ARTIFICIAL INTELLIGENCE

OMB Action Needed to Address Privacy-Related Gaps in Federal Guidance

Report to Congressional Addressees

March 2026
GAO-26-107681
United States Government Accountability Office

Accessible Version

GAO Highlights

ARTIFICIAL INTELLIGENCE

OMB Action Needed to Address Privacy-Related Gaps in Federal Guidance

GAO-26-107681
March 2026

Highlights of GAO-26-107681, a report to congressional addressees

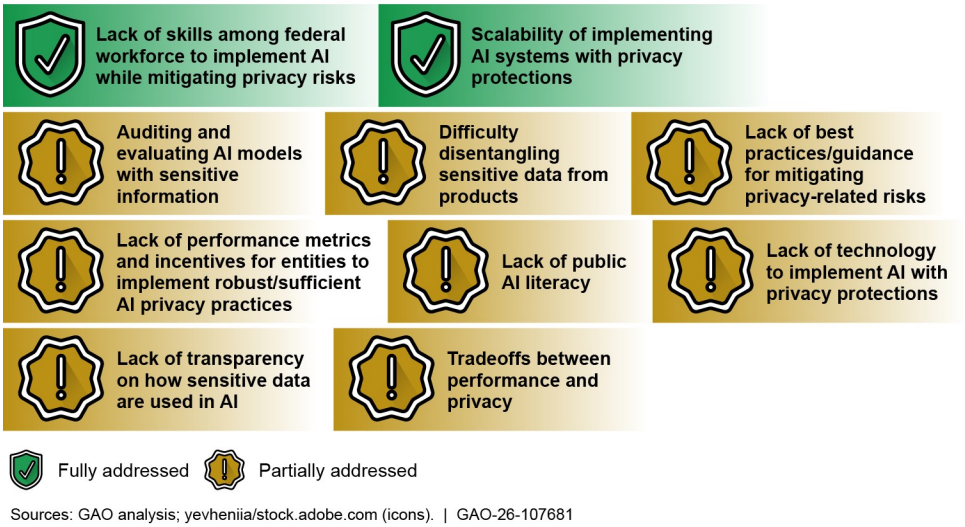
For more information, contact: Marisol Cruz Cain at CruzCainM@gao.gov.

What GAO Found

GAO convened a panel of experts who identified privacy risks and challenges associated with the use of artificial intelligence (AI), which align with GAO's prior reporting on AI use. For example, the experts noted that using AI may reveal sensitive information in raw data sets, potentially exposing personal and private information, among other privacy risks. At the same time, the experts identified several challenges that federal agencies face in addressing these risks. These include the lack of technology to implement AI with appropriate privacy protections and the potential performance tradeoff when adjusting or removing certain data for the sake of privacy.

The Office of Management and Budget (OMB)'s government-wide AI guidance does not fully address all the identified privacy-related risks and challenges. Specifically, OMB's guidance does not specify the types of known privacy-related risks that agencies should consider when establishing policies to address privacy in AI. OMB's guidance provides direction on addressing two challenges identified by the panelists: the need for enhanced skills among the federal workforce to effectively implement AI and the ability to accelerate and scale the implementation of AI systems with privacy protections. However, the guidance does not fully address the remaining eight challenges.

Extent to Which the Office of Management and Budget's Government-wide Guidance Addressed 10 Selected Expert-identified Privacy-related Challenges When Using Artificial Intelligence (AI), as of January 2026



Sources: GAO analysis; yevheniia/stock.adobe.com (icons). | GAO-26-107681

Given the risks and challenges, additional guidance from OMB could help ensure agencies take appropriate steps to protect the privacy of sensitive data when using AI. OMB could also use existing mechanisms, such as the Chief AI Officer Council or Federal Privacy Council, as forums for interagency information-sharing about strategies or best practices for addressing AI-related privacy challenges. Without this additional direction, risks are increased that agencies' use of AI would disclose sensitive data, or compromise privacy in other ways.

Why GAO Did This Study

AI is rapidly evolving and has significant potential to transform society and people's lives. Further, surges in AI capabilities have led to a wide range of innovations with substantial promise for improving the operations of government agencies. However, AI can also pose significant risks to individuals, groups, and organizations. As a result, when agencies use AI to carry out their missions, they need to consider privacy-related risks and challenges. They also need to ensure that they have implemented appropriate risk management and privacy controls to protect the private information of the American public.

In this report, GAO (1) describes the risks and challenges associated with protecting privacy when using AI and (2) examines the extent to which OMB addressed these risks and challenges in government-wide guidance.

To do so, GAO assembled a panel of experts and compiled a non-exhaustive list of privacy risks and challenges associated with AI. GAO also reviewed OMB's AI-related guidance to determine if it highlighted the specific types of privacy risks identified by the experts. Further, GAO compared OMB's AI-related government-wide guidance to 10 selected challenges to determine if they could be addressed by the contents of the guidance.

What GAO Recommends

GAO is making two recommendations to OMB to fully address the identified risks and challenges via updated guidance or by facilitating additional information sharing. GAO provided OMB with a copy of the draft report for its review and comment. OMB did not provide comments.

Contents

Abbreviations

- AI artificial intelligence
- EO executive order
- HIPAA Health Insurance Portability and Accountability Act of 1996
- NIST National Institute of Standards and Technology
- NSF National Science Foundation
- OMB Office of Management and Budget
- PET privacy-enhancing technologies
- PIA privacy impact assessment
- PII personally identifiable information
- SAOP senior agency official for privacy

March 26, 2026

Congressional Addressees

Artificial intelligence (AI) is rapidly evolving and has significant potential to transform society and people's lives.[1] According to the Department of Commerce's National Institute of Standards and Technology (NIST), remarkable surges in AI capabilities have led to a wide range of innovations, including autonomous vehicles and Internet of Things devices in our homes.[2] This rapidly growing transformative technology also holds substantial promise for improving the operations of government agencies. For example, the Department of Health and Human Services used an AI chatbot to assist the agency's security team by providing an automated email response for general physical security questions.[3]

However, AI also poses risks that can negatively impact individuals, groups, organizations, communities, society, and the environment. For example, AI systems may be trained on data that can change over time, sometimes significantly and unexpectedly, affecting system functionality and trustworthiness.[4] In addition, AI systems are inherently socio-technical in nature, meaning they are influenced by societal dynamics and human behavior. AI risks can emerge from the interplay of technical aspects combined with societal factors related to how a system is used, who operates it, and the social context in which it is deployed.

Risks introduced or heightened by AI may also include risks to privacy. To carry out their respective missions, federal agencies use information systems to collect and process large amounts of personally identifiable information (PII),[5] which is used for various government programs, such as health insurance or student loans. For example, using AI in health care settings may raise privacy concerns about individuals' medical data.[6] Accordingly, when using AI to carry out their missions, agencies need to consider privacy-related risks and challenges and ensure that they have implemented appropriate risk management and privacy controls, all to protect the private information of the American public.

[1]AI, in general, refers to computer systems that are able to solve problems and perform tasks that have traditionally required human intelligence and that continually get better at their assigned tasks. The White House, Office of Science and Technology Policy, *American Artificial Intelligence Initiative: Year One Annual Report,* (Washington, D.C.: Feb. 2020) and GAO*, Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon Systems*, GAO-22-104765 (Washington, D.C.: Feb. 17, 2022).

[2]Artificial Intelligence, NIST, (accessed on March 18, 2026), https://www.nist.gov/artificial-intelligence. The Internet of Things generally refers to the technology and devices that allow for the connection and interaction of "things" throughout places such as buildings, vehicles, and transportation infrastructure.

[3]A chatbot is a computer program that simulates human conversation with an end user. Not all chatbots are equipped with AI, but modern chatbots increasingly use conversational AI techniques such as natural language processing to understand user questions and automate responses to them.

[4]The AI model learning process is achieved by using large data sets that identify the desired outcome, with the AI developer validating that the model is producing the desired results.

[5]In general, PII is any information that can be used to distinguish or trace an individual's identity, such as name, date or place of birth, and Social Security number; or that otherwise can be linked to an individual.

[6]For previous reporting on data privacy in health care, see GAO, *Artificial Intelligence in Health Care: Benefits and Challenges of Technologies to Augment Patient Care*, GAO-21-7SP (Washington, D.C.: Nov. 30, 2020).

We performed this work under the authority of the Comptroller General to evaluate the results of a program or activity that the government carries out under existing law.[7] Specifically, we performed this work to inform Congress, federal agencies, and the public of the steps the federal government is taking to protect privacy when using AI. Our objectives were to (1) describe the risks and challenges associated with protecting privacy when using AI and (2) examine the extent to which the Office of Management and Budget (OMB) had addressed privacy-related risks and challenges associated with AI in government-wide guidance.

To address the first objective, we convened a 3-day virtual panel of 12 experts from a variety of fields and affiliations to discuss risks to privacy when using AI and challenges associated with ensuring the implementation of adequate privacy protections when using AI.[8] Specifically, we asked a series of questions aimed at identifying privacy risks and challenges when using AI that could affect private and public sector organizations, including federal agencies. Based on the panel discussions, we developed non-exhaustive lists related to the (1) risks and challenges associated with protecting privacy when using AI; (2) ways the federal government can help protect privacy when working with AI; and (3) other actions and technical solutions that are available to protect privacy when using AI.[9]

To address the second objective, we reviewed OMB's AI-related guidance to determine if it highlighted privacy risks similar to those identified by the experts during our January 2025 panel discussion.[10] To determine if the guidance addressed challenges highlighted by the experts, we selected 10 challenges from the 13 identified by our expert panels that we determined could be addressed by OMB guidance to agencies.[11] We excluded three challenges because it is not reasonable to expect that they would be discussed and addressed in OMB government-wide guidance. For example, although OMB provides legislative proposals to Congress, OMB does not have authority to enact or amend federal statutes related to AI or privacy.

We then compared OMB's guidance to the 10 selected challenges and assessed each as:[12]

- **fully addressed** if the guidance addressed all components of the identified challenge;
- **partially addressed** if the guidance addressed some aspects of the identified challenge, but not all aspects; and
- **not addressed** if the guidance did not address any component of the identified challenge.

[7]31 U.S.C. § 717(b)(1).

[8]To select the experts for the roundtable discussion, we followed a multi-step process to select participants with expertise in one or more areas related to AI and privacy from four affiliation categories—federal, industry, nonprofit, and academic research.

[9]The comments provided by the experts reflected their own views and not those of the organizations with which they are affiliated. Further, the experts' views may not correspond with those of others with similar backgrounds and expertise.

[10]Appendix I provides further details on how we chose which OMB guidance to focus on for our review.

[11]These challenges are listed in appendix I.

[12]We focused our analyses to the following OMB guidance: (1) *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust,* OMB Memorandum M-25-21, (Washington, D.C.: Apr. 3, 2025), (2) *Driving Efficient Acquisition of Artificial Intelligence in Government,* OMB Memorandum M-25-22 (Washington, D.C.: Apr. 3, 2025), (3) *Phase 2 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Open Government Data Access and Management Guidance,* OMB Memorandum M-25-05 (Washington, D.C.: Jan. 15, 2025), (4) *Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance,* OMB Memorandum M-19-23 (Washington, D.C.: July 10, 2019), and (5) *Managing Information as a Strategic Resource,* OMB Circular A-130 (Washington, D.C.: July 2016). Additional details related to why we focused our analysis to these five OMB guidance documents are discussed in appendix I.

Further, we assessed the OMB guidance to determine if it provided agencies with direction or resources they can use to mitigate privacy risks when using AI. Additional details about our objectives, scope, and methodology are discussed in appendix I.

We conducted this performance audit from July 2024 to March 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

AI is a rapidly growing, transformative technology with applications found in many aspects of modern life. While AI definitions vary,[13] the current administration defines AI as a set of techniques, including machine learning, that is designed to approximate a cognitive task.[14] It also defines it as any artificial system that:

- performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets;
- is developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action;
- is designed to think or act like a human, including cognitive architectures and neural networks;
- is designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.[15]

AI holds substantial promise for improving government operations. For example, the National Aeronautics and Space Administration reported using AI that enables intelligent targeting of scientific specimens that match scientists' specifications by planetary rovers.[16] In addition, the Office of Personnel Management uses AI to improve user experiences on its employment website, USAJobs, by providing users job recommendations based on their skills and opportunity descriptions.

While AI tools promise widespread benefits, their increased adoption has also raised significant concerns about their impact on protecting PII. For example, in 2021, Congress directed the Federal Trade Commission to study and report on whether and how AI may be used to identify, remove, or address a wide variety of online harms. The commission reported that while AI continues to advance in cybersecurity as a tool to address online harms, Congress, regulators, scientists, and others should exercise great care and focus attention on several related considerations.[17] Specifically, the report said that personal data collected and used for AI should be explainable and contestable in a manner that protects the privacy of the subjects of that shared data.

[13]GAO, *Artificial Intelligence: Use and Oversight in Financial Services*, GAO-25-107197 (Washington, D.C.: May 19, 2025).

[14]OMB, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, M-25-21.

[15]The term "artificial intelligence" has the meaning provided in Section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, Title II, subtitle B, § 238(g), 132 Stat. 1636, 1697-1698 (10 USC § 2358 note).

[16]GAO, *Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements*, GAO-24-105980 (Washington, D.C.: Dec. 12, 2023).

[17]Federal Trade Commission, *Combatting Online Harms Through Innovation,* Report to Congress, Jun. 16, 2022.

Additionally, the commission reported that entities who build, procure, or deploy AI tools should consider responsibility for both the inputs and the outputs and that they should keep privacy and security in mind—including their treatment of the training data.

Federal Laws, Executive Actions, and Government-wide Guidance for Agencies' Protection of PII

The large amount of PII collected by federal agencies highlights the importance of having strong programs in place for ensuring privacy protections are implemented when agencies are using AI. Federal laws, along with executive branch policy and guidance, establish agency requirements and responsibilities for ensuring the protection of PII and other sensitive personal information. These requirements and responsibilities are related to protecting PII generally and also apply when agencies are using AI that involves PII.[18] They include the following:

- **Privacy Act of 1974.** The act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records.[19] It requires agencies to issue notices to the public when they establish or make changes to systems of records. The notices identify, among other things, the types of data collected, the types of individuals about whom information is collected, the intended "routine" uses of the data, and procedures that individuals can use to review and correct personal information.
- **E-Government Act of 2002.** The act strives to enhance protection for personal information in government information systems by requiring that agencies conduct, where applicable, a privacy impact assessment (PIA) for each system.[20] Agencies must conduct a PIA before developing or procuring IT that collects, maintains, or disseminates information that is in an identifiable form.[21] This assessment is an analysis of how federal systems collect, store, share, and manage personal information.
- **OMB Circular A-130, *Managing Information as a Strategic Resource*.** This July 2016 circular establishes general policy for the planning, budgeting, governance, acquisition, and management of federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services.[22] Appendix II of A-130 outlines general responsibilities for agencies managing information resources that involve PII and summarizes the key privacy requirements for managing those resources. These include developing, implementing, documenting, maintaining, and overseeing agency-wide privacy programs.
- **Executive Order (EO) 13719, *Establishment of the Federal Privacy Council*.** This 2016 EO directs OMB to issue a revised policy on the role and designation of the senior agency official for privacy

[18]The discussion of PII applies to all executive branch agencies. Individual agencies may also have responsibilities for overseeing privacy under area-specific privacy laws such as the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, title II, subtitle F, § 262(a), 110 Stat. 1936, 2021 (Aug. 21, 1996) (codified as amended at 42 U.S.C. §§ 1320d–1320d-9), which covers certain categories of health-related information, and the Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, title V, § 513, 88 Stat. 571 (Aug. 21, 1974) (codified as amended at 20 U.S.C. § 1232g), which pertains to the privacy of student records.

[19]Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (Dec. 31, 1974) (codified as amended at 5 U.S.C. § 552a). A system of records is a collection of information about an individual under control of an agency from which information is retrieved by the name of an individual or other identifier. 5 U.S.C. § 552a(a)(4), (5).

[20]E-Government Act of 2002, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921 (Dec. 17, 2002).

[21]A PIA must also be conducted before initiating any new data collection involving identifiable information that will be collected, maintained, or disseminated using IT, including AI technologies, if the same questions or reporting requirements are imposed on ten or more people.

[22]OMB, *Managing Information as a Strategic Resource,* Circular A-130.

(SAOP).[23] The revised policy includes guidance on the SAOP responsibilities at their agencies, required level of expertise, adequate level of resources, and other matters. Further, the EO established the Federal Privacy Council as the principal interagency forum to improve the government privacy practices of agencies and entities acting on their behalf.

- **OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy*.** As directed by EO 13719, OMB issued this guidance in September 2016 to clarify and update the role of the SAOP.[24] It describes the position, expertise, and authority the official should have, and it provides details on their responsibilities. It notes that the SAOP should have a central leadership role at the agency with visibility into agency operations and a position high enough to regularly engage with senior leadership. It also states that the official should have the skills, knowledge, and expertise to lead the agency's privacy program and the necessary authority to carry out privacy-related functions.
- **NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.** This September 2020 publication provides a catalog of security and privacy controls for information systems, including AI, and organizations. For example, the publication includes a control related to malicious code protection and how AI techniques can be used to detect, analyze, and describe the characteristics or behavior of malicious code, among other things.[25]
- **NIST Privacy Framework.** This document is a voluntary tool developed in collaboration with stakeholders intended to help organizations identify and manage privacy risks to build innovative products and services while protecting individuals' privacy. The document also provides guidance related to how agencies can use the framework to identify and prioritize outcomes to effectively manage AI privacy risks.[26]

Federal Laws and Executive Branch Actions Address Privacy Considerations in Agencies' Use of AI

Over the past 6 years, EOs and federal laws, as well as White House and federal guidance have addressed agencies' implementation of AI and provided requirements and information related to protecting the privacy of PII (see figure 1).

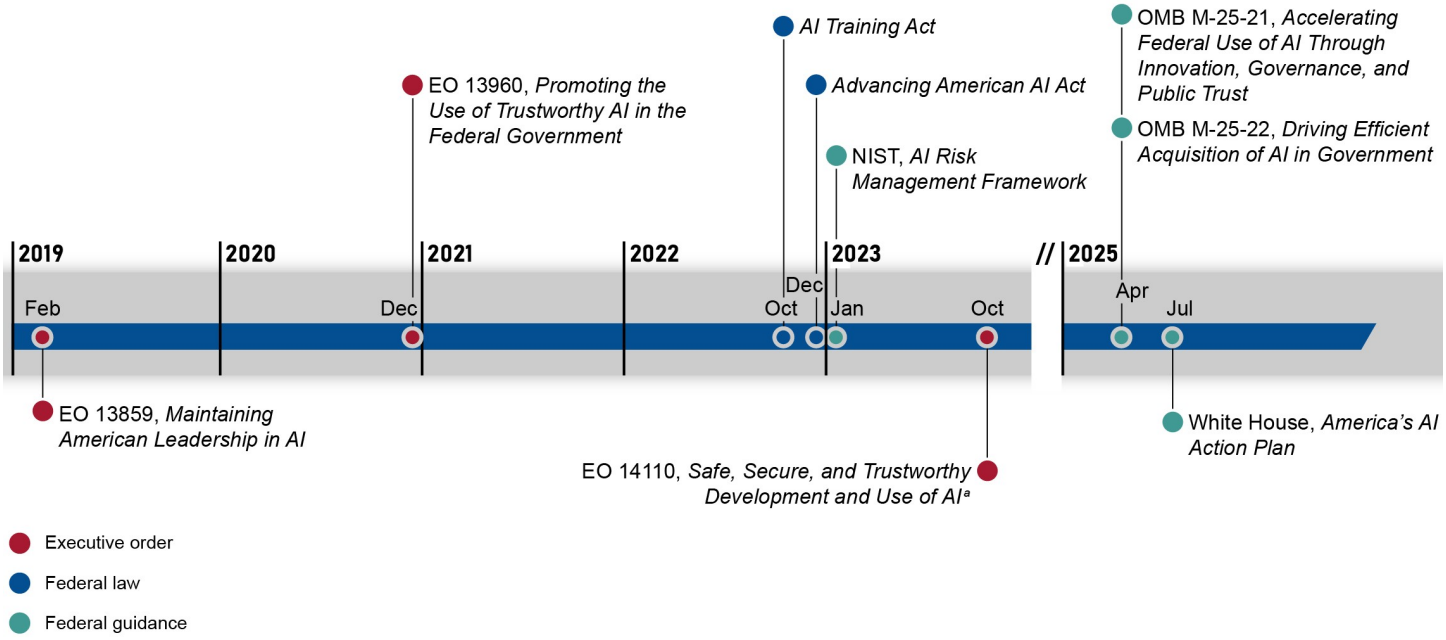
[23]Exec. Order No. 13719, 81 Fed. Reg. 7687, *Establishment of the Federal Privacy Council*, (Feb. 09, 2016).

[24]OMB, *Role and Designation of Senior Agency Officials for Privacy,* M-16-24 (Washington, D.C.: Sept. 15, 2016).

[25]NIST, Special Publication 800-53, Revision 5: *Security and Privacy Controls for Information Systems and Organizations* (Gaithersburg, MD.: September 2020).

[26]NIST first issued the privacy framework, version 1.0, in January 2020. In April 2025, NIST issued a draft of version 1.1 of the framework for public review and comment. NIST Cybersecurity White Paper Initial Public Draft, *NIST Privacy Framework 1.1*, (Gaithersburg, MD.: April 2025).

Figure 1: Timeline of Selected Federal Efforts Related to Artificial Intelligence and Privacy



EO = executive order, AI =artificial intelligence, OMB = Office of Management and Budget, NIST = National Institute of Standards and Technology

Source: GAO analysis of federal guidance and legislation on AI. | GAO-26-107681

[a]EO 14110 was rescinded by EO 14148.

As shown above, the selected federal efforts related to AI and privacy include the following:

- In February 2019, the White House issued EO 13859, establishing the American AI Initiative. Among other things, the order included a requirement for OMB to issue guidance for agencies on the regulation of AI applications. Further, EO 13859 states that the guidance should include information on ways to reduce barriers to the use of AI technologies while protecting civil liberties and privacy.[27]
- In December 2020, the White House issued EO 13960, on promoting the use of trustworthy AI. The order states that agencies must design, develop, acquire, and use AI in a manner that fosters public trust and confidence while protecting privacy, civil rights, and civil liberties.[28]
- In October 2022, the AI Training Act was enacted to ensure that the acquisition workforce of executive agencies has knowledge of the capabilities and risks associated with AI. It includes a requirement for OMB, in coordination with the General Services Administration (GSA), to develop and implement an AI training program for the executive branch's acquisition workforce that includes information related to the risks posed by AI to privacy, among other things.[29]
- In December 2022, the Advancing American AI Act was enacted to encourage agency AI-related programs and initiatives. The act states that it is intended to promote the adoption of modernization business

[27]Exec. Order No. 13859, 84 Fed. Reg. 3967, *Maintaining American Leadership in Artificial Intelligence* (Feb. 11, 2019).

[28] Exec. Order No. 13960, 85 Fed. Reg. 78939, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government* (Dec. 3, 2020).

[29]AI Training for the Acquisition Workforce Act, Pub. L. No. 117-207, 136 Stat. 2238 (2022) (codified at 41 U.S.C. § 1703).

practices and advanced technologies across the federal government that include the protection of privacy, among other things.[30]

- In October 2023, the White House issued EO 14110 to advance a coordinated, federal government-wide approach to the development and safe and responsible use of AI. This EO included specific privacy-related requirements for three agencies, OMB, the National Science Foundation (NSF), and NIST.[31] Specifically, the order identified four requirements for OMB, including issuing a request for information to inform potential revisions to its guidance on implementing the privacy provisions of the E-Government Act of 2002. The EO identified three requirements for NSF, including funding the creation of a research coordination network dedicated to advancing privacy research and, in particular, the development, deployment, and scaling of privacy-enhancing technologies (PET).[32] The order also required NIST to create guidelines for agencies to evaluate the efficacy of differential privacy-guarantee protections, including for AI. However, this EO has since been rescinded.[33]
- In July 2025, the White House issued America's AI Action Plan to set near-term policy goals and associated recommendations for the federal government to execute. Among other things, the plan includes a policy recommendation to create an AI procurement toolbox, managed by GSA and in coordination with OMB, that would allow federal agencies to choose multiple models uniformly and easily in a manner that is compliant with relevant privacy, data governance, and transparency laws.[34]

Two federal agencies, OMB and NIST, have also issued guidance related to protecting privacy when using AI. OMB serves as the primary agency for establishing and updating government-wide AI policy and guidance based on requirements in several of the EOs and laws. In January 2025, the President instructed OMB to revise two key AI-related memorandums,[35] and OMB issued the revised memoranda in April 2025:

- **OMB Memorandum M-25-21, *Accelerating Federal Use of AI Through Innovation, Governance, and Public Trust*.**[36] The memorandum is intended to provide guidance to agencies on how to innovate and promote the responsible adoption, use, and continued development of AI, while ensuring appropriate safeguards are in place to protect privacy, among other things. It also includes requirements for agencies, such as revisiting, and updating where necessary, their internal policies on IT infrastructure, data, cybersecurity, and privacy as they pertain to AI by December 29, 2025. Agencies are also required to

[30]Advancing American AI Act, Div. G of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, Div. G title LXXII, subtitle B, §§7221-7228,136 Stat. 2395, 3668-3676 (2022) (codified at 40 U.S.C. § 11301 note).

[31]Exec. Order No. 14110, 88 Fed. Reg. 75191, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (Oct. 30, 2023) (rescinded by Exec. Order No. 14148, 90 Fed. Reg. 8247 (Jan 20, 2025)).

[32]PETs are a collection of tools, techniques, and methods designed to protect individuals' personal information and ensure their privacy in digital environments.

[33]Actions taken to implement the privacy-related requirements of this order include the following: In January 2024, OMB issued a request for information on how agencies' PIAs may be more effective at mitigating privacy risks, including those that are further exacerbated by AI. In February 2024, NSF funded the establishment of a Research Coordination Network dedicated to advancing privacy-preserving data sharing and analytics. NSF reported in a press release that the network will bring together experts from academia, industry, and government to support the development, deployment, and scaling of privacy enhancing technology tools. In March 2025, NIST issued *Guidelines for Evaluating Differential Privacy Guarantees* to help evaluate the efficacy of differential privacy-guarantee protections, including for AI. NIST, *Guidelines for Evaluating Differential Privacy Guarantees*, Special Publication 800-226, (Gaithersburg, MD: March 2025). According to NIST, differential privacy is a mathematical framework that quantifies privacy loss to entities when their data appears in a dataset.

[34]The White House, *Winning the Race: America's AI Action Plan* (Washington, D.C.: July 2025).

[35]Exec. Order No. 14179, 90 Fed. Reg. 8741, *Removing Barriers to American Leadership in Artificial Intelligence* (Jan. 23, 2025).

[36]OMB, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, M-25-21. This memorandum replaced OMB Memorandum M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*.

develop policies that set the terms for acceptable use of generative AI and establish safeguards and oversight mechanisms for using this tool without posing undue risk.[37] In addition, the memorandum also instructed OMB to establish and chair a Chief AI Officer Council to coordinate the development and use of AI in agencies' programs and operations.

- **OMB Memorandum M-25-22, *Driving Efficient Acquisition of Artificial Intelligence in Government*.**[38] The memorandum is intended to provide guidance to agencies to improve their ability to acquire AI responsibly. Further, it states that agencies shall establish policies and processes that ensure compliance with privacy requirements in law and policy. This is applicable whenever agencies acquire an AI system or service, or an agency contractor uses an AI system or service, that will create, collect, use, process, store, maintain, disseminate, disclose, or dispose of federal information containing PII.

NIST has also issued guidance related to addressing privacy-related risks when using AI. Specifically, in January 2023, NIST issued an AI Risk Management Framework.[39] This guidance document is intended for voluntary use by organizations designing, developing, deploying, or using AI systems. The document describes characteristics of trustworthy AI systems, including being secure and resilient, safe, and privacy-enhanced, among others. NIST has also issued other guidance related to AI and privacy. For example, in March 2025, NIST issued a report that identified current challenges in the life cycle of AI systems, along with a taxonomy of concepts and defined terminologies in the field of adversarial machine learning.[40] Specifically, it discussed privacy attacks and described corresponding methods for mitigating and managing the consequences of those privacy attacks, such data reconstruction, among other things.

GAO Has Issued AI Guidance and Reported on Privacy Challenges Associated with AI Use

Recognizing the increasing importance and usage of AI, we have issued guidance related to assessing AI systems for data security and privacy. Specifically, in June 2021, we published a framework to help managers ensure accountability and the responsible use of AI in government programs and processes.[41] The framework described four principles—governance, data, performance, and monitoring—and associated key practices to consider when implementing AI systems. Each of the practices contained a set of questions and procedures for auditors and third-party assessors to consider when reviewing efforts related to AI. For example, for the data principle, an audit procedure to assess privacy would be to review security and privacy assessments to assess whether the methodology, test plans, and results identify deficiencies and/or risks and the extent to which they are promptly corrected.

In addition, we have reported on agencies' use of AI and the actions that need to be taken to protect sensitive personal data held by federal agencies. We also highlighted the importance of taking steps to protect

[37]Generative AI differs from other AI systems in its ability to create novel content, in the vast volumes of data it requires for training, and in the greater size and complexity of its models.

[38]OMB, *Driving Efficient Acquisition of Artificial Intelligence in Government*, M-25-22. This memorandum replaced OMB Memorandum M-24-18, *Advancing the Responsible Acquisition of Artificial Intelligence in Government*.

[39]NIST, *Artificial Intelligence Risk Management Framework*, NIST AI 100-1 (Gaithersburg, MD.: Jan. 26, 2023).

[40]NIST, *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations,* NIST AI 100-2e2025 (Gaithersburg, MD.: Mar. 24, 2025).

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

individuals' sensitive data and establishing programs and processes for ensuring that appropriate privacy protections are implemented. For example:

- In September 2013, we reported that the advent of new and more advanced technologies had vastly increased the amount and nature of personal information collected along with the number of parties that used or shared this information.[42] Subsequently, we reported that the current statutory framework for protecting the privacy of U.S. consumers did not fully address changes in technology and marketplace practices from August 2012 through September 2013. Accordingly, we suggested that Congress consider strengthening the current framework for consumer privacy to reflect the effects of changes in both the technology and the marketplace, while also ensuring that any limitations on data collection and sharing do not unduly inhibit the benefits to industry and consumers. As of March 2026, legislative action had not yet been taken to address this matter.
- In September 2022, we reported on challenges agencies were experiencing in implementing their privacy programs, among other things.[43] We found that privacy officials from 20 of the 24 Chief Financial Officers Act agencies[44] reported applying privacy requirements to new and emerging technologies, including AI, as a challenge. Further, 13 of these 20 agencies stated that this was due to lack of federal guidance for newer technologies such as AI technologies, or a lack of knowledge and expertise for applying privacy requirements to these technologies. This could include privacy, security, and acquisition roles and requirements for AI, cloud service providers, and other new technologies.
- In November 2024, we reported that new and emerging technologies, including AI, have changed society's understanding of how to protect the civil rights and civil liberties of all Americans.[45] Therefore, we examined federal agencies' civil rights and civil liberties protections related to data collection, sharing, and use. Among other things, agencies pointed out that emerging technologies, such as AI, pose new questions and concerns with protecting civil rights and civil liberties. Further, while some aspects of existing federal guidance address important civil rights and civil liberties issues, such as privacy and risks from using AI, they do not address other areas of concern, technologies, and methods of data collection. We suggested that Congress direct an appropriate federal entity to issue government-wide guidance or regulations addressing this matter. As of March 2026, legislative action had not yet been taken to address this matter.

[42]GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

[43]GAO, *Privacy: Dedicated Leadership Can Improve Programs and Address Challenges*, GAO-22-105065 (Washington, D.C.: Sept. 22, 2022).

[44]The Chief Financial Officers Act of 1990, Pub. L. No. 101-576, 104 Stat. 2838 (Nov. 15, 1990), as amended, established Chief Financial Officers to oversee financial management activities at 23 civilian executive departments and agencies as well as the Department of Defense. The list of 24 entities is often referred to collectively as Chief Financial Officer Act agencies, and is codified, as amended, in § 901 (b) of Title 31 of the U.S. Code. The 24 agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs, the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

[45]GAO, *Information Technology: Government-Wide Guidance on Handling Data Could Improve Civil Rights and Civil Liberties Protections*, GAO-25-106057 (Washington, D.C.: Nov. 19, 2024).

Experts Identified Privacy Risks and Challenges Associated with the Use of AI and Ways to Address Them

The experts at the roundtable we convened identified 10 key risks, which we defined as the potential negative outcomes or specific threats to privacy that could arise from AI usage if not properly addressed (e.g., data breaches, misuse, bias). An example of a risk is the potential invasion of privacy from data aggregation when using the technology. The experts also identified 13 key challenges, which we defined as the difficulties or obstacles in the process of implementing and managing AI while mitigating privacy-related risks (e.g., regulatory compliance, transparency, data quality). One example of a challenge is that there is currently not a comprehensive privacy law in the United States, leaving gaps and potentially providing inconsistent levels of protection.[46]

Additionally, the experts identified ways the federal government can help protect privacy when working with AI, including actions agencies, Congress, and the White House can take and technological solutions that can be used to address associated privacy risks and challenges. For example, the experts emphasized the need for a coordinated national strategy that prioritizes privacy and is supported by robust legislation and stakeholder collaboration to help balance AI innovation with individual privacy rights.

Risks Associated with Protecting Privacy When Using AI

The experts identified 10 key risks related to privacy when using AI, including potential invasions of privacy from data aggregation and the use of data for purposes exceeding what was originally intended. Table 1 identifies the 10 risks and associated descriptions.

Table 1: Expert-Identified Risks Associated with Protecting Privacy When Using Artificial Intelligence (AI)

Risk name	Associated risk description
Data persistence	Data may continue to exist in AI systems and be difficult to extract/remove once collected.
Data re-identification	AI has the ability to cross-reference multiple data sets from seemingly independent and anonymous outputs to reidentify anonymized data.[a]
Generation of deceptive or inaccurate outputs	AI may be used to intentionally or unintentionally generate deceptive outputs (e.g., deepfakes) or inaccurate outputs (e.g., hallucinations)[b] that may result in harm towards individuals.
Improper disclosure	AI can reveal and cause improper sharing of individuals' data when it infers additional sensitive information from raw data.
Increased accessibility to sensitive information	AI can make sensitive information more accessible to a wider audience (e.g., data brokers) than intended.
Invasion of privacy from data aggregation	AI may combine various pieces of data about a person to make inferences beyond what is explicitly captured in those data (e.g., social scoring),[c] which can invade an individuals' personal space and solitude by revealing private information (e.g., health-related, financial, location).
Lack of security over data	Inadequate AI data requirements and storage practices can result in data breaches and improper access.

[46]As discussed earlier, we have also previously reported on the gaps in privacy-related laws. For example, in 2013, we reported that gaps exist in the current statutory framework for privacy. Additionally, we found the framework does not fully reflect the Fa ir Information Practice Principles, widely accepted principles for protecting the privacy and security of personal information that have served as a basis for many of the privacy recommendations federal agencies have made. See GAO-13-663.

Risk name	Associated risk description
Lack of transparency related to data use	AI may be used without providing individuals with notice and control over how their data is being used.
Lack of transparency in AI model algorithmic decision-making	The workings of AI models could include decisions based on individual data that one is unaware of and that can lead to privacy risks.
Secondary use of data	The use of personal data for purposes other than originally intended can be exacerbated by AI's ability to repurpose data.

Source: GAO analysis of comments from subject matter experts. | GAO-26-107681

[a]Anonymized data is information from which personally identifiable information (PII), such as names, addresses, and unique identifiers, has been removed or modified so that individuals are not re-identified from the data.

[b]Hallucinations are outputs that seem plausible but are ultimately false.

[c]Social scoring is the evaluation or classification of individuals or groups based on their social behavior, economic status, or predicted personal characteristics.

The experts warned that while the use of AI can provide significant benefits, such as increased speed and productivity in analysis and decision-making across many industries (e.g., health care and finance), it also introduces key privacy risks such as those listed in table 1. According to the experts, compared to traditional technologies (e.g., rule-based or manual systems), AI exacerbates privacy risks due to its ability to process and analyze vast datasets at unprecedented scale and speed,[47] and in ways that exceed original data collection purposes (also referred to as "secondary use"). The experts explained that an example of this is personal data collected for one purpose, such as health data for patient care, being used to train AI models for other applications. For instance, related to biological samples and DNA, the experts warned that people may consent to one kind of data use but, with the use of AI, anonymized data can be reidentified and used to identify or make predictions about an individual (e.g., predicting criminal behavior or other tendencies).

In addition, the experts agreed that potential invasions of privacy from data aggregation using AI is a major concern. AI can be used to combine various pieces of data about a person to make inferences beyond what is explicitly captured in those data (e.g., social scoring).[48] The experts also explained that the ability to use AI to combine multiple data sets, including from seemingly independent and anonymous outputs creates significant privacy risks. A notable example is China's use of AI to construct a nationwide social credit system.[49] China's construction of this system has been identified as a major concern by both the executive branch and some members of Congress, because of the broad controls such a system is likely to give the Chinese government over U.S. citizens and companies operating in China. It has been widely reported that China is using surveillance measures and AI to collect and analyze vast amounts of data from various sources including surveillance cameras, financial documents, social media, and DNA and health care records to create comprehensive profiles and monitor the behavior of individuals.

Further, according to the experts, the ability of AI to make this information more accessible to a wider audience than originally intended (e.g., data brokers, foreign adversaries, and other entities) puts individuals' privacy and

[47]For example, in health care, traditional analysis of health data may be done in a system manually, such as by reviewing medical imaging data. In contrast, the ability of AI to process these images far surpasses traditional systems, with AI models being able to process images faster and detect abnormalities with high accuracy, cross-referencing them with patient histories and medical databases in real-time.

[48]Social scoring is the evaluation or classification of individuals or groups based on their social behavior, economic status, or predicted personal characteristics.

[49]China began constructing a nationwide social credit system in 2014. The social credit system has been developed into two conn ected but distinct systems: a system for monitoring individual behavior and a more robust system for monitoring corporate behavior. See Congressional Research Service, *China's Corporate Social Credit System* (Washington, D.C.: Jan. 17, 2020).

sensitive information at increased risk. In addition, inadequate data requirements and storage practices for AI create the risk of data breaches and improper access.

The experts' comments align with our prior reporting on AI use. For example, we previously reported that financial institutions' use of AI can expose consumers to new privacy risks.[50] Specifically, the benefits of AI use for financial institutions can include improved efficiency, reduced costs, and enhanced customer experience—such as more affordable, personalized investment advice. However, the use of certain machine learning and generative AI models may result in breaches of sensitive data directly or by inference, including by deducing identities from anonymized data. Recent reports have highlighted that organizations may be lacking proper AI access controls that could result in data breaches. For example, International Business Machines Corporation, or IBM, reported that several organizations have experienced an AI-related breach, which suggests AI is already an easy, high-value target.[51]

Our previous reporting also covered how AI enables financial institutions to collect and analyze increasing amounts of sensitive consumer data. This may involve collecting, analyzing, and sharing PII and biometrics; customer website or app usage data; geospatial location; social media activity; and written, voice, and video communications. Financial institutions may also rely on third parties to develop AI models or to store data, which could heighten privacy risks. For example, cloud computing used in AI exacerbates privacy risks when financial institutions lack the expertise to conduct effective due diligence on cloud services.

Challenges Associated with Protecting Privacy When Using AI

The experts also identified 13 key challenges associated with protecting privacy when using AI, including gaps in AI and privacy-related laws and the lack of a federal workforce with the expertise to implement AI while mitigating privacy-related risks. Table 2 identifies the 13 challenges and associated descriptions.

Table 2: Expert-Identified Challenges Associated with Protecting Privacy When Using Artificial Intelligence (AI)

Challenge name	Associated challenge description
Auditing and evaluating AI models with sensitive information	Evaluating AI models without collecting and potentially exposing sensitive information can be difficult.
Difficulty disentangling sensitive data from products	Models, systems, and/or integrated products may have data stored in a way that cannot easily be segmented, making it hard to separate sensitive data from the entire dataset. This means using these products without the risk of sensitive data being exposed or used in ways that are not intended may be difficult.

[50]GAO-25-107197.

[51]Specifically, in its Cost of a Data Breach Report 2025, IBM reported that 13 percent of the organizations included in its research population reported breaches of AI models or applications, while 8 percent of organizations reported not knowing if they had been compromised in this way. Of those compromised, 97 percent reported not having AI access controls in place. As a result, 60 percent of the AI-related security incidents led to compromised data and 31 percent led to operational disruption. See *IBM Report: 13% Of Organizations Reported Breaches Of AI Models Or Applications, 97% Of Which Reported Lacking Proper AI Access Controls*.

Challenge name	Associated challenge description
Gaps in AI and privacy-related laws	There is not a comprehensive legal framework governing AI, privacy, or their intersection. Rather, individual laws cover different sectors (e.g., federal agencies, financial institutions, health care), leaving gaps and potentially providing inconsistent levels of protection.[a] For example: Federal laws lack requirements for the procurement and use of AI, and associated accountability measures to enforce them, making them insufficient in addressing privacy concerns and making current guidance on AI ineffective. Legal exemptions could potentially be used to bypass privacy protections, such as by using exemptions in law commonly referred to as "routine use" exemptions. This may result in the extensive use of data with AI and not having to go through the existing privacy-related checks and requirements.
Lack of best practices/guidance for mitigating privacy-related risks	There is a lack of clear rules, norms, and best practices related to privacy both at broad and sectoral levels as they apply to AI. As a result, entities do not fully understand which privacy-related guidance applies for their respective sectors/areas when using AI.
Lack of performance metrics and incentives for entities to implement robust/sufficient AI privacy practices	Without proper performance metrics and incentives, organizations may not be able to gauge the impact of AI on privacy or the effectiveness of privacy measures.
Lack of public AI literacy	There is a lack of understanding among the public about AI, leading to a lack of understanding of what they are consenting to.
Lack of skills among federal workforce to implement AI while mitigating privacy risks	Federal agencies struggle to hire new staff and/or train existing staff to ensure they have sufficient knowledge of AI and privacy to implement AI while mitigating privacy-related risks.
Lack of technology to implement AI with privacy protections	Organizations may lack access to tools that could be used to protect sensitive data when using AI.
Lack of transparency on how sensitive data are used in AI	Organizations do not always inform the public about how their data are used in AI models and algorithms. As a result, members of the public may face difficulties in pursuing their rights or interests. Further, for federal agencies, there is uncertainty related to the type of public engagement required to conduct privacy impact assessments (PIA) for their information systems that use AI.[b] As a result, agencies may conduct PIAs inconsistently and could potentially implement AI technology prior to addressing privacy-related issues.
Limited time to implement new AI-related requirements into law	AI evolves faster than the time it takes to develop and finalize legislation. By the time a law is enacted and implemented, the AI technology has likely evolved to the point where the requirements in the legislation are no longer fully effective.
Privacy skepticism	The widespread idea that privacy is an unattainable concept, potentially dissuading people in pursuing building/implementing privacy protections when working with AI.
Scalability of implementing AI systems with privacy protections	Organizations may have difficulty implementing AI systems, while mitigating privacy-related risks, at a scale that will work across multiple different datasets and scenarios.
Tradeoffs between performance and privacy	Adjusting/removing certain data for the sake of privacy, specifically in most significant contexts, can result in a consequential performance tradeoff.

Source: GAO analysis of comments from subject matter experts. | GAO-26-107681

[a]Additionally, states have varying laws governing AI and privacy. For example, states like Oregon, Colorado, and Connecticut require explicit consent before collecting sensitive data. However, Colorado only requires consent prior to sale. States without privacy laws are currently silent on this issue.

[b]PIAs document the process of analyzing how information, particularly personally identifiable information, is collected, used, shared, and maintained within a system or project.

The experts provided additional details related to the effects associated with the challenges listed below and their impacts in certain areas that affect privacy.

- **Gaps in laws and other requirements.** There is currently not a comprehensive privacy law in the United States. Rather, individual laws cover different sectors (e.g., federal agencies, financial institutions, health

care), leaving gaps and potentially providing inconsistent levels of protection.[52] Moreover, most existing privacy laws do not explicitly address AI and the unique privacy risks its use may create or exacerbate. For example, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 protects certain health data held by covered entities, such as providers.[53] However, the HIPAA protections, like other federal privacy frameworks, do not explicitly address AI. Accordingly, the experts said, there are gaps in protecting health-related information processed by AI systems. While the HIPAA Privacy Rule limits the disclosure of protected health information, use of health data by AI tools could create additional privacy risks.[54] For example, the experts explained that a covered provider's use of tools, such as third-party software for identifying markers for cancer by analyzing patient data, could potentially risk unauthorized use of health information like radiographic films.

Further, the experts noted that while privacy protections do exist, exemptions in the Privacy Act, such as the "routine use" exemption, could allow federal agencies to use data in AI more extensively than intended. Determining a qualifying routine use is often left to the discretion of agencies and OMB, although they must be noted and defined in publicly available system of records notices. The experts added that routine use exemptions claimed by agencies could allow data to be used in a very broad manner and likely in conjunction with AI technologies.[55]

As discussed earlier, we have previously reported on the gaps in federal privacy-related laws. For example, in 2013, we reported that gaps exist in the current statutory framework for privacy. Additionally, we found the framework does not fully reflect the Fair Information Practice Principles.[56] These are widely accepted principles for protecting the privacy and security of personal information that have served as a basis for many of the privacy recommendations federal agencies have made.[57] We have also noted that technological developments since the Privacy Act became law in 1974 have changed the way information is organized and shared among organizations and individuals.[58] Such advances have rendered some of the provisions of the Privacy Act and the E-Government Act of 2002 inadequate to fully protect all PII

[52]Additionally, states have varying laws governing AI and privacy.

[53]Pub. L. No. 104-191, Title II, Subtitle F, 110 Stat. 1936, 2021 (Aug. 21, 1996) as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, tit. XIII, 123 Stat. 115, 226 (Feb. 17, 2009). HIPAA governs protected health information (PHI) which is individually identifiable health information and applies to covered entities and business associates. Covered entities are health plans, health care providers, and health care clearinghouses. Business associates are third parties that (1) create, receive, maintain, or transmit PHI on behalf of a covered entity for a covered function; or (2) provide certain services to o r for a covered entity that involve the disclosure of PHI. 45 C.F.R. § 160.103.

[54]45 C.F.R. Part 164, Subpart E.

[55]Subsections (j) and (k) of the Privacy Act prescribe the circumstances under which exemptions can be claimed and identify the provisions of the act from which agencies can claim exemptions. When an agency uses the authority in the act to exempt a system of records from certain provisions, it is to issue a rule explaining the reasons for the exemption. For example, an agency can claim an exemption when the records are certain investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information.

[56]The Fair Information Practice Principles are a set of internationally recognized principles for protecting the privacy and security of personal information. A U.S. government advisory committee first proposed the practices in 1973 in response to concerns about the consequences computerized data systems could have on the privacy of personal information.

[57]GAO-13-663.

[58]GAO, *Privacy: Federal Law Should Be Updated to Address Changing Technology Landscape*, GAO-12-961T (Washington, D.C.: July 31, 2012).

collected, used, and maintained by the federal government.[59] The widespread adoption of AI tools will continue to introduce changes in how information is organized and shared.

- **Lack of AI literacy among the public and lack of federal agencies' transparency about how they are using sensitive data in AI.** Members of the public may lack literacy about AI, including the different types of AI, how models work, and their maturity. Further, they may have little idea about how agencies are using their data in AI applications or what the implications are for their privacy. As a result, the public may not be aware of how or when their data are being used in agencies' AI models and algorithms. The experts also warned that members of the public can experience difficulties related to pursuing their rights or interests. In addition, federal agencies face uncertainty related to the type of public engagement that is required when conducting PIAs for their information systems that use AI. As a result, the experts said, agencies may be conducting assessments inconsistently and implementing AI technology prior to addressing privacy-related issues.
- **Lack of skills among the federal workforce and technology for managing AI.** Federal staff may have insufficient expertise or training in the development and use of AI. This may be, in part, because the government struggles to compete for talent with the private sector. In addition, staff may not have access to more advanced tools that could be used to help protect sensitive data when using AI or the expertise to use those tools.

  This aligns with over a decade of our previous reporting in which we have identified mission-critical gaps in federal workforce skills and expertise in science, technology, engineering, and mathematics, including our reporting on a severe shortage of federal staff with AI expertise. Specifically, we have reported that improvements may have been hampered by uncompetitive compensation and the lengthy federal hiring process.[60]
- **Tradeoffs between performance and privacy.** The experts said that in many contexts there is a consequential performance trade off to removing certain data from the data pool. For example, for models to actually be predictive and useful in the context of health or finance, they need to have access to information that is accurate and often intimate or sensitive. This can result in significant privacy invasions and exposure of sensitive information.

Ways Federal Agencies and Leadership Can Address AI Privacy Risks and Challenges

The expert roundtable identified ways the federal government can help protect privacy when working with AI, including actions agencies, Congress, and the White House can take to address the associated privacy risks and challenges. The experts mentioned the following measures to mitigate AI-related privacy risks and address the challenges discussed above:

- **Balance privacy and utility.** To address the challenge of tradeoffs between performance and privacy, the experts emphasized the need for policies prioritizing privacy. This can include the enabling of opt-in

[59]OMB's most recent guidance for conducting PIAs was issued in 2016. See OMB, *Managing Information as a Strategic Resource*, Circular A-130.

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

mechanisms and data security-related laws that can help give users a choice regarding how their data is used and help protect privacy while maintaining AI functionality.[61]

- **Enact legislation and regulation.** To address gaps in laws and other requirements, the experts suggested that legislation should be enacted, including a comprehensive federal privacy law, to ensure more consistent levels of protection. In addition, they emphasized that privacy laws should explicitly address AI and its unique associated risks. Further, according to the experts, data aggregation and secondary use by third-party vendors could be limited by regulating data brokers' use of AI and use of geospatial data, among other things.
- **Improve transparency.** To address federal agencies' lack of transparency regarding how they are using sensitive data in AI, the experts suggested that agencies should conduct and disclose PIAs and technical details (e.g., model cards)[62] to build public trust and verify privacy compliance. In addition, they emphasized that clearer federal requirements are needed for agencies conducting PIAs related to the type of public engagement required for their information systems that use AI. According to the experts, this could ensure more consistent development of PIAs and privacy considerations, including those related to transparency, being taken prior to AI technology being implemented.
- **Prioritize funding and staffing.** To address the lack of a federal workforce and technology for implementing AI while mitigating privacy-related risks, the experts suggested that resources should be allocated to hire AI and privacy experts and acquire tools to manage associated risks effectively. In addition, they stated that the AI and privacy experts should collaborate to ensure appropriate privacy protections are implemented.

In addition to the actions listed above, the experts mentioned other steps that can help protect privacy while working with AI. Several of these measures are already in place to protect PII when using more traditional technologies. The experts also noted that these measures may have limitations such as insufficient scalability, risks introduced by tools, and reliance on human oversight. Accordingly, they emphasized that federal agencies and leadership should evaluate whether these measures may be needed or adequate for protecting privacy when using AI (see table 3).

Table 3: Expert-Identified Actions and Technical Solutions That Can Help Protect Privacy While Working with Artificial Intelligence (AI)

Action/solution	Experts' associated comments
Adopt technology-neutral rules	Adopt flexible privacy principles to ensure policies remain relevant as AI evolves, which can reduce rulemaking delays and burdens.
Apply data quality standards	Apply leading data quality standards, such as National Institute of Standards and Technology standards, before feeding data into AI systems, which can minimize risks from poor data integrity.
Conduct continuous risk assessments	Conduct privacy impact assessments (PIA)[a] and risk assessments on an ongoing basis, trigged by new risks to help adapt to rapidly changing uncertainties associated with AI's evolution.

[61]Opt-in and opt-out mechanisms determine how users consent to the collection and use of their personal data. Opt-in requires users to actively grant permission, while opt-out assumes consent unless the user takes action to prevent it.

[62]A model card is a document that provides essential information about a machine learning model. It aims to increase transparency and facilitate responsible deployment of AI models by clearly outlining the model's purpose, intended use, performance characteristics, and limitations.

Action/solution	Experts' associated comments
Develop metrics and audits	The National Institute of Standards and Technology and the U.S. Center for AI Standards and Innovation (formerly named the AI Safety Institute)[b] should develop standardized metrics for AI privacy impacts and subsidize external auditing ecosystems.
Develop testing infrastructure	Agencies should have access to shared technical infrastructure (e.g., test beds such as those used by the Department of Defense and the Department of Homeland Security), which can help evaluate AI systems in context by involving privacy experts to ensure robust assessments.
Elevate privacy leadership	Appoint statutory privacy officers, establish advisory boards, and foster cross-agency collaboration to prioritize privacy.
Enhance procurement practices	Conduct privacy-related risk evaluations for AI system acquisitions.
Establish a national strategy	Develop and implement a national strategy for AI use that prioritizes privacy as a core value and is supported by robust legislation and stakeholder collaboration.
Implement governance frameworks	Implement a layered governance approach, including using large language models[c] to interpret regulations and policies, dashboards for visibility, and alerts for privacy-enhancing technology (PET)[d] effectiveness. This requires standardized, measurable systems akin to privacy practices.
Leverage AI-driven tools	Leverage AI-driven tools that can, for example, draft PIAs, detect unauthorized data collection (e.g., web trackers), and analyze privacy documentation for compliance. Ensure human oversight when using these tools.
Strengthen enforcement	Agencies like the Federal Trade Commission, Consumer Financial Protection Bureau,[e] and the Department of Health and Human Services could leverage existing authorities for robust enforcement, supported by adequate funding and technical expertise.
Utilize cybersecurity-related testing	Utilize continuous testing for AI (e.g., red teams for identifying vulnerabilities) to identify privacy-related weaknesses. However, this type of testing typically focuses on security rather than identifying nuanced privacy-related issues and thus may have certain limitations.
Utilize dynamic consent management	Implement systems using metadata[f] to manage consent. This addresses the issue where individuals consent to their data initially being used for a certain use case, but the data may then be fed into an AI model for other uses. Further, this could address issues like re-identification when data is used in AI. This addresses the issue where AI is used to cross reference multiple data sets to reidentify anonymized data. For example, the experts recalled re-identification occurring with data related to biological samples and DNA.
Utilize PETs	Use PETs such as encryption, differential privacy, and tokenization, which can help protect data. However, these tools may not always be universally robust. For example, differential privacy has inherent limits in balancing utility and privacy, and encryption does not address all AI-specific risks like inference.

Source: GAO analysis of comments from subject matter experts. | GAO-26-107681

[a]PIAs document the process of analyzing how information, particularly personally identifiable information, is collected, used, shared, and maintained within a system or project.

[b]See U.S. Department of Commerce Press Release: https://www.commerce.gov/news/press-releases/2025/06/statement-us-secretary-commerce-howard-lutnick-transforming-us-ai.

[c]Large language models use training data to learn patterns in written language.

[d]PETs are a collection of tools, techniques, and methods designed to protect individuals' personal information and ensure their privacy in digital environments.

[e]The Consumer Financial Protection Bureau may not continue to exist as an oversight entity for AI due to the agency being phased out.

[f]Metadata provide descriptive information about a dataset in a structured, machine-readable format. They describe aspects of the dataset—such as the source of the data and when it was last updated—in clearly delineated fields.

OMB's Government-wide Guidance Does Not Fully Address Privacy-Related Risks and Challenges when Using AI

As discussed previously, the experts in the roundtable identified 10 privacy risks and 13 challenges related to protecting privacy when using AI.[63] With regard to the expert-identified risks, OMB's AI-related guidance did not specify privacy-related risks that agencies should consider when updating their policies on IT infrastructure, data, cybersecurity, and privacy as they pertain to AI. Of the 10 relevant challenges, OMB's AI, data, and privacy-related government-wide guidance fully addressed two and partially addressed eight.[64]

OMB AI Guidance Does Not Provide Details on Potential Privacy-Related Risks

As noted previously, OMB serves as the primary agency for establishing and updating government-wide AI policy and guidance. In addition, OMB is responsible for assisting federal agencies on privacy matters, developing federal privacy policy, and overseeing implementation of privacy policy by agencies. OMB's guidance on AI,[65] M-25-21, includes a requirement that agencies revisit, and update where necessary, their internal policies on IT infrastructure, data, cybersecurity, and privacy as they pertain to AI by December 29, 2025. The memo also:

- directs agencies to implement certain risk management procedures for "high-impact" AI-use cases;[66]
- requires agencies to assess the potential impacts of using AI, supported by documentation, on the privacy, civil rights, and civil liberties of the public; and
- states that the use of AI can create, contribute to, and exacerbate risks because AI outputs may be inaccurate or misleading, among other things.

However, the guidance did not specify the types of privacy-related risks that agencies should consider when updating their policies. In the memo, OMB acknowledges this limitation while providing guidance related to understanding AI risk management. Specifically, M-25-21 identifies a list of factors that can create, contribute to, or exacerbate risks from the use of AI.

However, it states that the list does not include all risks associated with AI, such as risks related to privacy, among other things. We reached out to OMB to share our observations and whether OMB planned to release guidance that specified the types of privacy-related risks that agencies should consider when updating their AI-related policies. However, OMB did not provide any comments or additional documentation.

[63]For the purposes of our discussion, the term "risks" refers to the potential negative outcomes or specific threats to privacy that could arise from AI usage if not properly addressed (e.g., data breaches, misuse, bias). The term "challenges" refers to the difficulties or obstacles in the process of implementing and managing AI while mitigating privacy-related risks (e.g., regulatory compliance, transparency, data quality).

[64]We did not assess OMB against three of the expert-identified challenges because we determined that it is not reasonable to expect that these challenges would be discussed and addressed in OMB government-wide guidance. Specifically, we did not assess OMB's guidance for the following three expert-identified challenges: (1) gaps in AI and privacy-related laws, (2) limited time to implement new AI-related requirements into law, and (3) privacy skepticism.

[65]OMB, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, M-25-21.

[66]According to OMB, high-impact use cases include, among others, AI with an output that serves as a principal basis for decisions or actions with legal, material, binding, or significant effect on an individual or entity's civil rights, civil liberties, or privacy.

Highlighting the types of privacy-related risks that can occur when using AI could assist the agencies in updating their relevant policies. Although OMB and other entities have reported on standards and best practices to help entities mitigate the risks of traditional software or information-based systems, the risks posed by AI systems are in many ways unique. For example, NIST has reported that AI systems may be trained on data that can change over time, sometimes significantly and unexpectedly, affecting system functionality and trustworthiness in ways that are hard to understand. Further, AI systems and the contexts in which they are deployed are frequently complex, making it difficult to detect and respond to failures when they occur.

Accordingly, while not every risk will apply to each use of AI, highlighting the types of privacy-related risks that can occur when using AI, such as those identified by the expert roundtable, could provide valuable assistance to agencies. For example, it could help agencies identify privacy risks arising from specific uses of AI and inform related impact assessments, as well as steps to mitigate risks. The experts suggested that federal entities that have AI oversight-related responsibilities could create standardized ways to assess how AI systems handle personal data and their potential privacy risks, ensuring accountability and informed policymaking.

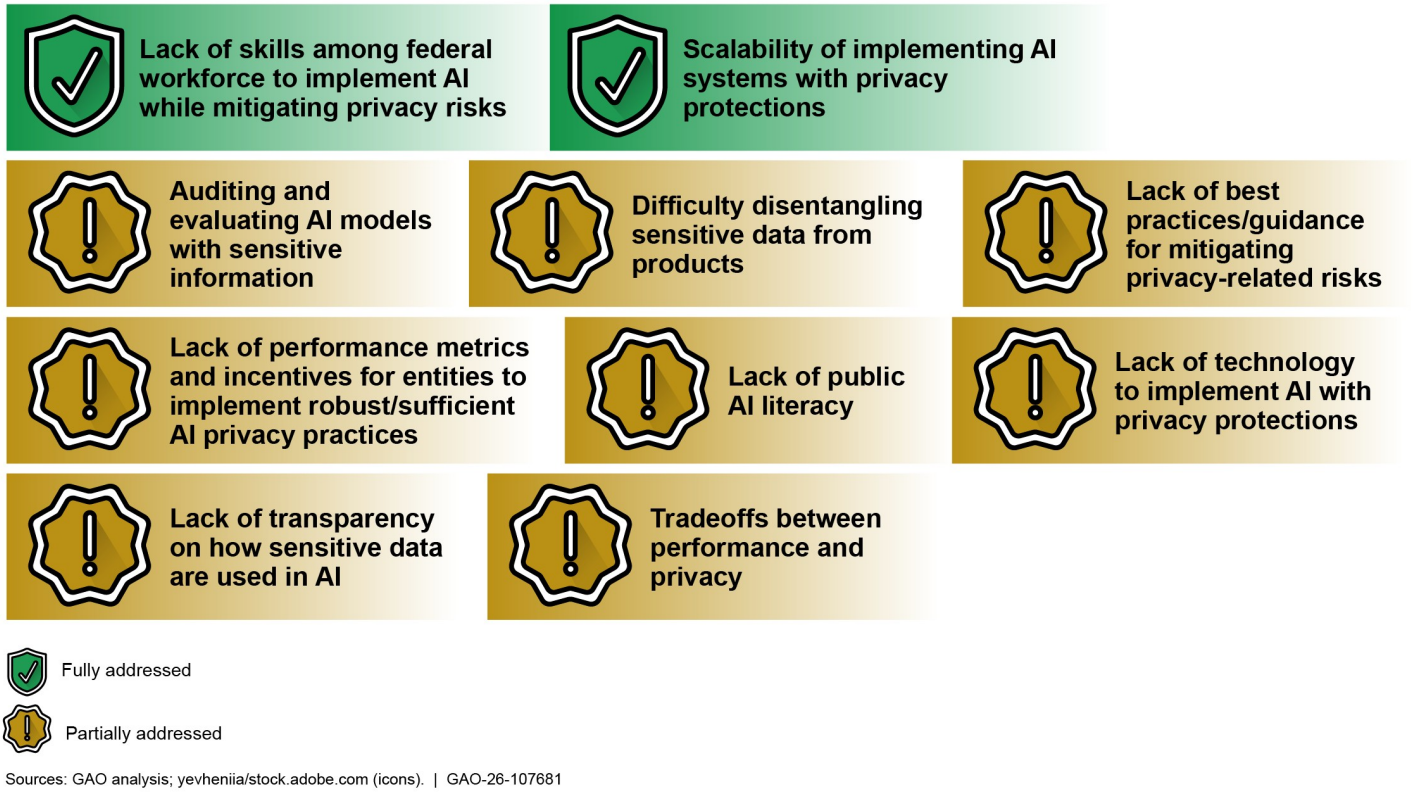
This type of information could be provided to agencies through existing channels that focus on addressing privacy-related risks and agencies use of AI, such as the Federal Privacy Council and Chief AI Officer Council. Such collaborative bodies could facilitate information sharing among agencies with different levels of experience and expertise in using AI. This is particularly important given that AI is still a new technology and agencies may be unfamiliar with the range of privacy risks that its use could introduce. Without additional information sharing, agencies may be unaware of the known privacy risks introduced by AI when assessing the impacts of its use and be hindered in implementing appropriate protections for sensitive data, including PII, when using AI.

OMB Guidance Fully Addressed Two Challenges Associated with Protecting Privacy and Partially Addressed Eight

Of the 10 relevant challenges, OMB's AI, data, and privacy-related government-wide guidance[67] fully addressed two and partially addressed eight (see figure 2).

[67]The OMB guidance documentation we assessed were (1) OMB, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust,* M-25-21, (2) OMB, *Driving Efficient Acquisition of Artificial Intelligence in Government,* M-25-22, (3) OMB, *Phase 2 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Open Government Data Access and Management Guidance,* M-25-05, (4) OMB, *Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance,* M-19-23, and (5) OMB, *Managing Information as a Strategic Resource,* Circular A-130.

Figure 2: Extent to Which the Office of Management and Budget's Government-wide Guidance Addressed 10 Selected Expert-identified Privacy-related Challenges When Using Artificial Intelligence (AI), as of January 2026



Sources: GAO analysis; yevheniia/stock.adobe.com (icons). | GAO-26-107681

Guidance Fully Addressed Two Privacy-Related Challenges

OMB's guidance fully addressed the following two expert-identified privacy-related challenges by providing agencies with direction or resources they can use to help ensure that they are mitigating privacy risks when using AI:[68]

- **Lack of skills among federal workforce to implement AI while mitigating privacy-related risks.** OMB M-25-21 states that the federal workforce has a responsibility to develop and maintain, at a minimum, foundational knowledge of how to use AI responsibly in performing their official duties. In addition, the memo states that agencies are strongly encouraged to prioritize recruiting, developing, and retaining technical talent in AI roles. The memo also states that agencies should leverage existing AI training programs and resources and develop additional technical training or resources, as needed, to increase practical, hands-on expertise with AI technologies. As discussed earlier, the AI Training Act required OMB, in coordination with GSA, to develop and implement an AI training program for the executive branch's acquisition workforce that includes information related to the risks posed by AI to privacy, among other

[68]We did not assess executive branch agencies other than OMB for this review. However, agencies' ability to implement OMB guidance and effectively address privacy challenges could be affected by available funding and resources, among other factors.

things. These efforts, if effectively implemented, should help ensure that agencies have the workforce necessary to implement privacy protections when using AI.[69]

- **Scalability of implementing AI systems with privacy protections.** OMB M-25-21 states that agencies should assess their AI maturity goals and accelerate and scale AI adoption, by appropriately resourcing areas such as data governance, IT, infrastructure, quality data assets, integration and interoperability, privacy, and security. In addition, the memo states that agencies are to utilize and scale existing tools, processes, and resources for AI whenever possible and invest in technical solutions to make compliance more efficient. The memo also states that agencies should focus their recruitment efforts on individuals that have demonstrated operational experience in designing, deploying, and scaling AI systems in high-impact environments. If effectively implemented, this guidance should better position agencies to implement AI at a scale that will work across multiple datasets and scenarios while also ensuring that appropriate privacy protections are in place.

Guidance Partially Addressed Eight Privacy-Related Challenges

OMB's existing government-wide guidance partially addressed eight expert-identified privacy-related challenges when using AI.

- **Auditing and evaluating AI models with sensitive information.** OMB M-25-21 provides some guidance to agencies on evaluating AI models. Specifically, the memo notes that agencies must develop pre-deployment testing and prepare risk mitigation plans that reflect expected real-world outcomes and identify expected benefits to the AI use. The memo further states if an agency does not have access to the underlying AI source code, models, or data, the agency must use alternative test methodologies, such as querying the AI service and observing the outputs or providing evaluation data to the vendor and obtaining results. Further, for high-impact uses of AI, agencies are required to complete AI impact assessments, which must address, among other elements, the quality and appropriateness of the relevant data and model capability and potential impacts of using the AI on the privacy, civil rights, and civil liberties of the public. The memo also notes that the risks of unintended disclosure differ by model and agencies should not assume that an AI model poses the same privacy and confidentiality risks as the data used to develop them.

  However, OMB's guidance does not provide specific information related to how to prevent the exposure of sensitive data when agencies are evaluating and auditing AI models. Experts in our panel noted that without using sensitive information, it can be difficult to evaluate the performance of a model.
- **Difficulty disentangling sensitive data from products.** OMB M-25-21 instructed agencies to assess their current state of AI maturity and develop plans and processes to ensure access to quality data for AI and data traceability. In this context, traceability refers to an agency's ability to track and internally audit

[69]We have recently reported that federal agencies face the challenge of hiring and developing an AI workforce for using and man aging generative AI. Specifically, six selected agencies reported challenges in attracting and developing individuals with expertise in generative AI. These agencies can also be affected by competition with the private sector for similarly skilled professionals. Furthermore, these agencies also reported difficulties in establishing and providing ongoing education and technical skill d evelopment of their current workforce. These agencies cited various constraints, such as the need for resources to establish training programs and maintaining training content as the technology rapidly evolves. See GAO, *Artificial Intelligence: Generative AI Use and Management at Federal Agencies*, GAO-25-107653 (Washington, D.C.: July 29, 2025). In addition to OMB's guidance, the experts noted that meeting this challenge could also require resources to hire AI and privacy experts.

datasets used for AI, and where relevant, key metadata.[70] Further, the memo states that agencies should develop adequate infrastructure and capacity to sufficiently share, curate, and govern agency data for use in training, testing, and operating AI. Requiring agencies to assess the quality and traceability of the data they are using should help them better identify and track sensitive data in their AI applications.

However, OMB's guidance does not provide specific information related to how agencies can store the data they are using in AI so that sensitive data can be separated from the dataset. For example, the guidance does not discuss the need to segment or isolate sensitive data used in AI applications so that it is not vulnerable to unauthorized access.

- **Lack of best practices/guidance for mitigating privacy-related risks.** OMB M-25-22 includes a requirement for agencies to establish policies and processes to protect privacy.[71] Specifically, the memo requires agencies to establish policies and processes, including contractual terms and conditions, that ensure compliance with privacy requirements in law and policy whenever agencies acquire an AI system or service. This also applies if an agency contractor uses an AI system or service that will create, collect, use, process, store, maintain, disseminate, disclose, or dispose of federal information containing PII. Additionally, the memo states that agencies shall ensure that their senior agency officials for privacy have early and ongoing involvement in agency acquisition or contractor use of AI involving PII, including during pre-solicitation acquisition planning and when defining requirements, to manage privacy risks and ensure compliance with law and policy related to privacy.

  However, OMB has not yet issued AI-related government-wide guidance that establishes clear rules, norms, or best practices with respect to privacy for agencies that are developing AI solutions internally.

- **Lack of performance metrics and incentives for entities to implement robust/sufficient AI privacy practices.** OMB M-25-21 encourages agencies, where practicable, to better track and evaluate performance of their procured AI. Further, the guidance states that agencies should consider contractual terms that prioritize the continuous improvement, performance monitoring, and effectiveness of procured AI, among other things. In addition, OMB M-25-22 on *Driving Efficient Acquisition of Artificial Intelligence in Government* states that agencies shall establish policies and processes, including contractual terms and conditions, that ensure compliance with privacy requirements in law and policy whenever agencies acquire an AI system or service, or an agency contractor uses an AI system or service, involving federal information containing PII. The memo also notes that agencies can establish contract incentives based on metrics to improve the performance and interoperability of AI systems and services.

  However, OMB's guidance does not identify performance measures specific to addressing privacy-related risks when using AI. This includes standardized metrics for AI privacy impacts that agencies could use to assess performance and establish contractual requirements.

- **Lack of public AI literacy.** As discussed earlier, OMB M-25-21 identified guidance related to improving the federal workforce's AI literacy. In addition, to ensure accountability to the taxpayer, the memo states that agency AI strategies, which needed to be publicly released by September 30, 2025, should be understandable, accessible to the public, and transparent about how the agencies' investments in AI

[70]Metadata provide descriptive information about a dataset in a structured, machine-readable format. They describe aspects of the dataset—such as the source of the data and when it was last updated—in clearly delineated fields.

[71]OMB M-25-22 also refers agencies to the privacy-related requirements established in OMB Circular A-130 on *Managing Information as a Strategic Resource*.

innovation benefit the American people.[72]

However, while these strategies could increase the public's understanding of how the agencies' use of AI will benefit them, OMB's guidance does not explicitly require agencies to include specific privacy-related details related to AI's limitations and risks.

In addition, OMB's guidance does not discuss how agencies can establish new or update existing processes to ensure that individuals who interact with their AI technologies understand what they are consenting to. For example, the guidance does not (1) explicitly require agencies to include in their AI strategies specific privacy-related details related to AI's limitations and risks or (2) discuss how agencies can establish new or update existing processes to ensure that individuals who interact with their AI technologies understand what they are consenting to.

- **Lack of technology to implement AI with privacy protections.** OMB M-25-21 instructs agencies to assess their current state of AI maturity and develop plans and processes to develop AI-enabling infrastructure across the lifecycle including development, testing, deployment, and continuous monitoring. In addition, the memo states that agencies should ensure that AI developers have access to adequate IT infrastructure, including high-performance computing infrastructure specialized for AI training and inference, where necessary. Further, it states that agencies should ensure that AI developers have access to the software tools, open-source libraries, and deployment and monitoring capabilities necessary to rapidly develop, test, and maintain AI applications. Such steps could assist agencies in ensuring that they have the tools and infrastructure to implement AI with appropriate privacy protections in place.

  However, OMB M-25-21 does not provide guidance related to tools agencies can use to protect sensitive data when using AI. For example, as discussed earlier, the experts identified using PETs, such as differential privacy, to help protect sensitive data when using AI, but OMB's guidance did not specify any differential privacy tools that agencies could use.

- **Lack of transparency on how sensitive data are used in AI.** As discussed earlier, OMB M-25-21 states that, by September 30, 2025, agencies must have developed an AI strategy for identifying and removing barriers to their responsible use of AI. The memo states that the strategies should be understandable, accessible to the public, and transparent about how their investments in AI will benefit the American public. In addition, the memo states that the strategies should explain how the agency plans to develop the necessary operations, governance, and infrastructure to manage risks from the use of AI, including risks related to information security and privacy. The memo also requires agencies to make the AI strategies that they subsequently develop publicly available on the agency's website.[73]

  However, OMB's guidance does not provide information related to how agencies should conduct PIAs to

[72]The agencies have begun to make these strategies publicly available. For example, see Social Security Administration, *Social Security Administration Enterprise Artificial Intelligence Strategy: Empowering SSA's Mission with Artificial Intelligence* (Sept. 2025) at https://www.ssa.gov/ai/policy/SSA%20Enterprise%20Artificial%20Intelligence%20Strategy%20Report.pdf and Department of Homeland Security, *Department of Homeland Security Artificial Intelligence (AI) Strategy (Sept. 2025)* at https://www.dhs.gov/sites/default/files/2025-09/25_0926_cio_dhs_ai_strategy_for_omb_m-25-21_508.pdf.

[73]As discussed earlier, the agencies have begun to make these strategies publicly available.

ensure privacy-related risks arising from the use of AI are considered.[74] PIAs can be a critical tool for providing an increased level of transparency and accountability regarding specific uses of AI involving PII and how they are mitigating any associated privacy risks. While agencies' AI strategies may provide general information on how they are addressing privacy risks related to AI, PIAs provide more specific information about the risks and mitigation steps associated with particular IT systems, including AI applications.

- **Tradeoffs between performance and privacy.** OMB M-25-21 encourages agencies, where practicable, to better track and evaluate performance of their procured AI by conducting ongoing testing and validation on AI model performance, the effectiveness of vendor AI offerings, the associated risk management measures agencies are taking, and testing their AI in real-world conditions. In addition, OMB M-25-22 states that agencies are strongly encouraged to use performance-based techniques, such as performance work statements and quality assurance surveillance plans, to identify requirements and contract terms. M-25-22 also states these performance-based requirements allow agencies to understand and assess vendor claims about their proposed use of AI systems or services prior to contract award, acquire AI capabilities that address their needs, and perform post-award monitoring. This could provide agencies a more informed view of the performance of AI tools and, potentially, how to assess potential tradeoffs between performance and certain risks, such as those related to privacy.

  However, OMB's guidance does not specifically discuss the potential tradeoffs between privacy and performance. For example, it does not address factors agencies should consider when assessing the impact on performance of implementing privacy protections.

We reached out to OMB to share our observations on the extent to which its guidance addressed these eight challenges and to get the office's perspective on why these challenges were not addressed. However, OMB did not provide any comments or additional documentation. Without additional information or direction on addressing these challenges, agencies will be hindered in protecting privacy when using AI, as well as making the public aware of the associated risks and steps they are taking them to mitigate them. Such information sharing could be facilitated through a variety of mechanisms, including new or updated guidance, information sharing among interagency forums such as the Chief AI Officer Council or the Federal Privacy Council, or training such as that required by the AI Training Act.[75]

Conclusions

AI is a fast-evolving and extremely transformative technology with the potential to change how government does business and improve many aspects of daily life for the American public. Notwithstanding AI's potential positive effects, the use of AI can introduce and even heighten privacy-related risks. Such risks can negatively impact the public should federal agencies not take steps to implement privacy protections.

[74]In January 2024, OMB issued a request for information on how PIAs could be more effective at mitigating privacy risks related to AI. In November 2024, OMB officials stated they had reviewed the public comments received, but did not yet have a plan to issue new PIA guidance. They stated that before considering any changes to guidance, they planned to conduct additional research, conduct further engagement with agencies, and consider the full range of feedback received from all stakeholders. However, as of January 2026, OMB had not provided further updates on the status of this new guidance.

[75]As discussed earlier, the AI Training Act was enacted to ensure that the acquisition workforce of executive agencies has knowledge of the capabilities and risks associated with AI. It includes a requirement for OMB, in coordination with GSA, to develop and implement an AI training program for the executive branch's acquisition workforce that includes information related to the risks posed by AI to privacy, among other things.

This concern was echoed by the experts who participated in our roundtable discussion. These experts emphasized risks related to protecting privacy when using AI, such as potential invasions of privacy, and discussed the challenges related to protecting privacy, including gaps in AI and privacy-related laws. The experts also identified actions the federal government can take and solutions to mitigate these privacy-related risks and challenges.

Given the government's growing use of AI, it is essential that OMB provides agencies with guidance related to the risks and challenges associated with protecting privacy when using AI. To its credit, OMB has issued government-wide guidance addressing some of the expert-identified, privacy-related risks and challenges. However, OMB can assist agencies further by specifying the types of privacy-related risks that agencies should consider when updating their AI-related policies. OMB can also utilize existing AI and privacy channels to provide more details about known privacy risks to ensure agencies are appropriately considering what privacy protections they should implement when using AI. Without providing this additional information, agencies are at risk of potentially exposing sensitive information that can negatively impact the public, among other things.

Recommendations for Executive Action

We are making two recommendations to OMB:

- The Director of OMB should specify examples of known privacy-related risks that agencies should consider when updating their policies as they pertain to AI. (Recommendation 1)
- The Director of OMB should facilitate additional information sharing or issue government-wide guidance related to:
    - how agencies should consider privacy when evaluating and auditing AI models that contain sensitive information;
    - storing data in a manner where sensitive data can be separated from the dataset;
    - clear rules, norms, and best practices with respect to privacy that agencies should use when developing AI solutions internally;
    - performance metrics agencies can use to assess privacy-related impacts when using AI;
    - actions agencies can take to ensure that members of the public who interact with their AI technologies understand what they are consenting to;
    - technological tools agencies can use to protect sensitive data when using AI;
    - incorporating AI-specific considerations into privacy impact assessments, including identifying risks and informing the public about how PII is involved in the use of AI; and
    - potential tradeoffs between privacy and performance agencies can consider when using AI. (Recommendation 2)

Agency Comments

We provided a draft of this report to OMB, the Department of Commerce, and NSF for their review and comment. OMB did not provide comments, and the Department of Commerce and NSF stated that they had no comments.

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

If you or your staff have any questions about this report, please contact me at (202) 512-5017 or cruzcainm@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.

//SIGNED//

Marisol Cruz Cain
Director, Information Technology and Cybersecurity

List of Addressees

The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Frank Pallone, Jr.
Ranking Member
Committee on Energy and Commerce
House of Representatives

The Honorable Robert Garcia
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Martin Heinrich
United States Senate

The Honorable Ron Wyden
United States Senate

The Honorable Lori Trahan
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe the risks and challenges associated with protecting privacy when using artificial intelligence (AI), and (2) examine the extent to which the Office of Management and Budget (OMB) had addressed privacy-related risks and challenges associated with AI in government-wide guidance. To address these objectives, we used a variety of approaches, including an expert panel discussion, analyses of the panel discussion to compile the key statements provided by the selected experts, analyses of OMB's existing AI, data, and privacy related guidance, a review of selected agencies' documentation, and interviews with selected federal agency officials.

Expert Panel Discussion

Expert Selection

To select the experts for the panel discussions to address the first objective, we followed a multi-step process. To generate a list of potential participants, we (1) reviewed a list of experts that had been developed to support a generative AI product we issued in June 2024;[1] (2) identified experts from previously held AI-related expert panels and forums; and (3) consulted with internal stakeholders to identify additional AI or privacy-related experts that we should consider for the panel.

Once we compiled the expert list, we reviewed each expert's current and past work to assign them to one of the following three areas of expertise:

- technological development and advancement of strategies and tools to protect personal identifiable information (PII) data when using AI applications;
- management and/or use of AI applications that use PII data; and
- development and/or input on AI or privacy specific policies, regulations, and laws that address privacy risks associated with AI and the steps organizations should take to address those risks.

If an expert could be associated with more than one area of expertise, we used our professional judgment to associate that expert with the area of expertise that we believed their work and opinions would be most closely associated with.

After we associated every potential expert to a single area of expertise, we assigned each expert to one of the following affiliation categories, based on the institutional affiliation of their current job or research position: (1) federal agencies; (2) academics researching work related to addressing privacy risks associated with AI; (3) nongovernmental organizations, including think tanks, nonprofits, and advocacy groups; and (4) private industry. If an expert had more than one affiliation, we used our professional judgment to determine their current and most relevant affiliation. In addition, we considered each expert for the panel if they held the relevant position within one calendar year from the date of our planned panel, which occurred in January 2025.

[1]See GAO, *Artificial Intelligence: Generative AI Technologies and Their Commercial Applications*, GAO-24-106946 (Washington, D.C.: June 20, 2024). In addition, for this list, we only considered the experts that also had privacy-related experience.

To ensure a balanced distribution, we selected three experts from each of the four affiliation categories for each of the three areas of expertise. This resulted in a total of 12 experts planned for the panel. Further, to ensure a sufficient range and balance of the expert's opinions on this topic area, we also considered the gender of the experts. Table 4 provides the final list of experts we selected.

Table 4: List of Expert Participants in GAO's Panel on Privacy Risks Associated with Artificial Intelligence (AI), Held January 13–15, 2025

Expert	Institutional affiliation at time of GAO expert selection
Mackenzie J. Arnold	Director of U.S. Policy Institute For Law & AI
Rumman Chowdhury, Ph.D.	Co-Founder Humane Intelligence
Barbara Cosgrove	Vice President, Chief Privacy and Trust Officer Workday, Inc.
Michelle Finneran Dennedy	Founder, Chief Executive Officer PrivacyCode, Inc.
Dominique Duval-Diop, Ph.D.	Deputy Chief Data Officer U.S. Department of Commerce, Office of the Undersecretary of Economic Affairs
Cynthia Dwork	Gordon McKay Professor of Computer Science at the Harvard Paulson School of Engineering Harvard University
A. Michael Froomkin	Laurie Silvers & Mitchell Rubenstein Distinguished Professor of Law Member University of Miami Institute for Data Science & Computing
Jennifer King, Ph.D.	Privacy and Data Policy Fellow Stanford Institute for Human-Centered Artificial Intelligence
Deirdre Kathleen Mulligan	Principal Deputy Chief Technology Officer White House Office of Science and Technology Policy
Timothy R. Noonan	Deputy Director for Health Information Privacy, Data, & Cybersecurity U.S. Department of Health and Human Services, Office for Civil Rights
Jeramie D. Scott	Senior Counsel and Director for Project on Surveillance Oversight Electronic Privacy Information Center
Heather West	Senior Director of Cybersecurity and Privacy Services Venable

Legend: Ph.D. = doctor of philosophy

Source: GAO. | GAO-26-107681

To help identify any potential biases or conflicts of interest, before finalizing the participation of experts, we asked each expert who participated in the panel to disclose whether they had investments, sources of earned income, organizational positions, relationships, or other circumstances that could affect, or could be viewed to affect, their statements during the panel. None of the experts reported potential conflicts that would affect their ability to participate in the panel.

Panel Discussion

In January 2025, we convened a 3-day virtual panel of 12 experts from a variety of fields and affiliations to discuss risks to privacy when using AI and challenges associated with ensuring the implementation of

adequate privacy protections when using AI. Specifically, we asked a series of questions aimed at identifying privacy risks and challenges when using AI that could affect private and public sector organizations, including federal agencies.

The panel discussions, including the responses provided via the video software's chat function, were recorded and transcribed to ensure that we accurately captured experts' statements. Further, to ensure accuracy, a GAO analyst reviewed each of the transcripts to update and eliminate any errors by comparing the transcription to the audio recording. A second GAO analyst then reviewed each updated transcript to validate the changes made to address the inaccuracies.

We then analyzed the panel transcripts to develop non-exhaustive lists regarding (1) risks and challenges associated with protecting privacy when using AI; (2) ways the federal government can help protect privacy when working with AI; and (3) other actions and technical solutions that are available to address privacy-related risks and challenges when using AI.[2]

To stimulate discussion and provide a common ground on the key terms used for the discussion on privacy-related risks and challenges associated with AI, we provided our experts with a list of key definitions in advance of the panel. These include the two key definitions that we use throughout the report:

- The term "risks" refers to the potential negative outcomes or specific threats to privacy that could arise from AI usage if not properly addressed (e.g., data breaches, misuse, bias).
- The term "challenges" refers to the difficulties or obstacles in the process of implementing and managing AI while mitigating privacy-related risks (e.g., regulatory compliance, transparency, data quality).

Analyses of OMB's AI, Data, and Privacy-Related Guidance

To address the second objective, we reviewed OMB's AI-related guidance to determine if it highlighted specific types of privacy risks similar to those identified by the experts during our January 2025 panel discussion. We also compared OMB government-wide guidance related to AI, data, and privacy to selected challenges associated with protecting privacy when using AI, as identified by our selected experts during the January 2025 panel discussion.

As discussed earlier, the experts identified a total of 13 challenges related to protecting privacy when using AI. From these 13 expert-identified challenges, we excluded three challenges because it is not reasonable to expect that they would be discussed and addressed in OMB government-wide guidance. For example, although OMB provides legislative proposals to Congress, OMB does not have authority to enact or amend federal statutes related to AI or privacy.[3] Table 5 identifies the 10 selected expert-identified challenges and associated descriptions.

[2]The comments provided by the experts reflected their own views and not those of the organizations with which they are affiliated. Further, the experts' views may not correspond with those of others with similar backgrounds and expertise.

[3]The three expert-identified challenges that we excluded from our OMB analyses were: (1) gaps in AI and privacy-related laws, (2) limited time to implement new AI-related requirements into law, and (3) privacy skepticism.

Table 5: Ten Selected Expert-identified Privacy-related Challenges When Using Artificial Intelligence (AI)

Challenge	Associated description
Auditing and evaluating AI models with sensitive information	Evaluating AI models without collecting and potentially exposing sensitive information can be difficult.
Difficulty disentangling sensitive data from products	Models, systems, and/or integrated products may have data stored in a way that cannot easily be segmented, making it hard to separate sensitive data from the entire dataset. This means using these products without the risk of sensitive data being exposed or used in ways that are not intended may be difficult.
Lack of best practices/guidance for mitigating privacy-related risks	There is a lack of clear rules, norms, and best practices related to privacy both at broad and sectoral levels as they apply to AI. As a result, entities do not fully understand which privacy-related guidance applies for their respective sectors/areas when using AI.
Lack of performance metrics and incentives for entities to implement robust/sufficient AI privacy practices	Without proper performance metrics and incentives, organizations may not be able to gauge the impact of AI on privacy or the effectiveness of privacy measures.
Lack of public AI literacy	There is a lack of understanding among the public on AI, leading to a lack of understanding of what they are consenting to.
Lack of skills among federal workforce to implement AI while mitigating privacy-related risks	Federal agencies struggle to hire new staff and/or train existing staff to ensure they have sufficient knowledge on AI and privacy to implement AI while mitigating privacy-related risks.
Lack of technology to implement AI with privacy protections	Organizations may lack the access to tools that could be used to protect sensitive data when using AI.
Lack of transparency on how sensitive data are used in AI	Organizations do not always inform the public about how their data are used in AI models and algorithms. As a result, members of the public may face difficulties in pursuing their rights or interests. Further, for federal agencies, there is uncertainty related to the type of public engagement required to conduct privacy impact assessments for their information systems that use AI. As a result, agencies may conduct privacy impact assessments inconsistently and could potentially implement AI technology prior to addressing privacy-related issues.
Scalability of implementing AI systems with privacy protections	Organizations may have difficulty implementing AI systems, while mitigating privacy-related risks, at a scale that will work across multiple different datasets and scenarios.
Tradeoffs between performance and privacy	Adjusting/removing certain data for the sake of privacy, specifically in most significant contexts, can result in a consequential performance tradeoff.

Source: GAO analysis of comments from subject matter experts. | GAO-26-107681

To determine the extent to which OMB had addressed these 10 challenges, we focused our analysis to five OMB guidance documents because they included AI, data, and privacy-related requirements that were applicable for federal agencies. As context, in January 2025, the White House issued Executive Order 14179 on *Removing Barriers to American Leadership in Artificial Intelligence*, which instructed OMB to review and revise OMB memorandums M-24-10 and M-24-18.

In April 2025, OMB issued two new AI-related memorandums (see below) and they included additional requirements for federal agencies that impacted our engagement scope. Accordingly, we focused our review on these two new AI-related memorandums that had been issued by the current administration as well as three additional applicable OMB guidance documents that were referenced in these two memorandums.[4] This limited our analyses to the following OMB guidance:

[4]These memorandums identified additional OMB AI-related guidance. However, we excluded guidance that was not applicable for AI applications developed and deployed outside of the federal government, such as OMB Memorandum M-21-06 on *Guidance for Regulation of Artificial Intelligence Applications* (Washington, D.C.: Nov. 17, 2020).

- OMB Circular No. A-130 on *Managing Information as a Strategic Resource*; [5]
- OMB Memorandum M-19-23 on *Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance*;[6]
- OMB Memorandum M-25-05 on *Phase 2 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Open Government Data Access and Management Guidance*;[7]
- OMB Memorandum M-25-21 on *Accelerating Federal Use of AI through Innovation, Government, and Public Trust*;[8] and
- OMB Memorandum M-25-22 on *Driving Efficient Acquisition of Artificial Intelligence in Government*.[9]

To confirm that each of these challenges were not addressed in any other existing OMB guidance, we provided OMB with our preliminary assessments to give the office an opportunity to explain how each of these challenges were addressed in its existing guidance. As of January 2026, OMB has not identified any other AI, data, or privacy-related guidance documentation that addresses the challenges.

Further, we assessed OMB's government-wide guidance for each of the 10 challenges as:

- **fully addressed** if the guidance addressed all components of the identified challenge;
- **partially addressed** if the guidance addressed some aspects of the identified challenge, but not all aspects; and
- **not addressed** if the guidance did not address any component of the identified challenge.

In addition, we also had two GAO analysts review the related OMB guidance to obtain agreement on the assessment ratings we identified for each challenge.

Lastly, as part of our analysis, we assessed the OMB guidance to determine if it provided agencies with direction or resources they could use to mitigate privacy risks when using AI. We also determined how OMB externally communicates information related to addressing the challenges associated with protecting privacy when using AI.

Review of Agency Documentation and Interviews

We reviewed agency documentation and interviewed agency officials from the Department of Commerce, the National Science Foundation, and OMB to obtain information related to the steps they had taken to address privacy considerations in AI. When we initiated this engagement in July 2024, we planned to assess actions these agencies had taken to meet requirements in Executive Order 14110 on the *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*.

[5]OMB, *Managing Information as a Strategic Resource,* Circular A-130.

[6]OMB, *Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance*, M-19-23.

[7]OMB, *Phase 2 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Open Government Data Access and Management Guidance,* M-25-05.

[8]OMB, *Accelerating Federal Use of AI through Innovation, Government, and Public Trust*, M-25-21.

[9]OMB, *Driving Efficient Acquisition of Artificial Intelligence in Government*, M-25-22.

Although Executive Order 14110 was rescinded in January 2025, each of the three agencies had already taken actions to address their respective requirements. These actions remain relevant to how the federal government is going to manage privacy-related risks when using AI. As such, we describe the actions these agencies took in the background section of this report. We also interviewed OMB officials further to obtain additional information on whether they believe their existing (or planned) guidance address the selected expert-identified challenges.

We conducted this performance audit from July 2024 to March 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Marisol Cruz Cain, at CruzCainM@gao.gov

Staff Acknowledgments

In addition to the contact named above, Lee McCracken (Assistant Director), Javier Irizarry (Analyst-In-Charge), Lamis Alabed, John Bornmann, Christopher Businsky, Quade Bywater, Jillian Clouse, Kara Lovett Epperson, Elizabeth Harris, Tyler Mountjoy, Sarah Ong, Scott Pettis, Zsaroq Powe, Brandon Sanders, Andrew Stavisky, Umesh Thakkar, Jonathan Wall, and Marshall Williams, Jr. made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube.
Subscribe to our 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

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us