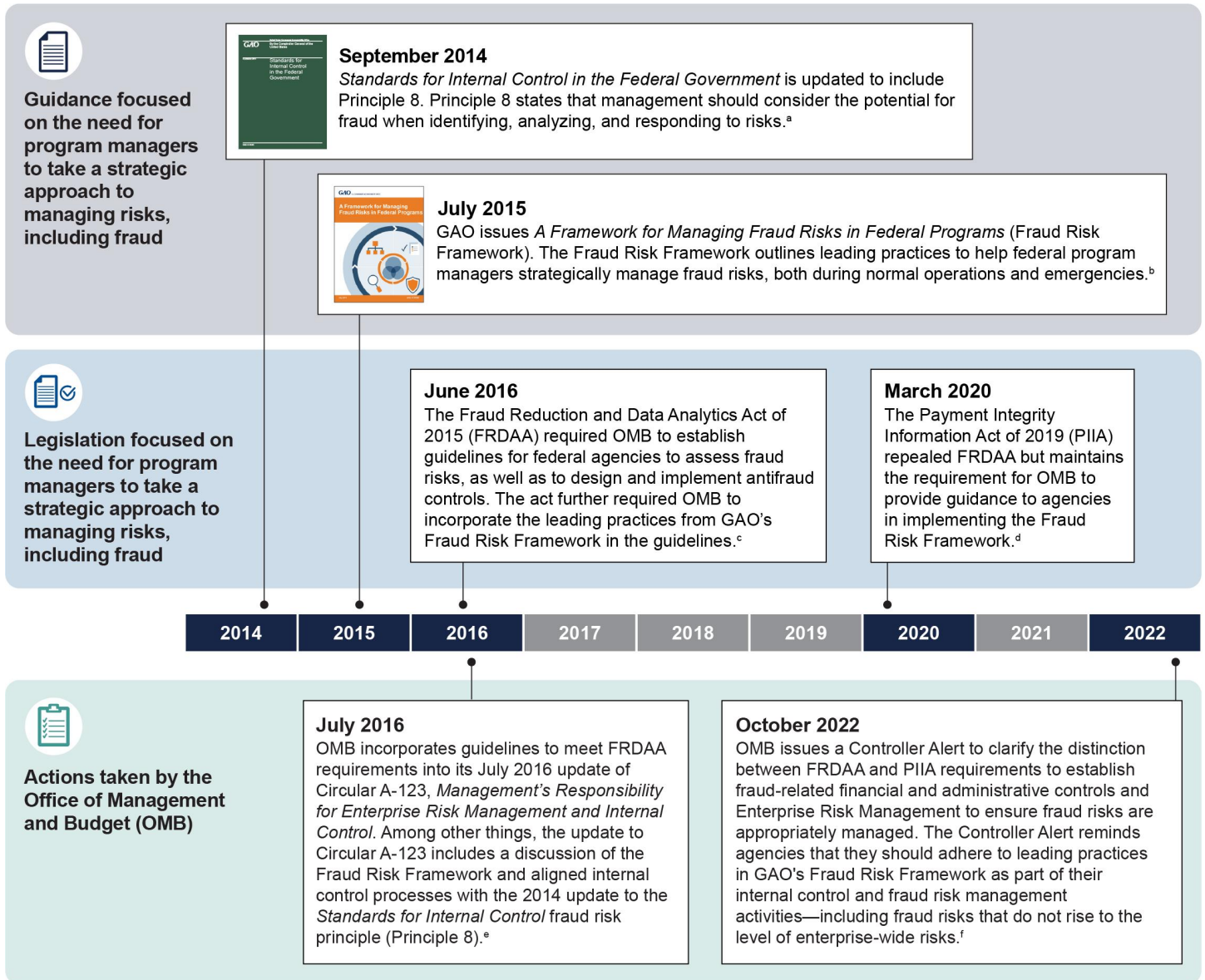
---

---

## Legislation and Guidance

Legislation and guidance have increasingly focused on the need for program managers to take a strategic approach to managing risks, including fraud (see fig. 2).

**Figure 2: Legislation and Guidance Related to Fraud Risk Management**



Sources: GAO and sdcoret/stock.adobe.com (icons). | GAO-23-106567

---

**Text of Figure 2: Legislation and Guidance Related to Fraud Risk Management**

- 1) Guidance focused on the need for program managers to take a strategic approach to managing risks, including fraud
  - a) September 2014 - *Standards for Internal Control in the Federal Government* is updated to include Principle 8. Principle 8 states that management should consider the potential for fraud when identifying, analyzing, and responding to risks.<sup>a</sup>
- 2) July 2015 - GAO issues *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework). The Fraud Risk Framework outlines leading practices to help federal program managers strategically manage fraud risks, both during normal operations and emergencies.<sup>b</sup>
- 3) Legislation focused on the need for program managers to take a strategic approach to managing risks, including fraud
  - a) June 2016 - The Fraud Reduction and Data Analytics Act of 2015 (FRDAA) required OMB to establish guidelines for federal agencies to assess fraud risks, as well as to design and implement antifraud controls. The act further required OMB to incorporate the leading practices from GAO's Fraud Risk Framework in the guidelines.<sup>c</sup>
  - b) March 2020 - The Payment Integrity Information Act of 2019 (PIIA) repealed FRDAA but maintains the requirement for OMB to provide guidance to agencies in implementing the Fraud Risk Framework.<sup>d</sup>
- 4) Actions taken by the Office of Management and Budget (OMB)
  - a) July 2016 - OMB incorporates guidelines to meet FRDAA requirements into its July 2016 update of Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. Among other things, the update to Circular A-123 includes a discussion of the Fraud Risk Framework and aligned internal control processes with the 2014 update to the *Standards for Internal Control* fraud risk principle (Principle 8).<sup>e</sup>
  - b) October 2022 - OMB issues a Controller Alert to clarify the distinction between FRDAA and PIIA requirements to establish fraud-related financial and administrative controls and Enterprise Risk Management to ensure fraud risks are appropriately

---

managed. The Controller Alert reminds agencies that they should adhere to leading practices in GAO's Fraud Risk Framework as part of their internal control and fraud risk management activities—including fraud risks that do not rise to the level of enterprise-wide risks.<sup>f</sup>

Source: GAO. | GAO-23-106567

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

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

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

<sup>d</sup>Pub. L. No. 116-117, § 2(a), 134 Stat. 113, 131-132 (2020), codified at 31 U.S.C. § 3357.

<sup>e</sup>OMB, *Management's Responsibility for Enterprise Risk Management and Internal Control*, OMB Circular A-123 (Washington, D.C.: July 15, 2016).

<sup>f</sup>OMB, *Establishing Financial and Administrative Controls to Identify and Assess Fraud Risk*, CA-23-03 (Washington, D.C.: Oct. 17, 2022). Enterprise risk management is a decision-making tool that can assist federal leaders to anticipate and manage risks across their portfolios. Prior to implementing enterprise risk management, risk management focused on traditional internal control concepts for managing risk exposures. Beyond traditional internal controls, enterprise risk management promotes risk management by considering its effect across the entire organization and how it may interact with other identified risks.

Congress enacted FRDAA to improve federal agency controls and procedures to assess and mitigate fraud risks, and to improve agencies' development and use of data analytics for the purpose of identifying, preventing, and responding to fraud. As mentioned, FRDAA required OMB to establish guidelines for federal agencies to create controls to identify and assess fraud risks and to design and implement anti-fraud control activities. The act further required OMB to incorporate the leading practices from the Fraud Risk Framework in the guidelines. In addition, FRDAA required agencies to annually report to Congress on their progress in implementing the act for each of the first 3 fiscal years after its enactment.

To comply with FRDAA, OMB updated existing guidelines for agencies to establish financial and administrative controls to manage fraud risks. Specifically, OMB incorporated guidelines to meet FRDAA requirements into its July 2016 update of Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. This particular update of Circular A-123 introduced requirements for agencies to implement enterprise risk management and integrate with existing internal control capabilities to improve mission delivery, reduce costs, and focus

corrective actions on key risks.<sup>10</sup> The update to Circular A-123 also included a discussion of the Fraud Risk Framework and aligned internal control processes with the 2014 update to the Green Book—such as the reference to the fraud risk principle (Principle 8).

In March 2020, PIIA repealed FRDAA but required the OMB guidelines to remain in effect, subject to modification by OMB as necessary, and in consultation with GAO.

In October 2022, in response to one of our recommendations in this area, OMB issued a Controller Alert to clarify the distinction between FRDAA/PIIA requirements to establish fraud-related financial and administrative controls and enterprise risk management to ensure fraud risks are appropriately managed.<sup>11</sup> The Controller Alert reminds agencies that they should adhere to leading practices in GAO’s Fraud Risk 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.

The Controller Alert also reminds agencies that the dollar thresholds established in 31 U.S.C. § 3352 by PIIA 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. As such, all programs regardless of their improper payment risks or rates should be strategically managing their fraud risks. Clarifying these requirements for fraud risk management will help ensure that agencies are better positioned to

---

<sup>10</sup>Enterprise risk management is a decision-making tool that can assist federal leaders to anticipate and manage risks across their portfolios. Prior to implementing enterprise risk management, risk management focused on traditional internal control concepts for managing risk exposures. Beyond traditional internal controls, enterprise risk management promotes risk management by considering its effect across the entire organization and how it may interact with other identified risks.

<sup>11</sup>In December 2018, we reported that the OMB guidelines were unclear on the relationship between requirements for managing fraud risks and enterprise risk management requirements and that uncertainty about the difference between enterprise risk management and FRDAA requirements may have affected agencies’ implementation of the requirements in the act. We recommended that OMB enhance the guidelines for agencies to establish the controls required by FRDAA by clarifying the difference between FRDAA and enterprise risk management requirements. As noted, OMB has since taken action to address this recommendation. OMB, *Establishing Financial and Administrative Controls to Identify and Assess Fraud Risk*, CA-23-03 (Washington, D.C., Oct. 17, 2022).

---

improve controls and procedures to assess and mitigate fraud risks in federal programs.

---

## Key Areas for Improving Fraud Risk Management

Our prior work has highlighted five areas in which federal agencies need to take additional actions to help ensure they are effectively managing fraud risks, consistent with leading practices in the Fraud Risk Framework.<sup>12</sup> Specifically, agencies need to take additional actions related to (1) designating an entity to lead fraud risk management, (2) assessing fraud risks, (3) designing and implementing an antifraud strategy, (4) using data analytics to manage fraud risks, and (5) managing fraud risks in emergencies. From July 2015 through December 2022, we made 142 recommendations to over 40 agency or program offices related to one or more of these areas to align with leading practices from the Fraud Risk Framework or the Green Book’s fraud risk principle.<sup>13</sup> As of January 2023, agencies needed to take additional action to fully address 74 of these recommendations.<sup>14</sup> In addition, our prior work identified opportunities for Congress to take action to focus agency attention on strategic fraud risk management.

---

<sup>12</sup>The Fraud Risk Framework’s leading practices can be implemented at the agency level or the program level. In some instances, prior work assessed fraud risk management efforts at the agency level and in other instances prior work assessed efforts at the program level. We generally use the term “agency” in this report to include agencies or programs.

<sup>13</sup>Some recommendations relate to more than one area. For example, we made a recommendation to the Department of Health and Human Services’s Administration for Children and Families to conduct a fraud risk assessment to provide a basis for the documentation and development of an antifraud strategy for the Child Care and Development Fund. This recommendation is included in the number of recommendations related to assessing fraud risks and designing and implementing an antifraud strategy.

<sup>14</sup>Of the 142 recommendations, 67 were closed as implemented, one was closed as not implemented, 11 were open but had been partially addressed, and 63 were open and had not been addressed. We follow up on recommendations we have made and update the status at least once per year. Experience has shown that it takes time for some recommendations to be implemented. Of the 142 recommendations, 21 were made on or after January 1, 2022, and 19 of the 21 remained open as of January 2023.



---

---

## Federal Agencies Need to Improve Fraud Risk Management Efforts in Five Areas

### Designating an Entity to Lead Fraud Risk Management

The first component of the Fraud Risk Framework—commit—calls for agencies to designate an entity to lead fraud risk management activities. Specifically, the Fraud Risk Framework calls for the designated antifraud entity to have defined responsibilities and the necessary authority to perform its role in managing the fraud risk assessment process (in the second component) and coordinating antifraud initiatives, among other things. We have consistently reported that leadership commitment is the critical element for initiating and sustaining progress and making the types of management and operational improvements required for narrowing or removing areas from our list of programs and operations at high risk of waste, fraud, abuse, or mismanagement, or in need of transformation.<sup>15</sup> Further, our prior work has shown that when agencies formally designate an entity to design and oversee fraud risk management activities, their efforts can be more visible across the agency, particularly to executive leadership.<sup>16</sup>

Our prior work has identified instances in which agencies have designated an antifraud entity that aligns with leading practices from our Fraud Risk Framework. For example, in April 2017, we reported that the Social Security Administration (SSA) demonstrated a commitment to antifraud efforts by conducting a study to evaluate its fraud risk management approach and, shortly thereafter, by establishing a dedicated antifraud office within the agency.<sup>17</sup> Specifically, SSA established the Office of Anti-Fraud Programs in November 2014. The office is responsible for coordinating antifraud efforts, developing antifraud policies, and creating and implementing fraud mitigation plans across SSA, among other things. We reported that these responsibilities are consistent with leading practices and help SSA show commitment to

---

<sup>15</sup>We designate federal programs and operations as “high risk” due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or because they need transformation. GAO, *High-Risk Series: Key Practices to Successfully Address High-Risk Areas and Remove Them from the List*, [GAO-22-105184](#) (Washington, D.C.: Mar. 3, 2022).

<sup>16</sup>For example, see GAO, *Medicare and Medicaid: CMS Needs to Fully Align Its Antifraud Efforts with the Fraud Risk Framework*, [GAO-18-88](#) (Washington, D.C.: Dec. 5, 2017).

<sup>17</sup>GAO, *SSA Disability Benefits: Comprehensive Strategic Approach Needed to Enhance Antifraud Activities*, [GAO-17-228](#) (Washington, D.C.: Apr. 17, 2017).

combating fraud and help ensure that antifraud initiatives are coordinated across the agency.

Our prior work, however, has also identified instances in which federal agencies need to take additional action related to designating an entity to lead fraud risk management activities. Specifically, from July 2015 through December 2022, we made eight recommendations to federal agencies in this area. This work includes recommendations to dedicate an entity to oversee fraud risk management activities or to document the fraud risk management responsibilities of the antifraud entity. Of the eight recommendations, six remained open as of January 2023.<sup>18</sup>

For example, in October 2021, we found that DOL had not clearly assigned defined responsibilities to a dedicated antifraud entity.<sup>19</sup> We recommended that DOL designate a dedicated antifraud entity with clearly defined and documented responsibilities and authority, including responsibility and authority for facilitating communication among stakeholders about fraud-related issues. In February 2023, DOL told us it designated its chief financial officer (CFO) as the dedicated entity responsible for managing the process of assessing fraud risks to the Unemployment Insurance program. However, it is still too early to tell whether the CFO will perform this role in a manner that is consistent with leading practices, such as by coordinating antifraud initiatives across the agency and serving as the repository of knowledge on fraud controls, among other things. As such, we will continue to monitor DOL's progress in implementing this recommendation. Until DOL and other agencies fully establish a dedicated entity for managing fraud risks in a manner that is consistent with leading practices, they will lack a critical element of agency commitment to effective fraud risk management.

### Assessing Fraud Risks

The second component of the Fraud Risk Framework—*assess*—calls for agencies to plan and conduct regular fraud risk assessments, including

---

<sup>18</sup>Of the eight recommendations, two were closed as implemented, one was open but had been partially addressed, and five were open and had not been addressed. As previously noted, we follow up on recommendations we have made and update the status at least once per year. Experience has shown that it takes time for some recommendations to be implemented. Of the eight recommendations, two were made on or after January 1, 2022, and both remained open as of January 2023.

<sup>19</sup>GAO, *COVID-19: Additional Actions Needed to Improve Accountability and Program Effectiveness of Federal Response*, [GAO-22-105051](#) (Washington, D.C.: Oct. 27, 2021).

identifying and assessing fraud risks and documenting the results in a fraud risk profile. In particular, an effective antifraud entity tailors the approach for carrying out a fraud risk assessment to the program. Planning and conducting a fraud risk assessment can help managers to fully consider fraud risks to their programs—including existing and emerging risks—and to analyze their likelihood and impact, and prioritize risks. Such an assessment can provide the detailed information and insights needed to create a fraud risk profile, which, in turn, is the basis for creating an antifraud strategy (in the third component). As a result, fully assessing fraud risks can better position management to determine the extent to which antifraud controls may no longer be relevant or cost effective and strengthen antifraud controls, by designing and implementing the most-appropriate control activities to respond to the full portfolio of fraud risks.

Our prior work has identified instances in which agencies have taken steps to assess fraud risks in accordance with leading practices from our Fraud Risk Framework. For example, in response to a recommendation we made in 2017, the Centers for Medicare & Medicaid Services (CMS) has taken steps to assess fraud risks in the Medicare and Medicaid programs. Specifically, in December 2017, we found that CMS had taken steps to identify some fraud risks to the Medicare and Medicaid programs, but it had not conducted a fraud risk assessment for either program.<sup>20</sup> We also found that CMS would be unable to design and implement the most-appropriate control activities to respond to its full portfolio of fraud risks by following its approach at the time of our 2017 report. At that time, CMS's approach focused on addressing specific vulnerabilities among provider groups that had shown themselves to be particularly prone to fraud, waste, and abuse and did not fully consider other sources of fraudulent behaviors, such as those posed by health-insurance plans, contractors, or employees. We recommended that CMS conduct fraud risk assessments for Medicare and Medicaid to include fraud risk profiles and plans for regularly updating the assessments and profiles.

In response to our recommendation, CMS provided us with documentation of risk assessment frameworks for program areas within Medicare and Medicaid. These frameworks include a standard format to document vulnerabilities, risk levels, residual risks, and mitigation

---

<sup>20</sup>[GAO-18-88](#).

strategies, among other topics.<sup>21</sup> CMS's approach also includes regularly re-examining vulnerabilities based on risk and environmental factors, consistent with leading practices. We have continually designated Medicare and Medicaid as high risk, partly due to their vulnerability to fraud, waste, and abuse. Conducting risk assessments is an important step that can better position CMS to develop an antifraud strategy with specific control activities to address these substantial fraud risks.

Federal agencies, however, need to take additional action to implement our other recommendations related to assessing fraud risks. Specifically, from July 2015 through December 2022, we made 73 recommendations to federal agencies related to assessing fraud risks. This includes recommendations to plan and conduct regular fraud risk assessments, revise or update existing fraud risk management activities to include a fraud risk tolerance, or document a fraud risk profile. Of the 73 recommendations, 36 remained open as of January 2023.<sup>22</sup>

For example, in September 2019, we found that the Office of Head Start (OHS) had not conducted a comprehensive fraud risk assessment of the Head Start program.<sup>23</sup> We also reported on vulnerabilities in some Head Start centers' controls for detecting potential fraud. Posing as fictitious families, we attempted to enroll children at a nongeneralizable selection of Head Start centers in metropolitan areas. For each of the 15 covert tests we conducted, we provided incomplete or potentially disqualifying information during the enrollment process, such as pay stubs that exceeded income requirements. In five of 15 covert tests, we found potential fraud. For example, in three of these five cases, documents we later retrieved from the three Head Start centers showed that our

---

<sup>21</sup>Residual risk is the risk that remains after inherent risks have been mitigated by existing control activities.

<sup>22</sup>Of the 73 recommendations, 36 were closed as implemented, one was closed as not implemented, three were open but had been partially addressed, and 33 were open and had not been addressed. We follow up on recommendations we have made and update the status at least once per year. Experience has shown that it takes time for some recommendations to be implemented. Of the 73 recommendations, seven were made on or after January 1, 2022, and all seven remained open as of January 2023.

<sup>23</sup>GAO, *Head Start: Action Needed to Enhance Program Oversight and Mitigate Significant Fraud and Improper Payment Risks*, [GAO-19-519](#) (Washington, D.C.: Sept. 13, 2019).

---

applications had been doctored to exclude income information we provided, which would have shown the fictitious family to be ineligible.<sup>24</sup>

During the course of that review, OHS officials told us they did not believe the Head Start program was at a significant risk of fraud. However, without a comprehensive fraud risk assessment, OHS cannot support this determination. We recommended that OHS perform a fraud risk assessment for the Head Start program, to include assessing the likelihood and impact of the fraud risks it faces.

As of January 2023, OHS told us that its fraud risk assessment approach is still under development and that a timeline for completing this work had not been established. Completing a fraud risk assessment could help OHS better identify and address the fraud risk vulnerabilities we identified and better position OHS to design and implement an effective antifraud strategy for the Head Start program. Similarly, taking steps to address recommendations in this area can help ensure other agencies with open recommendations are best positioned to design and implement the most-appropriate control activities to respond to their full portfolios of fraud risks.

### Designing and Implementing an Antifraud Strategy

The third component of the Fraud Risk Framework—design and implement—calls for agencies to determine risk responses and document an antifraud strategy that describes the agency’s approach for addressing the prioritized fraud risks identified during the fraud risk assessment. A key element of an antifraud strategy is to describe the agency’s activities for preventing, detecting, and responding to fraud, as well as monitoring and evaluation, among other things. Developing and documenting an antifraud strategy based on a fraud risk assessment can help agencies to develop a coordinated approach to address the range of fraud risks and to appropriately target and allocate resources to the most significant risks. Entities that do not create an antifraud strategy based explicitly on a fraud risk assessment and corresponding fraud risk profile might fail to address fraud vulnerabilities that could affect their performance, undermine their reputation, or impair their ability to fulfill their missions.

---

<sup>24</sup>To view selected video clips of these undercover enrollments, go to <https://www.gao.gov/products/GAO-19-519>.

Our prior work has found instances in which agencies have taken steps to design and implement an antifraud strategy. For example, in July 2018 we found that the Export-Import Bank of the United States (EXIM) had instituted a number of antifraud controls, but it had not developed an antifraud strategy based on a fraud risk profile, or implemented specific control activities to achieve such a strategy.<sup>25</sup> We recommended that EXIM develop and implement an antifraud strategy with specific control activities, based on the results of fraud risk assessments and a corresponding fraud risk profile. In response to our recommendation, in 2019 EXIM developed an antifraud strategy with specific control activities based on the results of its fraud risk assessment and took steps to implement the strategy. Developing and documenting an antifraud strategy can help EXIM ensure it is strategically managing its fraud risks.

Federal agencies, however, need to take additional steps to design and implement effective antifraud strategies. From July 2015 through December 2022, we made 21 recommendations in this area. This includes recommendations to develop an antifraud strategy that aligns with assessed fraud risks, document the antifraud strategy, or update an existing antifraud strategy. Of the 21 recommendations, 11 remained open as of January 2023.<sup>26</sup>

For example, in March 2017, we reported that the Department of Energy (DOE) had not implemented leading practices—including developing and documenting a strategy to mitigate assessed fraud risks—to manage its risk of fraud and improper payments.<sup>27</sup> According to DOE officials, they did not implement leading practices for managing the department’s risk of fraud because they consider the risk of fraud to be low. Because DOE had not developed and documented an antifraud strategy that describes its programs’ approaches for addressing fraud risks, DOE was missing an opportunity to allocate resources more effectively to respond to fraud

---

<sup>25</sup>GAO, *Export-Import Bank: The Bank Needs to Continue to Improve Fraud Risk Management*, [GAO-18-492](#) (Washington, D.C.: July 19, 2018).

<sup>26</sup>Of the 21 recommendations, 10 were closed as implemented, two were open but had been partially addressed, and nine were open and had not been addressed. As previously noted, we follow up on recommendations we have made and update the status at least once per year. Experience has shown that it takes time for some recommendations to be implemented. Of the 21 recommendations, five were made on or after January 1, 2022, of which three remained open as of January 2023.

<sup>27</sup>GAO, *Department of Energy: Use of Leading Practices Could Help Manage the Risk of Fraud and Other Improper Payments*, [GAO-17-235](#) (Washington, D.C.: Mar. 30, 2017).

risks. We recommended that DOE develop and document an antifraud strategy that describes the programs' approaches for addressing the prioritized fraud risks identified during a fraud risk assessment.

At the time, DOE generally concurred with this recommendation but did not provide plans to develop and document an antifraud strategy to address the recommendation. Specifically, DOE stated that DOE believed it had implemented the requirements of the 2016 update to OMB Circular A-123 and believed it had embedded its antifraud strategy within its internal control program.<sup>28</sup> However, DOE officials told us during the audit that they had not developed or documented a DOE-wide antifraud strategy or directed individual programs to develop program-specific strategies. In January 2021, we found that DOE was planning to develop an antifraud strategy in fiscal year 2022.<sup>29</sup> As of February 2023, we are continuing to monitor DOE's progress in implementing this recommendation. Until DOE and other agencies with open recommendations in this area implement those recommendations, they are missing an opportunity to organize and focus resources in a way that would allow them to strategically mitigate the likelihood and impact of fraud.

### Using Data Analytics to Manage Fraud Risks

The Fraud Risk Framework's leading practices include managers implementing data-analytics activities as part of an overall antifraud strategy. According to the Fraud Risk Framework, data-analytics activities can include a variety of techniques. For example, data-mining and data-matching techniques can enable agencies to identify potential fraud or improper payments that have already been awarded, thus assisting agencies in recovering these dollars. Predictive analytics can identify potential fraud before making payments. In particular, we have highlighted the importance of data matching and other techniques to

---

<sup>28</sup>As discussed previously, we reported in December 2018 that OMB guidelines were unclear on the relationship between requirements for managing fraud risks and enterprise risk management requirements and that uncertainty about the difference between enterprise risk management and FRDAA requirements may have affected agencies' implementation of the requirements in the act. We recommended that OMB enhance the guidelines for agencies to establish the controls required. OMB has since taken action to address this recommendation.

<sup>29</sup>GAO, *Department of Energy Contracting: Improvements Needed to Ensure DOE Assesses its Full Range of Contracting Fraud Risks*, [GAO-21-44](#) (Washington, D.C.: Jan. 13, 2021).

verify self-reported information and other information necessary for determining eligibility for enrolling in programs or receiving benefits.

Our prior work has identified instances in which agencies have used data analytics in alignment with leading practices from our Fraud Risk Framework. For example, in 2019 we reported that, according to U.S. Citizenship and Immigration Services (USCIS) officials, the agency had data-analytics capabilities that it used as part of its efforts to identify and prevent fraud within immigration benefit programs. However, we found that USCIS had not applied these capabilities as an antifraud tool specifically for the self-petition program for foreign national victims of battery or extreme cruelty committed by certain U.S. citizens or lawful permanent residents. We recommended that USCIS develop and implement data-analytics capabilities for the self-petition program as a means to prevent and detect fraud as provided by GAO's Fraud Risk Framework.

In response to our recommendation, in December 2020 USCIS officials provided us documentation of their analysis of self-petition application data to identify populations of self-petitions vulnerable to fraud. USCIS officials told us they plan to build on and improve their data-analysis tools as a part of their ongoing annual fraud risk assessments. By employing data analytics within the self-petition program, USCIS can improve its efforts to detect and prevent potential fraud in self-petition filings, as well as inform the self-petition program's regular fraud risk assessments.

Federal agencies, however, need to take additional actions to implement other recommendations in this area. Specifically, from July 2015 through December 2022, we made 40 recommendations to federal agencies to use data analytics in accordance with leading practices to help manage fraud risks in their programs. This includes recommendations to design and implement data-analytics activities to prevent and detect fraud, such as using data matching to verify self-reported information. Of the 40 recommendations, 20 remained open as of January 2023.<sup>30</sup>

---

<sup>30</sup>Of the 40 recommendations, 20 were closed as implemented, three were open but had been partially addressed, and 17 were open and had not been addressed. We follow up on recommendations we have made and update the status at least once per year. Experience has shown that it takes time for some recommendations to be implemented. Of the 40 recommendations, seven were made on or after January 1, 2022, and all seven remained open as of January 2023.



For instance, in 2020 we determined that limitations in the Federal Aviation Administration’s (FAA) use of data in its processes for registering civil aircraft hindered FAA’s ability to prevent registry fraud and abuse. Specifically, FAA’s registry is vulnerable to fraud and abuse when applicants register aircraft using opaque ownership structures that afford limited transparency into who is the actual beneficial owner (i.e., the person who ultimately owns and controls the aircraft). Such structures can be used to own aircraft associated with money laundering or other illegal activities (see example in figure 3). We also reported that FAA has an opportunity to develop data-analytics capabilities to detect indicators of fraud and abuse in the registry.

**Figure 3: Case Study Illustrating Aircraft-Related Criminal Activity Risks**



Sources: GAO analysis of court records and FAA information; GAO (photos and icons). | GAO-23-106567

**Text of Figure 3: Case Study Illustrating Aircraft-Related Criminal Activity Risks**

**U.S.-registered aircraft purchased with assets derived from illegal activity**

- U.S. corporation with Venezuelan beneficial owner purchased aircraft using proceeds from a scheme that involved a black-market currency exchange involving Venezuelan bolivars and U.S. dollars.
- An intermediary established a corporation on behalf of the foreign beneficial owner and registered aircraft with the Federal Aviation Administration (FAA).

---

Source: GAO analysis of court records and FAA information. | GAO-23-106567

U.S. law enforcement seized the aircraft because it was purchased with assets traceable to money laundering or other illegal activity, and the aircraft was forfeited to the U.S. government.

To address these concerns, we made multiple recommendations, including recommendations for FAA to collect and analyze data to identify patterns of activity indicative of fraud or abuse, among other things. Since our report, FAA has reported that it plans to take steps to address these recommendations, including steps to partner with external government agencies to identify ways to share data and verify eligibility. However, these efforts have not been completed and, as of January 2023, the recommendations remained open. Until FAA fully implements these steps, it is limited in its ability to prevent fraud and abuse in aircraft registrations, which enable aircraft-related criminal, national security, or safety risks. Similarly, taking steps to address open recommendations in this area can help ensure and enhance coordination efforts with other agencies in effectively using data to prevent or detect fraud.

### Managing Fraud Risks in Emergencies

During emergencies—such as natural disasters, public health emergencies, or economic crises—federal agencies must get relief funds out quickly while ensuring appropriate financial and other safeguards are in place. Recognizing fraud risks, and thoughtfully and deliberately managing them in an emergency environment, can help federal managers safeguard public resources while providing needed relief. The leading practices from the Fraud Risk Framework apply during normal operations, as well as during emergencies. We have previously reported that emergency-related considerations and adjustments, such as the heightened risk of fraud in an emergency environment and the need to adjust risk tolerance in assessing fraud risks, facilitate fraud risk management in an emergency environment.<sup>31</sup> Figure 4 shows illustrative

---

<sup>31</sup>We also have ongoing work developing a framework to provide principles and practices that can help federal managers mitigate improper payments in emergency assistance programs. Specifically, the framework will incorporate standards for internal controls and for financial and fraud risk management practices as well as requirements from relevant laws and guidance on improper payments. This work will highlight aspects of managing improper payments that arise in the context of emergency assistance, which may necessitate special considerations. This framework is also intended as a resource for Congress to use when designing new programs or appropriating additional funding in response to emergencies.
















---

**Letter**

---

examples of fraud risks and schemes applicable to an emergency environment.

**Figure 4: Examples of Fraud Risks and Possible Schemes Targeting Government and Private Businesses and Individuals during Emergencies**

Fraud committed by	Examples								
<p><b>Fraud against Government</b></p>	<table border="1"> <tr> <td data-bbox="363 569 727 905">  <p><b>Business or individual beneficiaries through false statements</b></p> </td> <td data-bbox="740 569 1503 905"> <ul style="list-style-type: none"> <li>▶ Small business inflates claimed payroll expense to qualify for a larger Small Business Administration (SBA) loan</li> <li>▶ Large business misreports the number of employees to appear eligible for an SBA loan</li> <li>▶ Business owner certifies SBA loan will be used to pay employees, but diverts funds for personal use</li> <li>▶ Individual inappropriately files unemployment insurance claims in multiple states during the same time frame using the same personal information</li> <li>▶ Self-employed individual overstates earnings in unemployment insurance claim</li> </ul> </td> </tr> <tr> <td data-bbox="363 915 727 1171">  <p><b>Parties providing goods or services</b></p> </td> <td data-bbox="740 915 1503 1171"> <ul style="list-style-type: none"> <li>▶ Vendor bills for nonexistent personal protective equipment (PPE)</li> <li>▶ Vendor substitutes noncompliant, substandard PPE and certifies it satisfied contract specifications</li> <li>▶ Vendor creates false appearance of competition and inflates prices by disguising ownership in multiple fake companies submitting false bids or by disguising availability of services from actual competitors</li> <li>▶ Health care provider bills Medicare or Medicaid for COVID-related testing that was never administered</li> </ul> </td> </tr> <tr> <td data-bbox="363 1182 727 1350">  <p><b>Government employees</b></p> </td> <td data-bbox="740 1182 1503 1350"> <ul style="list-style-type: none"> <li>▶ Employee reports government property as stolen and takes it for personal use</li> <li>▶ Contracting officer receives kickbacks during contract award or administration</li> <li>▶ Employee inflates time and attendance records</li> </ul> </td> </tr> <tr> <td data-bbox="363 1360 727 1528">  <p><b>Criminal organizations<sup>a</sup></b></p> </td> <td data-bbox="740 1360 1503 1528"> <ul style="list-style-type: none"> <li>▶ Criminals use synthetic identities (combining real and fictitious information) to apply for unemployment insurance</li> <li>▶ Hackers send emails to government employees to access government-held data</li> </ul> </td> </tr> </table>	 <p><b>Business or individual beneficiaries through false statements</b></p>	<ul style="list-style-type: none"> <li>▶ Small business inflates claimed payroll expense to qualify for a larger Small Business Administration (SBA) loan</li> <li>▶ Large business misreports the number of employees to appear eligible for an SBA loan</li> <li>▶ Business owner certifies SBA loan will be used to pay employees, but diverts funds for personal use</li> <li>▶ Individual inappropriately files unemployment insurance claims in multiple states during the same time frame using the same personal information</li> <li>▶ Self-employed individual overstates earnings in unemployment insurance claim</li> </ul>	 <p><b>Parties providing goods or services</b></p>	<ul style="list-style-type: none"> <li>▶ Vendor bills for nonexistent personal protective equipment (PPE)</li> <li>▶ Vendor substitutes noncompliant, substandard PPE and certifies it satisfied contract specifications</li> <li>▶ Vendor creates false appearance of competition and inflates prices by disguising ownership in multiple fake companies submitting false bids or by disguising availability of services from actual competitors</li> <li>▶ Health care provider bills Medicare or Medicaid for COVID-related testing that was never administered</li> </ul>	 <p><b>Government employees</b></p>	<ul style="list-style-type: none"> <li>▶ Employee reports government property as stolen and takes it for personal use</li> <li>▶ Contracting officer receives kickbacks during contract award or administration</li> <li>▶ Employee inflates time and attendance records</li> </ul>	 <p><b>Criminal organizations<sup>a</sup></b></p>	<ul style="list-style-type: none"> <li>▶ Criminals use synthetic identities (combining real and fictitious information) to apply for unemployment insurance</li> <li>▶ Hackers send emails to government employees to access government-held data</li> </ul>
 <p><b>Business or individual beneficiaries through false statements</b></p>	<ul style="list-style-type: none"> <li>▶ Small business inflates claimed payroll expense to qualify for a larger Small Business Administration (SBA) loan</li> <li>▶ Large business misreports the number of employees to appear eligible for an SBA loan</li> <li>▶ Business owner certifies SBA loan will be used to pay employees, but diverts funds for personal use</li> <li>▶ Individual inappropriately files unemployment insurance claims in multiple states during the same time frame using the same personal information</li> <li>▶ Self-employed individual overstates earnings in unemployment insurance claim</li> </ul>								
 <p><b>Parties providing goods or services</b></p>	<ul style="list-style-type: none"> <li>▶ Vendor bills for nonexistent personal protective equipment (PPE)</li> <li>▶ Vendor substitutes noncompliant, substandard PPE and certifies it satisfied contract specifications</li> <li>▶ Vendor creates false appearance of competition and inflates prices by disguising ownership in multiple fake companies submitting false bids or by disguising availability of services from actual competitors</li> <li>▶ Health care provider bills Medicare or Medicaid for COVID-related testing that was never administered</li> </ul>								
 <p><b>Government employees</b></p>	<ul style="list-style-type: none"> <li>▶ Employee reports government property as stolen and takes it for personal use</li> <li>▶ Contracting officer receives kickbacks during contract award or administration</li> <li>▶ Employee inflates time and attendance records</li> </ul>								
 <p><b>Criminal organizations<sup>a</sup></b></p>	<ul style="list-style-type: none"> <li>▶ Criminals use synthetic identities (combining real and fictitious information) to apply for unemployment insurance</li> <li>▶ Hackers send emails to government employees to access government-held data</li> </ul>								
<p><b>Fraud against Private businesses and individuals</b></p>	<table border="1"> <tr> <td data-bbox="363 1556 727 1837">  <p><b>Criminal organizations</b></p> </td> <td data-bbox="740 1556 1503 1837"> <p><b>Criminal organizations engaging in:</b></p> <ul style="list-style-type: none"> <li>▶ Online scams offering COVID-19 testing or treatment</li> <li>▶ Sale of counterfeit PPE</li> <li>▶ Identity theft to claim Economic Impact Payments to individuals</li> <li>▶ Robocalls or emails with payment instructions or malware to steal personal information</li> <li>▶ False representation as a government employee demanding payments to expedite receipt of government assistance</li> </ul> </td> </tr> </table>	 <p><b>Criminal organizations</b></p>	<p><b>Criminal organizations engaging in:</b></p> <ul style="list-style-type: none"> <li>▶ Online scams offering COVID-19 testing or treatment</li> <li>▶ Sale of counterfeit PPE</li> <li>▶ Identity theft to claim Economic Impact Payments to individuals</li> <li>▶ Robocalls or emails with payment instructions or malware to steal personal information</li> <li>▶ False representation as a government employee demanding payments to expedite receipt of government assistance</li> </ul>						
 <p><b>Criminal organizations</b></p>	<p><b>Criminal organizations engaging in:</b></p> <ul style="list-style-type: none"> <li>▶ Online scams offering COVID-19 testing or treatment</li> <li>▶ Sale of counterfeit PPE</li> <li>▶ Identity theft to claim Economic Impact Payments to individuals</li> <li>▶ Robocalls or emails with payment instructions or malware to steal personal information</li> <li>▶ False representation as a government employee demanding payments to expedite receipt of government assistance</li> </ul>								

Sources: GAO analysis; GAO (icons). | GAO-23-106567

**Text of Figure 4: Examples of Fraud Risks and Possible Schemes Targeting Government and Private Businesses and Individuals during Emergencies**

	<b>Fraud committed by</b>	<b>Examples</b>
Fraud against Government	Business or individual beneficiaries through false statements	<ul style="list-style-type: none"> <li>• Small business inflates claimed payroll expense to qualify for a larger Small Business Administration (SBA) loan</li> <li>• Large business misreports the number of employees to appear eligible for an SBA loan</li> <li>• Business owner certifies SBA loan will be used to pay employees, but diverts funds for personal use</li> <li>• Individual inappropriately files unemployment insurance claims in multiple states during the same time frame using the same personal information</li> <li>• Self-employed individual overstates earnings in unemployment insurance claim</li> </ul>
	Parties providing goods or services	<ul style="list-style-type: none"> <li>• Vendor bills for nonexistent personal protective equipment (PPE)</li> <li>• Vendor substitutes noncompliant, substandard PPE and certifies it satisfied contract specifications</li> <li>• Vendor creates false appearance of competition and inflates prices □by disguising ownership in multiple fake companies submitting false bids or by disguising availability of services from actual competitors</li> <li>• Health care provider bills Medicare or Medicaid for COVID-related testing that was never administered</li> </ul>
	Government employees	<ul style="list-style-type: none"> <li>• Employee reports government property as stolen and takes it for personal use</li> <li>• Contracting officer receives kickbacks during contract award or administration</li> <li>• Employee inflates time and attendance records</li> </ul>
	Criminal organizations <sup>a</sup>	<ul style="list-style-type: none"> <li>• Criminals use synthetic identities (combining real and fictitious information) to apply for unemployment insurance</li> <li>• Hackers send emails to government employees to access government-held data</li> </ul>
Fraud against Private businesses and individuals	Criminal organizations	<p><b>Criminal organizations engaging in:</b></p> <ul style="list-style-type: none"> <li>• Online scams offering COVID-19 testing or treatment</li> <li>• Sale of counterfeit PPE</li> <li>• Identity theft to claim Economic Impact Payments to individuals</li> <li>• Robocalls or emails with payment instructions or malware to steal personal information</li> <li>• False representation as a government employee demanding payments to expedite receipt of government assistance</li> </ul>

Source: GAO analysis. | GAO-23-106567

Note: These fraud risks and variations on the schemes may also be present during nonemergency conditions. Some categories and examples may overlap.

<sup>a</sup>While fraud is by definition a criminal act, fraud by criminal organizations refers to nefarious activities associated with deliberate, organized, and sometimes large-scale schemes to liquidate credit accounts, launder money, or fraudulently obtain government benefits. Criminals use these large-scale schemes to fund organized crime, terrorism, and other illicit activities.

We expressed concern in March 2022 about the pace and extent to which agencies have implemented controls to prevent, detect, and respond to fraud in a manner consistent with leading practices since FRDAA was enacted in 2016.<sup>32</sup> Had agencies already been strategically managing their fraud risks, they would have been better positioned to identify and respond to the heightened risks that emerged during the COVID-19 pandemic. For example, we reported in September 2020 that implementing our 2019 recommendation that the Office of Head Start perform a fraud risk assessment for the Head Start program could help provide assurances that the \$750 million in funding received under the Coronavirus Aid, Relief, and Economic Security Act will be used by grantees as intended.<sup>33</sup> As discussed previously, that recommendation remains open.

Similarly, we expressed concerns that SBA's initial approach to managing fraud risks in PPP and the COVID-19 Economic Injury Disaster Loan program, as well as in its longstanding programs, has not been strategic. For example, when SBA developed its fraud risk assessments for the programs in October 2021, PPP had already stopped accepting new applications, and the COVID-19 Economic Injury Disaster Loan program would stop at the end of that year. As we mentioned in prior work, fraud risk assessments are most helpful in developing preventive fraud controls to avoid costly and inefficient "pay-and-chase" activities. For example, while the PPP fraud risk assessment can help SBA identify potential fraud as it continues to review the PPP loans for forgiveness, it could not be used to identify potential fraud during the application process.

From July 2015 through December 2022, we made 40 recommendations to federal agencies to implement changes to align with leading practices for managing fraud risks in emergency situations or programs.<sup>34</sup> This

---

<sup>32</sup>GAO, *Emergency Relief Funds: Significant Improvements Are Needed to Ensure Transparency and Accountability for COVID-19 and Beyond*, [GAO-22-105715](#) (Washington, D.C.: Mar. 17, 2022).

<sup>33</sup>Pub. L. No. 116-136, 134 Stat. 281, 558 (2020). GAO, *COVID-19: Federal Efforts Could be Strengthened by Timely and Concerted Actions*, [GAO-20-701](#) (Washington, D.C.: Sept. 21, 2020).

<sup>34</sup>This includes recommendations related to standing programs and activities to address emergency situations, such as Federal Emergency Management Agency programs and use of contracting and purchase cards in disaster response, as well as recommendations related to programs created or expanded in response to specific disasters or emergencies, such as the SBA's Paycheck Protection Program.

includes recommendations related to the themes discussed previously, such as designating dedicated antifraud entities for emergency programs, assessing fraud risks to emergency programs, and implementing antifraud strategies for emergency programs. Of the 40 recommendations, 29 remained open as of January 2023.<sup>35</sup>

For example, we have made several recommendations to DOL to improve fraud risk management in the UI programs, including recommendations to assess fraud risks and to design and implement an antifraud strategy to guide its actions.<sup>36</sup> DOL told us it has begun taking steps to implement these recommendations, such as developing a fraud risk management process and a fraud risk profile for the UI program. According to DOL, the UI antifraud strategy we recommended would then be based on the fraud risk profile, consistent with leading practices. As of February 2023, DOL planned to finalize its fraud risk profile, including an examination of existing fraud controls, by the end of calendar year 2023. Until DOL completes these efforts, it cannot ensure that it is effectively addressing fraud risks, some of which may persist in the regular UI program beyond the pandemic. Similarly, addressing open recommendations in this area can help ensure that federal managers safeguard public resources while providing needed relief during emergencies.

---

## Congressional Actions Can Improve Fraud Risk Management

Our prior work has identified actions that Congress can take to strengthen fraud risk management practices across the government. Specifically, in March 2022, we identified two matters for congressional consideration that can help improve federal agencies' fraud risk management efforts

---

<sup>35</sup>Of the 40 recommendations, 11 were closed as implemented, five were open but had been partially addressed, and 24 were open and had not been addressed. We follow up on recommendations we have made and update the status at least once per year. Experience has shown that it takes time for some recommendations to be implemented. Of the 40 recommendations, 10 were made on or after January 1, 2022, and all 10 remained open as of January 2023.

<sup>36</sup>[GAO-22-105051](#) and [GAO-23-105523](#).

across the five areas we identified.<sup>37</sup> These matters remained open as of January 2023.

**Reinstate the requirement for agencies to report on their antifraud controls and fraud risk management efforts in agency financial reports.** We previously reported that Congress’s ability to oversee agencies’ efforts to manage fraud risks is hindered by the lack of fraud-related reporting requirements. The Fraud Reduction and Data Analytics Act of 2015 and the Payment Integrity Information Act of 2019 required agencies to report on their antifraud controls and fraud risk management efforts in their annual financial reports. However, the requirement to report such information ended with the fiscal year 2020 annual financial report. Since then, there has been no similar requirement for agencies to report on their efforts to manage fraud risks.<sup>38</sup>

In March 2022, we recommended that Congress amend the Payment Integrity Information Act of 2019 to reinstate reporting requirements.<sup>39</sup> Requiring agencies to report annually on their antifraud controls and fraud risk management efforts will help facilitate congressional oversight and focus agency attention on strategic fraud risk management—both during normal operations and emergencies—and help align their efforts with leading practices. In turn, this may help ensure agencies put sound controls in place and build payment integrity controls upfront to avoid costly pay-and-chase activities.

**Establish a permanent analytics center of excellence to aid the oversight community in identifying improper payments and fraud.** Responsibilities for planning and implementing fraud risk management and detection activities start with agency management officials; however,

---

<sup>37</sup>In addition to the two actions to improve fraud risk management described here, we identified eight additional actions Congress can take to strengthen internal controls and financial management practices across the government and to increase transparency and accountability of emergency relief funding. See [GAO-22-105715](#). See app. I for a list of the 10 matters for congressional consideration. These matters were reiterated in a February 2023 testimony before the House Committee on Ways and Means and a February 2023 testimony before the House Committee on Oversight and Accountability. GAO, *Unemployment Insurance: DOL Needs to Address Substantial Pandemic UI Fraud and Reduce Persistent Risks*, [GAO-23-106586](#) (Washington, D.C.: Feb. 8, 2023) and *Emergency Relief Funds: Significant Improvements Are Needed to Address Fraud and Improper Payments*, [GAO-23-106556](#) (Washington, D.C.: Feb. 1, 2023).

<sup>38</sup>[GAO-22-105715](#).

<sup>39</sup>[GAO-22-105715](#).



the oversight community plays a critical role in identifying and investigating suspected fraud. The importance of this role in nonemergency periods is heightened during emergencies, such as the COVID-19 pandemic, as agencies work to implement large-scale relief efforts quickly.

At the outset of the pandemic, there was no permanent, government-wide analytical capability to help federal agencies identify fraud.<sup>40</sup> In March 2021, the American Rescue Plan Act of 2021 appropriated \$40 million to the Pandemic Response Accountability Committee (PRAC), which subsequently established the Pandemic Analytics Center of Excellence (PACE). The role of PACE is to help oversee the trillions of dollars in federal pandemic-related emergency spending. According to the PRAC, the goal of PACE is to build an “affordable, flexible, and scalable analytics platform” to support Offices of Inspectors General during their pandemic-related work, including beyond the organization’s sunset date in 2025.

However, PACE was not established until more than a year after agencies began distributing relief funds. The delayed establishment of the center resulted in the loss of valuable time for Offices of Inspectors General to help program officials understand fraud risks and identify potential fraud. In addition, the center is focused on pandemic programs only and is time-limited.

In March 2022, we recommended that Congress consider establishing a permanent analytics center of excellence to aid the oversight community

---

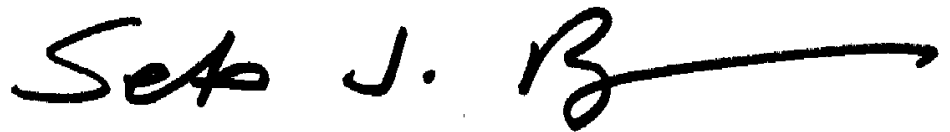
<sup>40</sup>Previously, this type of analytical capability had existed within the Recovery Operations Center, established by the Recovery Accountability and Transparency Board. The board, composed of agency inspectors general, was created by the American Recovery and Reinvestment Act of 2009 to oversee funds appropriated under the act. We previously recommended that Congress and the Department of the Treasury preserve the Recovery Operations Center’s functions, given its proven value in ensuring federal spending accountability. Congress and the Department of the Treasury did not implement our recommendations to make such a center permanent, and the Recovery Board and Recovery Operations Center’s activity terminated at the end of September 2015. See [GAO-22-105715](#) and GAO, *Federal Spending Accountability: Preserving Capabilities of Recovery Operations Center Could Help Sustain Oversight of Federal Expenditures*, [GAO-15-814](#) (Washington, D.C.: Sept. 14, 2015).

---

in identifying improper payments and fraud.<sup>41</sup> Without permanent government-wide analytics capabilities to assist the oversight community, agencies will have limited resources to apply to nonpandemic programs to ensure robust financial stewardship, as well as better prepare for applying fundamental financial and fraud risk management practices to future emergency funding.

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

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

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

Seto J. Bagdoyan  
Director, Forensic Audits and Investigative Service

---

<sup>41</sup>[GAO-22-105715](#). In a March 2023 fact sheet, the White House outlined a multipart proposal to address pandemic fraud. The proposal would establish a permanent antifraud data and analytics capability analogous to PACE for the inspector general community to be positioned to oversee future disaster relief and emergencies. The White House, "Fact Sheet: President Biden's Sweeping Pandemic Anti-Fraud Proposal: Going After Systemic Fraud, Taking on Identity Theft, Helping Victims" (Washington, D.C.: Mar. 2, 2023), accessed March 22, 2023, [https://www.whitehouse.gov/Pandemic\\_Anti-Fraud\\_Proposal](https://www.whitehouse.gov/Pandemic_Anti-Fraud_Proposal).

---

## Appendix I: Matters for Congressional Consideration

In a March 2022 testimony before the Senate Committee on Homeland Security and Governmental Affairs, we recommended the following 10 matters for congressional consideration:<sup>1</sup>

- Congress should pass legislation requiring the Office of Management and Budget (OMB) to provide guidance for agencies to develop plans for internal control that would then immediately be ready for use in, or adaptation for, future emergencies or crises and requiring agencies to report these internal control plans to OMB and Congress. (Matter for Congressional Consideration 1)
- Congress should amend the Payment Integrity Information Act of 2019 to designate all new federal programs making more than \$100 million in payments in any one fiscal year as “susceptible to significant improper payments” for their initial years of operation. (Matter for Congressional Consideration 2)
- Congress should amend the Payment Integrity Information Act of 2019 to reinstate the requirement that agencies report on their antifraud controls and fraud risk management efforts in their annual financial reports. (Matter for Congressional Consideration 3)
- Congress should establish a permanent analytics center of excellence to aid the oversight community in identifying improper payments and fraud. (Matter for Congressional Consideration 4)
- Congress should clarify that (1) chief financial officers (CFO) at CFO Act agencies have oversight responsibility for internal controls over financial reporting and key financial management information that includes spending data and improper payment information; and (2)

---

<sup>1</sup>GAO, *Emergency Relief Funds: Significant Improvements Are Needed to Ensure Transparency and Accountability for COVID-19 and Beyond*, [GAO-22-105715](#) (Washington, D.C.: Mar. 17, 2022). In addition, these matters were reiterated in a February 2023 testimony before the House Committee on Ways and Means and a February 2023 testimony before the House Committee on Oversight and Accountability. GAO, *Unemployment Insurance: DOL Needs to Address Substantial Pandemic UI Fraud and Reduce Persistent Risks*, [GAO-23-106586](#) (Washington, D.C.: Feb. 8, 2023) and *Emergency Relief Funds: Significant Improvements Are Needed to Address Fraud and Improper Payments*, [GAO-23-106556](#) (Washington, D.C.: Feb. 1, 2023).

executive agency internal control assessment, reporting, and audit requirements for key financial management information, discussed in an existing matter for congressional consideration in our August 2020 report,<sup>2</sup> include internal controls over spending data and improper payment information. (Matter for Congressional Consideration 5)

- Congress should require agency CFOs to (1) submit a statement in agencies' annual financial reports certifying the reliability of improper payments risk assessments and the validity of improper payment estimates, and describing the actions of the CFO to monitor the development and implementation of any corrective action plans; and (2) approve any methodology that is not designed to produce a statistically valid estimate. (Matter for Congressional Consideration 6)
- Congress should consider legislation to require improper payment information required to be reported under the Payment Integrity Information Act of 2019 to be included in agencies' annual financial reports. (Matter for Congressional Consideration 7)
- Congress should amend the DATA Act to extend the previous requirement for agency inspectors general to review the completeness, timeliness, quality, and accuracy of their respective agency data submissions on a periodic basis. (Matter for Congressional Consideration 8)
- Congress should amend the DATA Act to clarify the responsibilities and authorities of OMB and Department of the Treasury for ensuring the quality of data available on USAspending.gov. (Matter for Congressional Consideration 9)
- Congress should amend the Social Security Act to accelerate and make permanent the requirement for the Social Security Administration to share its full death data with the Department of the Treasury's Do Not Pay working system. (Matter for Congressional Consideration 10)

---

<sup>2</sup>GAO, *Federal Financial Management: Substantial Progress Made since Enactment of the 1990 CFO Act; Refinements Would Yield Added Benefits*, [GAO-20-566](#) (Washington, D.C.: Aug. 6, 2020).

---

## Appendix II: GAO Contact and Staff Acknowledgments

---

### GAO Contact

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

---

### Staff Acknowledgments

In addition to the contact named above, Jonathon Oldmixon (Assistant Director), Erin McLaughlin Villas (Analyst in Charge), Erin Buckley, and April Van Cleef made key contributions to this report. Other contributors include Irina Carnevale, David Dornisch, Paulissa Earl, Colin Fallon, Barbara Lewis, Flavio Martinez, Maria McMullen, and James Murphy.

---

---

## 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](mailto:ClowersA@gao.gov), (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

---

## Public Affairs

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

---

## Strategic Planning and External Liaison

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



**Please Print on Recycled Paper.**