United States Government Accountability Office

Testimony

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

FRAUD AND IMPROPER PAYMENTS

Data Quality and a Skilled Workforce Are Essential for Realizing Artificial Intelligence's Benefits
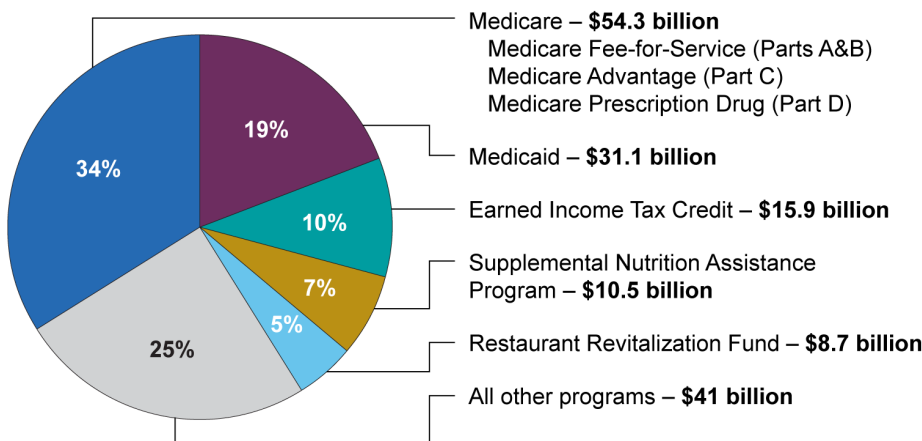
Statement of Dr. Sterling Thomas, Chief Scientist

A testimony before the Subcommittee on Government Operations, Committee on Oversight and Government Reform, House of Representatives. For more information, contact: Sterling Thomas at ThomasS2@gao.gov

What GAO Found

The federal government has tools and resources to help agencies combat fraud and improper payments. GAO has recommended improvements to the use of these tools and resources. For example, Congress should consider making permanent the Social Security Administration's requirement to share its full death data with the Do Not Pay system to help prevent fraud and improper payments. Further, GAO has identified leading practices for managing fraud risks at federal agencies and has made recommendations to agencies to implement these practices. For example, in 2024, GAO recommended that the Department of Defense revise its Fraud Risk Management Strategy to include data analytics as a method to address fraud. Further, by implementing GAO's recommendation, the Small Business Administration identified $4.7 billion in loans from the Paycheck Protection Program that were made before September 2020 and that went to ineligible recipients or were used for unauthorized purposes.

Programs Reporting the Largest Estimates of Improper Payments in Fiscal Year 2024

Medicare – **$54.3 billion**
  Medicare Fee-for-Service (Parts A&B)
  Medicare Advantage (Part C)
  Medicare Prescription Drug (Part D)

Medicaid – **$31.1 billion**

Earned Income Tax Credit – **$15.9 billion**

Supplemental Nutrition Assistance Program – **$10.5 billion**

Restaurant Revitalization Fund – **$8.7 billion**

All other programs – **$41 billion**

Source: GAO analysis of Office of Management and Budget PaymentAccuracy.gov data. | GAO-26-108850

Artificial intelligence (AI) and data analytics have the potential to enhance efforts to combat fraud and improper payments but also have challenges. For example, data analytics and AI could help agencies sift through large volumes of data. However, agencies need solid, reliable data and a human in the loop to ensure data reliability and appropriate application of the technology. GAO's *AI Accountability Framework for Federal Agencies and Other Entities* includes key practices for ensuring data used in AI systems are high quality, reliable, and appropriate for the intended purpose. Further, to improve the use of data analytics in identifying fraud and improper payments, GAO recommended in 2022 that Congress establish a permanent analytics center of excellence.

Additionally, the federal government requires an AI-ready workforce if AI is to help combat fraud and improper payments. However, GAO has identified mission-critical gaps in science, technology, engineering, and mathematics skills within the federal workforce and has reported on challenges agencies face in attracting and developing individuals with AI expertise.

Why GAO Did This Study

The distinct, yet interrelated, problems of fraud and improper payments are long-standing and pervasive. Fraud involves obtaining something of value through willful misrepresentation. Improper payments are payments that should not have been made or that were made in the wrong amount. GAO estimated that the federal government loses between $233 billion and $521 billion annually due to fraud, based on data for fiscal years 2018 through 2022. Since fiscal year 2003, cumulative improper payment estimates reported by executive branch agencies have totaled about $2.8 trillion. In fiscal year 2024, five programs accounted for most improper payments. These issues impact the integrity of federal programs and erode public trust.

The advancement of AI and other innovative technologies presents opportunities and challenges for combatting fraud and improper payments. This statement discusses (1) examples of tools and resources Congress and federal agencies can leverage to improve existing efforts to combat fraud and improper payments without the use of AI, (2) opportunities and challenges for using data analytics and AI to combat fraud and improper payments, and (3) challenges in developing an AI-ready federal workforce. This statement is based on a body of work GAO issued between 2015 and 2025 including GAO-25-108172, GAO-25-107508, GAO-21-519SP, and GAO-25-107653.

What GAO Recommends

GAO has made numerous recommendations to federal agencies and matters for Congressional consideration to address fraud and improper payments in federal programs.

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

Thank you for the opportunity to discuss artificial intelligence (AI) and data analytics, as well as other resources to combat fraud and improper payments in federal programs.

We have a long history of auditing fraud and improper payments, which we and executive branch agencies estimated to have collectively cost taxpayers trillions of dollars. In addition, these issues impact the integrity of federal programs and erode public trust.[1] We have issued numerous reports, guides, and recommendations about preventing fraud and improper payments. While innovative tools like AI could help prevent and detect fraud, as we reported in April 2025, these tools require careful implementation, high-quality data, and a workforce trained to use them.[2]

Fraud involves obtaining something of value through willful misrepresentation.[3] Improper payments are payments that should not have been made or that were made in the wrong amount, typically overpayments.[4] In 2024, we estimated that the federal government loses between $233 billion and $521 billion annually from fraud, using data for

---

[1]GAO, *Improper Payments: Agency Reporting of Payment Integrity Information,* GAO-25-107552 (Washington, D.C.: Jan. 23, 2025). GAO, *Improper Payments and Fraud: How They Are Related but Different,* GAO-24-106608 (Washington, D.C.: Dec. 7, 2023).
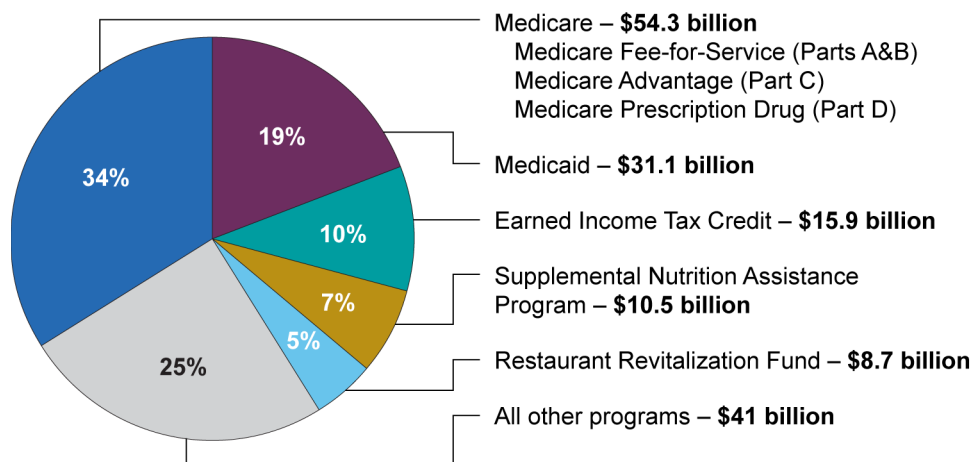
[2]GAO, *Fraud and Improper Payments*: *Data Quality and a Skilled Workforce Are Essential for Unlocking the Benefits of Artificial Intelligence*, GAO-25-108412 (Washington, D.C.: Apr. 9, 2025).

[3]Fraud can sometimes involve benefits that do not result in direct financial loss to the government (such as passport fraud). Improper payments, fraud, and fraud risk are related but distinct concepts. While unintentional error may cause improper payments, fraud involves obtaining something of value through willful misrepresentation. Whether an act is fraudulent is determined through the judicial or other adjudicative system. Fraud risk exists when individuals have an opportunity to engage in fraudulent activity.

[4]An improper payment is defined by law 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. 31 U.S.C. § 3351(4). Executive agency heads are required periodically to review the programs and activities they administer and make an estimation of each program or activity's improper payments. If in conducting such a review an agency head is unable to discern whether a payment was proper because of insufficient or lack of documentation, that payment must also be included in the improper payment estimate. 31 U.S.C. § 3352(a),(c).

fiscal years 2018 through 2022.[5] Since fiscal year 2003, cumulative improper payment estimates by executive branch agencies have totaled about $2.8 trillion, but are almost certainly greater, in part because agencies have not reported estimates for some programs as required.[6] For example, in 2025 we reported that agencies did not report required estimates for several risk-susceptible programs, including the Department of Health and Human Services' Temporary Assistance for Needy Families, the Department of Housing and Urban Development's Office of Public and Indian Housing's Tenant-Based Rental Assistance, and the Small Business Administration's Shuttered Venue Operators Grant programs.[7] Figure 1 shows that about 75 percent ($121 billion) of total government-wide estimated improper payments reported for fiscal year 2024 were concentrated in five program areas.[8]

Figure 1: Programs Reporting the Largest Estimates of Improper Payments in Fiscal Year 2024

Medicare – **$54.3 billion**
   Medicare Fee-for-Service (Parts A&B)
   Medicare Advantage (Part C)
   Medicare Prescription Drug (Part D)

Medicaid – **$31.1 billion**

Earned Income Tax Credit – **$15.9 billion**

Supplemental Nutrition Assistance Program – **$10.5 billion**

Restaurant Revitalization Fund – **$8.7 billion**

All other programs – **$41 billion**

Source: GAO analysis of Office of Management and Budget PaymentAccuracy.gov data. | GAO-26-108850

Note: Improper payment estimates displayed in the figure include both improper and unknown payments. Executive agency estimates of improper payments must treat as improper any payments

---

[5]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).

[6]GAO, *Improper Payments: Information on Agencies' Fiscal Year 2024 Estimates,* GAO-25-107753 (Washington, D.C.: Mar. 11, 2025).

[7]GAO, *Program Integrity: Agencies and Congress Can Take Actions to Better Manage Improper Payments and Fraud Risks,* GAO-25-108172 (Washington, D.C.: Mar. 11, 2025).

[8]GAO-25-107753.

Over the years, we have recommended ways that agencies can reduce fraud and improper payments, and ways that Congress can help. For example, from July 2015 through August 2023, we made 47 recommendations to federal agencies related to designing and implementing data-analytics activities to prevent and detect fraud, such as using data matching to verify self-reported information. One of these recommendations—to the Small Business Administration—prompted the agency to screen all Paycheck Protection Program loans made before September 2020 with a rules-based data analytic tool—just looking for indicators, not using AI. In doing so, the Small Business Administration identified $4.7 billion in loans that went to ineligible recipients or were used for unauthorized purposes.[9]

AI presents both opportunities and challenges for combatting fraud and improper payments in the federal government. My statement today discusses: (1) examples of tools and resources Congress and federal agencies can leverage to improve existing efforts to combat fraud and improper payments without the use of AI, (2) opportunities and challenges in using data analytics and AI to combat fraud and improper payments, and (3) challenges in developing an AI-ready federal workforce to deploy innovative tools to combat fraud and improper payments.

This statement is based on a body of work from July 2015 to December 2025 addressing improper payments, fraud, and artificial intelligence. More detailed information on the scope and methodology of our prior work can be found within the specific reports on which this statement is based. These reports are listed in the related products page at the end of this statement. In addition, appendix I includes a list of our selected completed and ongoing work on AI.

We conducted the work on which this statement is based in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objectives.

---

[9]GAO, *COVID Relief: Fraud Schemes and Indicators in SBA Pandemic Programs*, GAO-23-105331 (Washington, D.C.: May 18, 2023).

Congress and Federal Agencies Could Strengthen Use of Existing Tools and Resources to Combat Fraud and Improper Payments

While eliminating all fraud is not a realistic goal, the federal government has tools and resources in place to help agencies prevent fraudulent and improper payments before funds are distributed and to combat fraud and improper payments after they have occurred. Examples of these tools and resources include the Department of the Treasury's Do Not Pay system, GAO's A Framework for Managing Fraud Risks in Federal Programs (Fraud Risk Framework), and GAO's Antifraud Resource. Congressional and agency action on our matters and recommendations in these areas could improve these efforts.

Department of the Treasury's Do Not Pay system. One key resource for preventing fraud and improper payments is the Department of the Treasury's Do Not Pay system, which consolidates data on entities ineligible to receive payments. Do Not Pay is a data-matching service for agencies to use in preventing payments to ineligible individuals, such as those who are deceased. The Social Security Administration currently shares its full death data with Do Not Pay, but its requirement to do so expires in December 2026. In March 2022, we raised a matter for Congress to consider making this requirement permanent, which would enhance agencies' ability to verify identities and identify payments to the deceased.[10]

The sharing of these data has already yielded positive financial results. According to Treasury, Do Not Pay's first year of temporary access to the Social Security Administration's full death data resulted in total net benefits of $109 million, with benefits of at least $330 million projected over the 3-year approved access period outlined in legislation (December 2023 through December 2026).[11]

---

[10]We recommended that Congress amend the Social Security Act to accelerate and make permanent the requirement for Social Security Administration to share its full death data with the Treasury's Do Not Pay system. 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). Bills *Ending Improper Payments to Deceased People Act*, H.R. 2716, 119th Cong. (2025); S. 269, 119th Cong. (2025), and *PIIA Reform Act*, H.R.1533, 119th Cong. (2026), address this.

[11]GAO, *Confronting High Risks and Fiscal Challenges Is Crucial to a More Effective and Sustainable Government,* GAO-26-108824 (Washington, D.C.: Dec. 16, 2025).

GAO-26-108850

Our prior work has also demonstrated how data analytics can be used to confirm the validity of a Social Security number and whether a beneficiary is alive. Recently, we reported on preliminary results that showed how analytics involving the Social Security Administration's death data can identify potential health insurance fraud (see sidebar).

GAO's Fraud Risk Framework. For fraud risk management, preventive activities generally offer the most cost-efficient use of resources, since they allow the federal government to avoid a costly and inefficient "pay-and-chase" approach. Managers of federal programs maintain the primary responsibility for managing fraud risk. Since 2016, agencies have been required to adhere to leading practices in our Fraud Risk Framework to effectively design, implement, and operate an internal control system that addresses fraud risks.[12] One leading practice in the Fraud Risk Framework involves designing and implementing data analytic controls to prevent and detect fraud (see fig. 2).

Figure 2: Overview of GAO's Fraud Risk Framework

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

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

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

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

Source: GAO. | GAO-26-108850

---

[12]GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015). OMB's Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, directs executive agencies to adhere to the Fraud Risk Framework's leading practices as part of their efforts to effectively design, implement, and operate an internal control system that addresses fraud risks.

We have made several recommendations to federal agencies from our body of work on fraud risk management. More specifically, we have highlighted areas in which federal agencies need to take additional actions to help ensure the agencies are effectively managing fraud risks consistent with leading practices, such as using data analytics to better manage fraud risk. For example, in February 2024 we recommended that the Department of Defense revise its Fraud Risk Management Strategy to establish data analytics as a method for preventing, detecting, and responding to fraud.[13] Contrary to leading practices, we found that the department's strategy did not establish data analytics as a method for fraud risk management. Data analytics can include a variety of techniques, such as data matching to determine eligibility to receive federal contracts. For example, we reported that if an entity reports that it is a small business to receive federal contracts, the Department of Defense can use third-party data sources to verify that the entity qualifies as a small business. The Department of Defense did not agree with our recommendation but issued its revised Fraud Risk Management Strategy in June 2025. While the revised strategy requires components to develop action plans for implementing data-analytics activities in certain areas by a certain time, it does not provide specificity regarding the method for using data-analytics activities in preventing, detecting, and responding to fraud, nor does it discuss what or how data analytics are to be used.

Similarly, in August 2023, we recommended that the Department of Housing and Urban Development Assistant Secretary for Community Planning and Development identify ways to collect and combine contractor and subcontractor data across grantees and subrecipients to facilitate risk analyses, among other things.[14] We found that incomplete and inconsistent data impacted grantees' and subrecipients' ability to make eligibility determinations and limited the department's ability to oversee grantees' processes for managing fraud risk. The department is currently developing a Fraud Risk Playbook, which the department told us will inform the development of guidance to implement this recommendation. The Fraud Risk Playbook, along with tools and templates, is intended to help program offices design and implement fraud risk management programs, including fraud risk assessments.

---

[13]GAO, *DOD Fraud Risk Management: Enhanced Data Analytics Can Help Manage Fraud Risks,* GAO-24-105358 (Washington, D.C.: Feb. 27, 2024).

[14]GAO, *Disaster Recovery: HUD Should Develop Data Collection Guidance to Support Analysis of Block Grant Fraud Risks,* GAO-23-104382 (Washington, D.C.; Aug. 17, 2023).

Antifraud Resource. To further help agencies build prevention-focused antifraud efforts, in 2022, we developed a web-based Antifraud Resource, which provides interactive tools and resources for understanding and combatting fraud, such as fraud scheme examples (see fig. 3).[15]

Figure 3: Five Categories of Antifraud Resources

Fraud scheme examples: Fraud cases that involved federal programs and operations.

Fraud awareness resources: Educational resources that have been developed for federal employees and the public to understand the threat of fraud.

Fraud prevention and detection guidance: Specific actions that can be used to prevent and detect fraud.

Fraud risk-management principles: Core principles for effectively managing fraud risks. These materials are the same for all programs and operations.

GAO Reports: GAO reports related to fraud risks in federal programs and operations.

Source: GAO Antifraud Resource adapted from https://antifraud.gaoinnovations.gov/resources (data and icons). | GAO-26-108850

---

[15]GAO, "The GAO Antifraud Resource" (Washington, D.C.: Jan. 10, 2022), https://gaoinnovations.gov/antifraud_resource/.

Opportunities and Challenges in Using Data Analytics and AI to Combat Fraud and Improper Payments

Routine and Innovative Data Analytic Tools Can Help Reduce Fraud and Improper Payments

As we have previously reported, there are a range of data analytic tools—from basic to advanced—that can help prevent and detect fraudulent activity and improper payments in federal programs (see fig. 4). The advanced tools can be particularly helpful in identifying scale, connections, and outliers.

Figure 4: Examples of Data Analytic Tools for Preventing and Detecting Fraud in Federal Programs

Basic		Prevent	Detect
Edit checks — Compares data entries to requirements, and automatically denies entries that do not meet requirements or flags them for further review.		✓	
Data matching — Compares information from one source with information from another source, such as government or third-party databases, to identify any inconsistencies. Can be used to verify key information, including self-reported information and information necessary to determine eligibility.		✓	✓
Data mining — Analyzes data for connections that have not been previously discovered. Can be used to identify suspicious activity or transactions, including anomalies and other outliers, indicating potentially fraudulent activity that warrants further investigation.			✓
Predictive analytics — Includes a variety of automated systems and tools that can be used to identify particular types of behavior before transactions are completed. Can be used to detect patterns of behavior that individually may not be suspicious, but when conducted together, can indicate fraudulent activity.		✓	
Network analytics — Analyzes data to map relationships between people, entities, or other data points to uncover potentially unknown relationships. Also identifies "key players," which are influential or central individuals, entities, or other data points in a network.		✓	✓

Advanced

Legend:
✓ Can be used to prevent or detect fraud

Prevent. Stopping fraud from occurring before processing or approval. For example, flagging an application for follow-up before being approved.

Detect. Identifying potential fraud after a transaction was processed, such as after an application was approved and payment made.

Sources: GAO analysis of the GAO Fraud Risk Framework, the Chief Financial Officers Council and Bureau of the Fiscal Service Antifraud Playbook, and previous GAO reports (data); Icons-Studio/stock.adobe.com (icons). | GAO-26-108850

Note: More information about how data analytic tools can be used to prevent and detect fraud is available in GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015); and Chief Financial Officers Council and the Bureau of the Fiscal Service, *Program Integrity: The Antifraud Playbook* (Oct. 17, 2018).

Using AI to Reduce Fraud and Improper Payments Requires High-Quality Data and Responsible Use
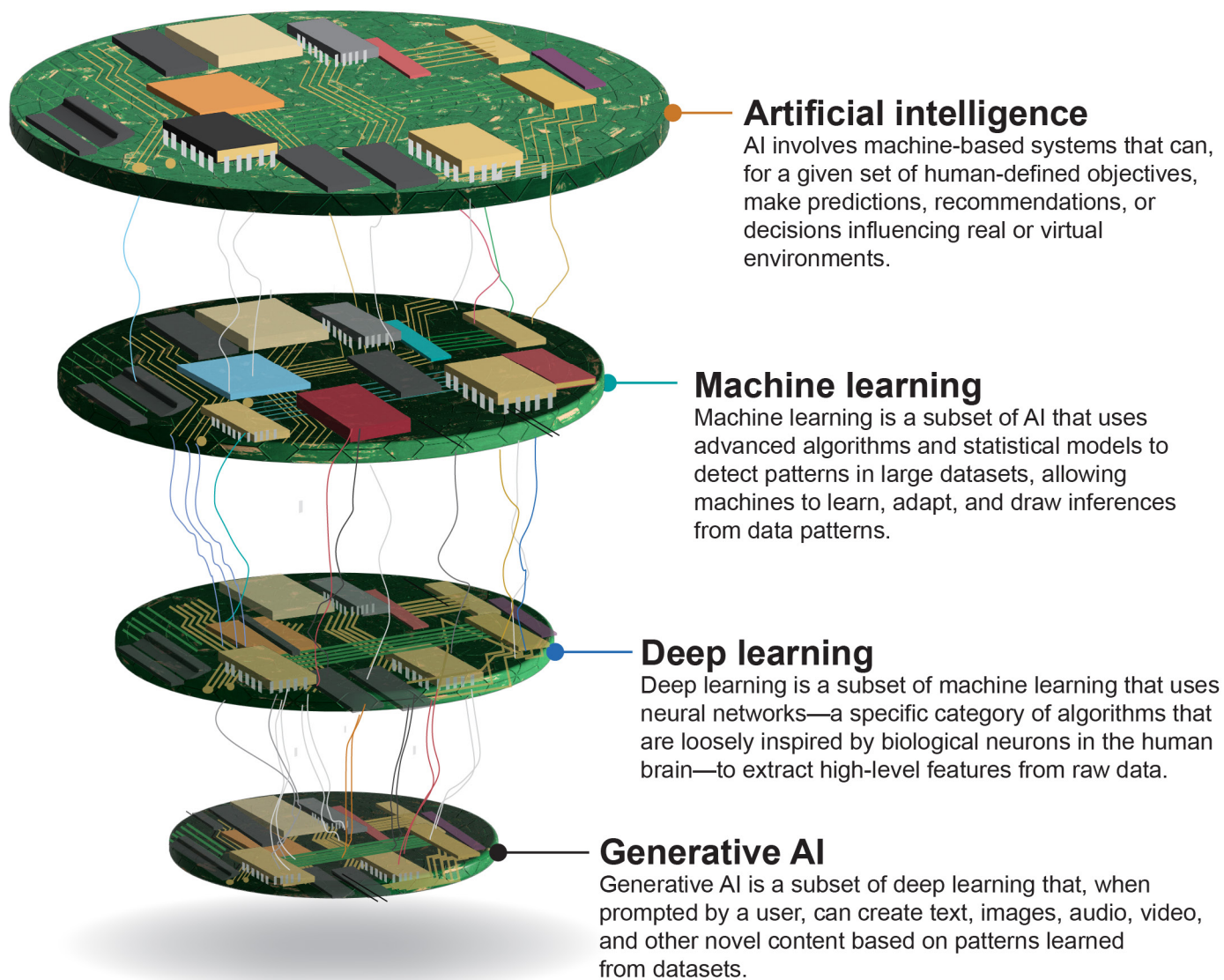
As we have previously reported, new innovations like AI-enabled tools can perform some of the tasks required to combat fraud and improper payments in the federal government.[16] However, these tools require sufficient high-quality data, an understanding of risks, and staff with knowledge of how to use AI. Introducing insufficient, unrelated, or bad data will make an AI model less reliable, and maintaining a "human in the loop" is vital to ensuring oversight of the data and processes. [17] An AI-enabled tool that produces errors will also erode trust in AI's ability to detect fraud—and therefore, the government's as well.

AI, in general, refers to computer systems that can solve problems and perform tasks that have traditionally required human intelligence. There are several subcategories of AI such as machine learning and generative AI (see fig. 5). Machine learning underpins many of the recent improvements in AI and could be used to detect fraud and improper payments. Generative AI refers to tools that can create text, images, audio, and other content using patterns learned from datasets.

---

[16]GAO-25-108412.

[17]Human in the loop refers to an approach to human oversight of the AI system "with the human retaining full control and the AI only providing recommendations or input." A human reviews the output of the AI system and makes the final decision. Info-communications Media Development Authority and Personal Data Protection Commission, *Model Artificial Intelligence Governance Framework, Second Edition* (Singapore, Jan. 2020).

Figure 5: Generative Artificial Intelligence (AI) and Machine Learning in Relation to Other Types of AI

Artificial intelligence
AI involves machine-based systems that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.

Machine learning
Machine learning is a subset of AI that uses advanced algorithms and statistical models to detect patterns in large datasets, allowing machines to learn, adapt, and draw inferences from data patterns.

Deep learning
Deep learning is a subset of machine learning that uses neural networks—a specific category of algorithms that are loosely inspired by biological neurons in the human brain—to extract high-level features from raw data.

Generative AI
Generative AI is a subset of deep learning that, when prompted by a user, can create text, images, audio, video, and other novel content based on patterns learned from datasets.

Source: GAO analysis and illustration. | GAO-26-108850

Many federal agencies are using or planning to use machine learning, including applications to support detecting fraud and improper payments. For example, in November 2020, the Small Business Administration worked with its loan-review contractor to put in place a machine-learning tool to rate borrower-forgiveness applications according to fraud risk and to clear batches of loans flagged during automated screening that were considered low risk.[18]

Machine-learning models work by identifying statistical relationships between inputs and outputs from a training dataset. Training is the process of feeding training data through the algorithm until it identifies statistical relationships of interest. Such models might improve detection or prevention of fraud and improper payments by revealing anomalous patterns, behaviors, and relationships with a speed and scale that was not possible before.[19]

Machine-learning models can also pose risks. For example, they may fail to detect improper payments (false negatives) and they can erroneously identify legitimate payments as improper (false positives). False positives, in turn, can delay or deny payments to rightful recipients.

Critical to mitigating such risk is training the model on high-quality data. A common phrase among AI developers is "garbage in, garbage out," meaning that poor data will give poor results. For detecting fraud and improper payments, incorrect labeling in historical data in the model could lead to false results. If these become too numerous, agencies could spend more time identifying AI's mistakes than they would save compared with traditional detection methods. The training data could also be adulterated by "data poisoning," a process by which someone changes the data, which changes the behavior of a system.

To help address these potential challenges, we have reported that agencies need solid, reliable "ground truth" data and a human in the loop to ensure data reliability and appropriate application of the technology.[20] AI does not replace the professional judgment of experienced staff in

---

[18]GAO, *COVID-19 Relief: Improved Controls Needed for Referring Likely Fraud in SBA's Pandemic Loan Programs*, GAO-25-107267 (Washington, D.C.: Mar. 24, 2025).

[19]Taka Ariga, "Artificial Intelligence Creates New Opportunities to Combat Fraud," *International Journal of Government Auditing*, Summer 2020 Edition.

[20]GAO, *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*, GAO-21-519SP (Washington, D.C.: June 30, 2021).

detecting potentially fraudulent activities. While AI can sift through large volumes of data, human intelligence is still an essential element for choosing appropriate actions and technology tools.

In addition, federal government data for identifying possible fraud and improper payments can vary in quality, reliability, and availability. For example, in our 2023 survey on fraud risk management, federal agencies told us that access to data to look for fraud indicators was a challenge.[21] We have also previously reported on challenges with federal agency data used to identify possible fraud and improper payments at the Federal Aviation Administration and Small Business Administration, among others. [22] We have made recommendations to federal agencies to help improve their use of data, such as recommending agencies implement data mining and other analytic practices to ensure data are sufficient for fraud risk analysis.

Moreover, to improve the use of data analytics in identifying fraud and improper payments, in 2022 we recommended that Congress establish a permanent analytics center of excellence.[23] We noted that such a center could include an AI-based tool to help in identifying fraud and improper payments. In July 2025, Congress extended the sunset date of the Pandemic Response Accountability Committee to September 30, 2034, and expanded its jurisdiction. The committee includes the Pandemic Analytics Center of Excellence; however, the committee and its analytics center are not permanent or government-wide.

In addition, while private-sector enterprises are exploring using generative AI to prevent and detect fraudulent activity, we have found that generative AI has challenges securing classified and sensitive data that private-sector users may not face.[24] In July 2025 we reported that, according to Department of Defense officials, generative AI models could aggregate

---

[21]GAO, *Fraud Risk Management: Agencies Should Continue Efforts to Implement Leading Practices*, GAO-24-106565 (Washington, D.C.: Nov. 01, 2023).

[22]GAO, *Aviation: FAA Needs to Better Prevent, Detect, and Respond to Fraud and Abuse Risks in Aircraft Registration,* GAO-20-164 (Washington, D.C.: March 25, 2020) and GAO, *Small Business Research Programs: Opportunities Exist for SBA and Agencies to Reduce Vulnerabilities to Fraud, Waste, and Abuse*, GAO-24-105470 (Washington, D.C.: Sept. 9, 2024).
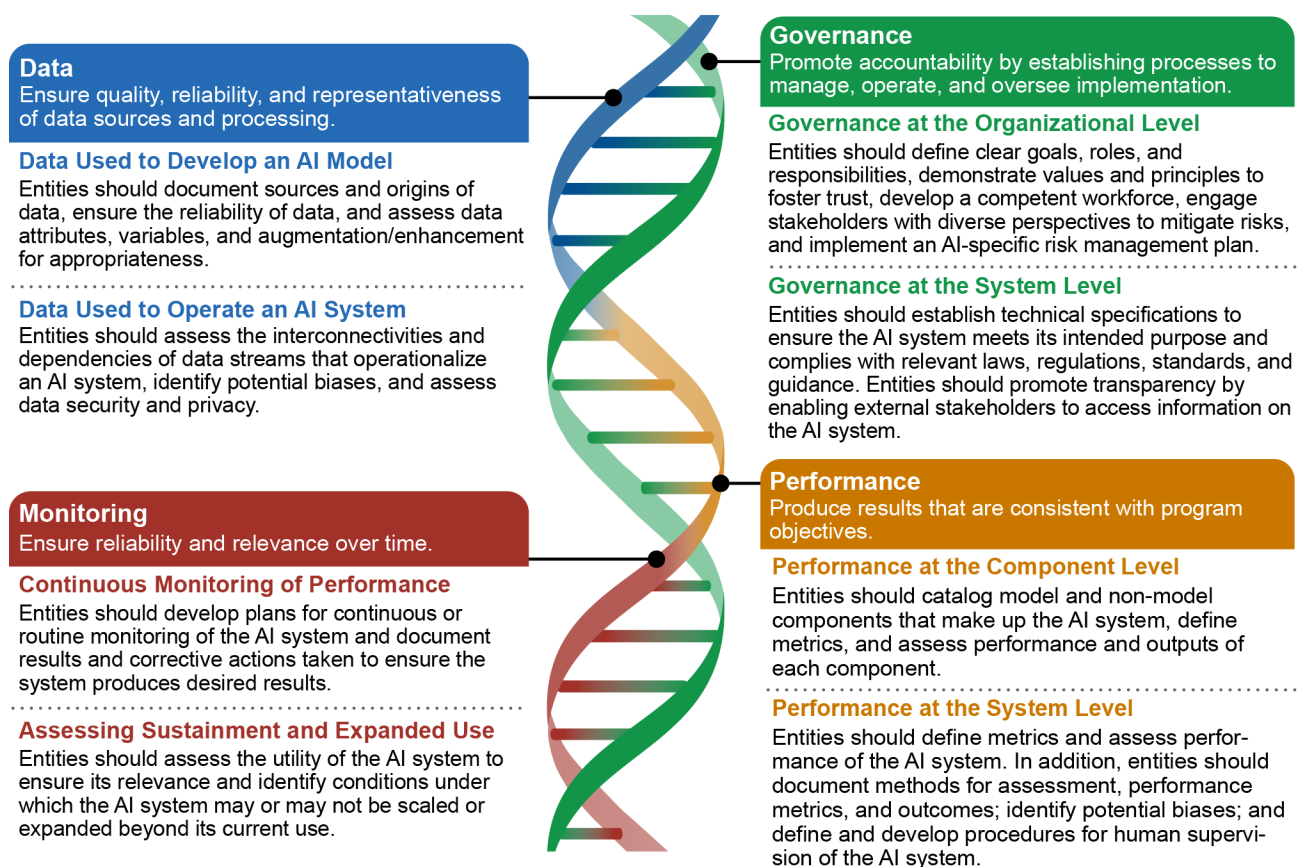
[23]GAO-22-105715.

[24]GAO, *Artificial Intelligence: Generative AI Use and Management at Federal Agencies,* GAO-25-107653 (Washington, D.C.: July 29, 2025).

various unclassified information contained in the model's training data and unintentionally output classified information. We reported that federal agencies are required to ensure that personal data, controlled unclassified information, and classified data used in the training and deploying of generative AI models are kept secure and compliant with federal requirements. Officials at five agencies told us that strict data security requirements may prevent them from performing generative AI research in certain agency mission areas.

In recognition of these opportunities and risks of AI, in 2021, we published our AI Accountability Framework for federal agencies and other entities (see fig. 6).[25] We identified 31 key practices to help ensure accountability and responsible AI use by federal agencies and other entities, which could include use for combatting fraud and improper payments. These key practices include ensuring systems are documented, designed, and governed appropriately for their intended uses; ensuring data quality; and recruiting and retaining personnel with the necessary multidisciplinary skills and experiences.

---

[25]GAO-21-519SP.

Figure 6: GAO Artificial Intelligence (AI) Accountability Framework

Data
Ensure quality, reliability, and representativeness of data sources and processing.

Data Used to Develop an AI Model
Entities should document sources and origins of data, ensure the reliability of data, and assess data attributes, variables, and augmentation/enhancement for appropriateness.

Data Used to Operate an AI System
Entities should assess the interconnectivities and dependencies of data streams that operationalize an AI system, identify potential biases, and assess data security and privacy.

Monitoring
Ensure reliability and relevance over time.

Continuous Monitoring of Performance
Entities should develop plans for continuous or routine monitoring of the AI system and document results and corrective actions taken to ensure the system produces desired results.

Assessing Sustainment and Expanded Use
Entities should assess the utility of the AI system to ensure its relevance and identify conditions under which the AI system may or may not be scaled or expanded beyond its current use.

Governance
Promote accountability by establishing processes to manage, operate, and oversee implementation.

Governance at the Organizational Level
Entities should define clear goals, roles, and responsibilities, demonstrate values and principles to foster trust, develop a competent workforce, engage stakeholders with diverse perspectives to mitigate risks, and implement an AI-specific risk management plan.

Governance at the System Level
Entities should establish technical specifications to ensure the AI system meets its intended purpose and complies with relevant laws, regulations, standards, and guidance. Entities should promote transparency by enabling external stakeholders to access information on the AI system.

Performance
Produce results that are consistent with program objectives.

Performance at the Component Level
Entities should catalog model and non-model components that make up the AI system, define metrics, and assess performance and outputs of each component.

Performance at the System Level
Entities should define metrics and assess performance of the AI system. In addition, entities should document methods for assessment, performance metrics, and outcomes; identify potential biases; and define and develop procedures for human supervision of the AI system.

Source: GAO. | GAO-26-108850

Challenges in Developing an AI-Ready Federal Workforce to Combat Fraud and Improper Payments

An AI-ready workforce is important for the federal government in using AI to combat fraud and improper payments in federal programs. For decades, however, we have identified mission-critical gaps in science, technology, engineering, and mathematics skills and expertise within the federal workforce. In December 2023 and July 2025, we reported on challenges in attracting and developing individuals with AI expertise in federal agencies, including Departments of Commerce, Defense, State, and Veterans Affairs; the National Aeronautics and Space Administration; and the Office of Personnel Management. [26] These challenges could also apply to creating a workforce that can use AI to prevent and detect fraud.

One option Congress has considered is to establish a new digital services academy—like the military academies—to train future workers.[27] In 2021, we convened technology leaders from government, academia, and nonprofits to discuss such an academy and related issues. They raised several comments including that:

- Current federal digital staff compensation is not competitive.
- Many digital staff may not be willing to endure the lengthy federal hiring process.
- An academy might best focus on master's degrees because agencies need staff with advanced skills.

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

GAO Contact and Staff Acknowledgements

Sterling Thomas, ThomasS2@gao.gov

Rebecca Shea, SheaR@gao.gov

In addition to the contacts named above, Joseph Cook (Assistant Director), Heather J. Dunahoo (Assistant Director), Claire McLellan (Analyst in Charge), Lisa Gardner, Allison Henn, Riley Wilson, Anika McMillon, and Victoria Aysola made key contributions to this testimony. Other staff who contributed to this testimony include Daniel Flavin, Rachael Johnson, and Jessica Steele.

---

[26]GAO, *Artificial Intelligence*: *Actions Needed to Improve DOD's Workforce Management*, GAO-24-105645 (Washington, D.C.: Dec. 14, 2023); GAO-25-107653.

[27]GAO, *Digital Services: Considerations for a Federal Academy to Develop a Pipeline of Digital Staff,* GAO-22-105388 (Washington, D.C.: Nov. 19, 2021).

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

WINTER 2026

A SELECTION OF AI WORK FROM GAO

GAO provides fact-based, nonpartisan answers to your questions about artificial intelligence.

These two pages include a selection of our recently published and ongoing work on AI and related topics.

Cybersecurity & Privacy

- **AI**: DHS Needs to Improve Risk Assessment Guidance for Critical Infrastructure Sectors
  GAO-25-107435 (2024)
- **Biometric Identification Technologies**: Considerations to Address Information Gaps and Other Stakeholder Concerns
  GAO-24-106293 (2024)
- **AI**: Fully Implementing Key Practices Could Help DHS Ensure Responsible Use for Cybersecurity
  GAO-24-106246 (2024)

  ONGOING
  - Privacy Risks Associated with AI
  - AI Cybersecurity Technology Assessment
  - AI Export Controls
  - Semiconductor Export Enforcement

AI Opportunities & Challenges

- **Malicious Use of Generative AI** (Science & Tech Spotlight)
  GAO-26-108695 (2025)
- **Veterans Affairs**: Key AI Practices Could Help Address Challenges
  GAO-25-108739 (2025)
- **AI Agents** (Science & Tech Spotlight)
  GAO-25-108519 (2025)
- **AI**: Federal Efforts Guided by Requirements and Advisory Groups
  GAO-25-107933 (2025)
- **Wildfire Management**: Technologies for Forecasting, Detection, Mitigation, and Response
  GAO-25-108589 (2025)
- **Smart Cities**: Technologies and Policy Options to Enhance Services and Transparency
  GAO-25-107019 (2025)
- **Wildfire Detection Technologies** (Science & Tech Spotlight)
  GAO-25-108161 (2025)

  ONGOING
  - Science and Technology Trends (2026)
  - Malicious Use of AI
  - AI Tools for Fraud Prevention and Detection

Federal Research & Management

- **AI**: Generative AI Use and Management at Federal Agencies
  GAO-25-107653 (2025)
- **AI**: Agencies Are Implementing Management and Personnel Requirements
  GAO-24-107332 (2024)
- **Immersive Technologies:** Most Civilian Agencies Are Using or Plan to Use Augmented Reality, Virtual Reality, and More
  GAO-24-106665 (2024)
- **Federal Regulation:** Selected Emerging Technologies Highlight the Need for Legislative Analysis and Enhanced Coordination
  GAO-24-106122 (2024)
- **AI**: GAO's Work to Leverage Technology and Ensure Responsible Use
  GAO-24-107237 (2024)
- **AI**: Agencies Have Begun Implementation but Need to Complete Key Requirements
  GAO-24-105980 (2023)
- **AI**: DOD Needs Department-Wide Guidance to Inform Acquisitions
  GAO-23-105850 (2023)

  ONGOING
  - SBA Use of AI Tools
  - Framework for Assessing AI Competitiveness
  - Assessing National AI Competitiveness

Finance

- **Property Technology for Homebuying:** Products Present Benefits and Risks Amid Evolving Federal Oversight
  GAO-25-107201 (2025)
- **Rental Housing:** Use and Federal Oversight of Property Technology
  GAO-25-107196 (2025)
- **AI:** Use and Oversight in Financial Services
  GAO-25-107197 (2025)
- **Fraud and Improper Payments:** Data Quality and a Skilled Workforce Are Essential for Unlocking the Benefits of AI
  GAO-25-108412 (2025)

  ONGOING
  - IRS Use of AI
  - Disaster Assistance Scams
  - AI in Insurance

Source: Bluehousestudio/stock.adobe.com (AI text image); GAO (analysis, icons, and graphical elements). | GAO-26-108850

Federal Workforce

- **Digital Surveillance**: Potential Effects on Workers and Roles of Federal Agencies
  GAO-25-107126 (2025)
- **Workplace Safety and Health**: OSHA Should Take Steps to Better Identify and Address Ergonomic Hazards at Warehouses and Delivery Companies
  GAO-24-106413 (2024)
- **AI**: Actions Needed to Improve DOD's Workforce Management
  GAO-24-105645 (2023)
- **FAA Workforce**: Better Assessing Employees' Skill Gaps Could Help FAA Prepare for Changes in Technology
  GAO-21-310 (2021)
- **Automated Technologies**: DOT Should Take Steps to Ensure Its Workforce Has Skills Needed to Oversee Safety
  GAO-21-197 (2020)
- **Federal Workforce**: Key Talent Management Strategies for Agencies to Better Meet Their Missions
  GAO-19-181 (2019)
- **Workforce Automation**: Better Data Needed to Assess and Plan for Effects of Advanced Technologies on Jobs
  GAO-19-257 (2019)

ONGOING
- Federal AI Acquisitions

Defense & Law Enforcement

- **Law Enforcement**: DHS Could Better Address Bias Risk and Enhance Privacy Protections for Technologies Used in Public
  GAO-25-107302 (2024)
- **Coast Guard**: Autonomous Ships and Efforts to Regulate Them
  GAO-24-107059 (2024)
- **Information Environment**: Opportunities and Threats to DOD's National Security Mission
  GAO-22-104714 (2022)
- **AI**: Status of Developing and Acquiring Capabilities for Weapon Systems
  GAO-22-104765 (2022)

ONGOING
- DOD Responsible AI Oversight and Implementation
- Agency Skills to Detect Foreign Information Operations
- Collaborative Combat Aircraft (CCA)

Health Care

- **Generative AI in Health Care** (Science & Tech Spotlight)
  GAO-24-107634 (2024)
- **National Institute on Aging**: Leading Project Management Practices Are Important for Large-Scale Health Data Efforts
  GAO-24-106886 (2024)
- **AI in Health Care**: Benefits and Challenges of Machine Learning Technologies for Medical Diagnostics
  GAO-22-104629 (2022)
- **Vaccine Development**: Capabilities and Challenges for Addressing Infectious Diseases
  GAO-22-104371 (2021)

ONGOING
- Medical Wearables in Clinical Decision Making

GAO's framework for AI accountability allows it to examine whether federal agencies are using models appropriately.

Governance
Promote accountability by establishing processes to manage, operate, and oversee implementation

Data
Ensure quality, reliability, and representativeness of data sources and processing

Performance
Produce results that are consistent with program objectives

Monitoring
Ensure reliability and relevance over time

GAO is a trusted source for fact-based, nonpartisan information about government agencies and programs. Our experts are well-positioned to help elected officials and their staff prioritize policy matters and develop oversight agendas.

GAO
U.S. GOVERNMENT ACCOUNTABILITY OFFICE
Ver. 2.1 | Updated: 1.8.2026

Read how GAO supports Congress
https://www.gao.gov/for-congress

Have a question for your committee's Congressional Relations Advisors?
https://www.gao.gov/for-congress/find-your-advisor

Source: Bluehousestudio/stock.adobe.com (AI text image); GAO (analysis, icons, and graphical elements). | GAO-26-108850

Related GAO Products

Confronting High Risks and Fiscal Challenges Is Crucial to a More Effective and Sustainable Government. GAO-26-108824. Washington, D.C.: December 16, 2025.

Artificial Intelligence: Generative AI Use and Management at Federal Agencies. GAO-25-107653. Washington, D.C.: July 29, 2025.

Fraud Risk in Federal Programs: Continuing Threat from Organized Groups Since COVID-19. GAO-25-107508. Washington, D.C.: July 10, 2025.

Fraud and Improper Payments: Data Quality and a Skilled Workforce Are Essential for Unlocking the Benefits of Artificial Intelligence. GAO-25-108412. Washington, D.C.: April 9, 2025.

COVID-19 Relief: Improved Controls Needed for Referring Likely Fraud in SBA's Pandemic Loan Programs. GAO-25-107267. Washington, D.C.: March 24, 2025.

Program Integrity: Agencies and Congress Can Take Actions to Better Manage Improper Payments and Fraud Risks. GAO-25-108172. Washington, D.C.: March 11, 2025.

Improper Payments: Agency Reporting of Payment Integrity Information. GAO-25-107552. Washington, D.C.: January 23, 2025.

Small Business Research Programs: Opportunities Exist for SBA and Agencies to Reduce Vulnerabilities to Fraud, Waste, and Abuse. GAO-24-105470. Washington, D.C.: September 9, 2024.

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.: April 16, 2024.

Artificial Intelligence: Actions Needed to Improve DOD's Workforce Management. GAO-24-105645. Washington, D.C.: December 14, 2023.

Improper Payments and Fraud: How They Are Related but Different. GAO-24-106608. Washington, D.C.: December 7, 2023.

Fraud Risk Management: Agencies Should Continue Efforts to Implement Leading Practices. GAO-24-106565. Washington, D.C.: November 01, 2023.

Disaster Recovery: HUD Should Develop Data Collection Guidance to Support Analysis of Block Grant Fraud Risks. GAO-23-104382. Washington, D.C.: August 17, 2023.

COVID Relief: Fraud Schemes and Indicators in SBA Pandemic Programs, GAO-23-105331. Washington, D.C.: May 18, 2023.

Digital Services: Considerations for a Federal Academy to Develop a Pipeline of Digital Staff. GAO-22-105388. Washington, D.C.: November 19, 2021.

Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities. GAO-21-519SP. Washington, D.C.: June 30, 2021.

Aviation: FAA Needs to Better Prevent, Detect, and Respond to Fraud and Abuse Risks in Aircraft Registration. GAO-20-164. Washington, D.C.: March 25, 2020.

A Framework for Managing Fraud Risks in Federal Programs. GAO-15-593SP. Washington, D.C.: July 28, 2015.