



September 2022

PRIVACY

Dedicated Leadership Can Improve Programs and Address Challenges

GAO Highlights

Highlights of [GAO-22-105065](#), a report to congressional requesters

Why GAO Did This Study

The protection of personal privacy has become a more significant issue in recent years with the advent of new technologies and the proliferation of personal information. Federal agencies collect and process large amounts of PII for various government programs. Accordingly, they must ensure that any PII they collect, store, or process is protected from unauthorized access, tampering, or loss.

Federal agencies are required to establish privacy programs for the protection of PII that they collect and process. Among other things, this includes designating a senior agency official for privacy with overall responsibility for the agency's privacy program. In addition, agencies are to conduct privacy impact assessments to analyze how personal information is collected, stored, shared, and managed in a federal system.

GAO was asked to review federal agencies' privacy programs. This report examines (1) the extent to which agencies have established programs for ensuring privacy protections; (2) challenges agencies reported experiencing in implementing their privacy programs; (3) reported benefits and limitations in agencies' use of privacy impact assessments; and (4) the extent to which agencies have senior leadership dedicated to privacy issues.

View [GAO-22-105065](#). For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov, or Marisol Cruz Cain at (202) 512-5017 or cruzainm@gao.gov.

September 2022

PRIVACY

Dedicated Leadership Can Improve Programs and Address Challenges

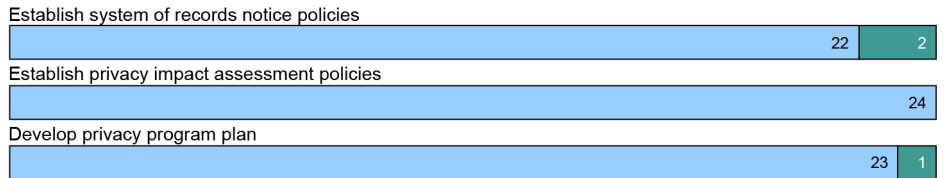
What GAO Found

The 24 Chief Financial Officer (CFO) Act of 1990 agencies varied in the extent to which they addressed key practices for implementing privacy programs:

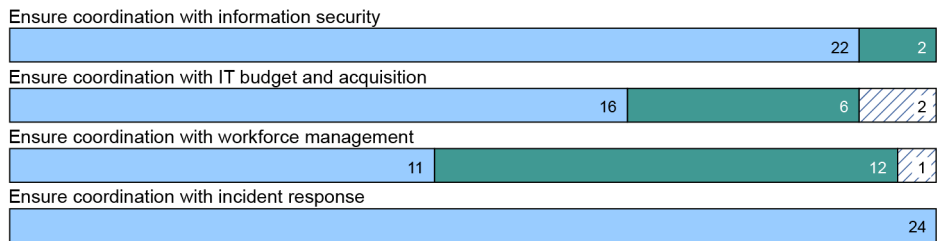
- Agencies generally established policies and procedures for key privacy activities. These included developing system of records notices, to identify personal data collected and how they are used; conducting privacy impact assessments; and documenting privacy program plans.
- Agencies varied in establishing policies and procedures for coordination between privacy programs and other agency activities, such as information security, budget and acquisition, workforce planning, and incident response.
- Many agencies did not fully incorporate privacy into their risk management strategies, provide for privacy officials' input into the authorization of systems containing personally identifiable information (PII), and develop a privacy continuous monitoring strategy.

Extent to Which 24 Chief Financial Officers Act of 1990 Agencies Addressed Key Practices for Establishing a Privacy Program

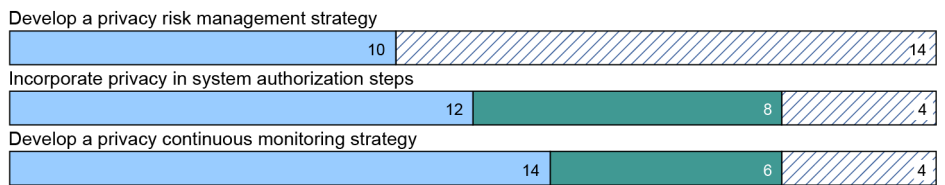
Privacy compliance activities



Coordination between privacy and other programs or functions

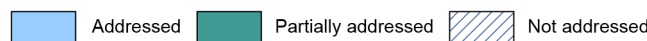


Risk management framework to manage privacy risks



0 6 12 18 24

Number of agencies



Source: GAO analysis of agency information. | GAO-22-105065

Without fully establishing these elements of their privacy programs, agencies have less assurance that they are consistently implementing privacy protections.

To do so, GAO compared policies and procedures at the 24 CFO Act agencies to key practices for establishing privacy programs. These practices included privacy compliance activities, coordination between privacy and other agency programs or functions, and activities to manage privacy risks.

In addition, GAO surveyed the 24 agencies on benefits and limitations of privacy impact assessments, and on challenges in implementing their privacy programs. GAO also interviewed privacy experts, relevant agency officials, and staff at OMB's privacy branch.

What GAO Recommends

GAO is recommending one matter for congressional consideration, that Congress consider legislation to designate a dedicated, senior-level privacy official at agencies that currently lack one. GAO is also making two recommendations to OMB to facilitate information sharing to help agencies address selected challenges and better implement privacy impact assessments.

Finally, GAO is making 62 recommendations to selected agencies to fully implement key practices for their privacy programs. This includes fully establishing policies and procedures for coordination between privacy programs and other agency functions and incorporating privacy into risk management activities.

Twenty agencies, including OMB, agreed with the recommendations, and several described planned actions to implement them. One agency did not explicitly state whether it agreed with the recommendations, but generally agreed with the report. One agency disagreed with the recommendations, while another disagreed with some recommendations and partially agreed with others. Two agencies stated that they had no comments on the report. GAO continues to believe all of its recommendations are warranted.

Agencies most frequently cited the following challenges in implementing their privacy programs (see table). Additional information sharing could help agencies address selected challenges.

24 Chief Financial Officer Act of 1990 Agency Challenges in Implementing Privacy Programs

Challenge	Number of agencies reporting challenge
Having sufficient resources	21
Applying privacy requirements to new technologies	20
Hiring privacy personnel	17
Integrating privacy and security controls	16
Coordinating with other agency offices and programs	15
Ensuring agency programs are implementing privacy requirements	15
Retaining privacy personnel	15
Training privacy professionals	14

Source: GAO analysis of agency data. | GAO-22-105065

Agencies and privacy experts identified benefits of privacy impact assessments, including providing public information and managing risks. However, they also identified factors that can limit the assessments' effectiveness. These include agencies not always initiating privacy impact assessments early enough to affect program decisions; privacy programs not aware of all agency systems with PII; and privacy programs unable to hold agency staff accountable for developing privacy impact assessments.

Addressing key privacy program practices, program challenges, and privacy impact assessment effectiveness requires significant leadership commitment at agencies. In accordance with Office of Management and Budget (OMB) guidance, the 24 agencies have each designated a senior agency official for privacy. However, most of these officials do not have privacy as their primary responsibility and have numerous other duties relating to, for example, managing IT and information security. Officials with primary duties other than privacy are unlikely to spend a majority of their time focused on privacy, and agencies generally delegated operational aspects of their privacy programs to less-senior officials. This makes it less likely that the senior agency officials for privacy will focus their attention on privacy in discussions with other senior agency leaders.

The shortcomings in agency policies and challenges they reported could be better addressed by a senior-level official with privacy as a primary area of responsibility. In particular, such an official could be better positioned to ensure a consistent focus on privacy at the level of senior leadership, facilitate cross-agency coordination, and elevate the importance of privacy. OMB privacy staff stated that they believed codifying a dedicated senior privacy official in statute would strengthen agency programs and better enable them to address challenges. In addition, several agency officials and privacy experts noted that a senior agency leader dedicated to privacy could better ensure cross-agency coordination and elevate the importance of privacy. Establishing such a position in law could enhance the leadership commitment needed to give attention to privacy issues across the government.

Contents

Letter		1
	Background	4
	Gaps Exist in Agency Policies for Ensuring Privacy Protections	15
	Agencies Identified Various Challenges Facing Their Privacy Programs	28
	Agencies and Experts Identified Benefits and Limitations of Privacy Impact Assessments	37
	Most Senior Agency Privacy Officials Do Not Have Privacy as Their Primary Assigned Duty	45
	Conclusions	49
	Matter for Congressional Consideration	50
	Recommendations for Executive Action	50
	Agency Comments and Our Evaluation	51
Appendix I	Objectives, Scope, and Methodology	61
Appendix II	Recommendations to Departments and Agencies	66
Appendix III	Details on the Extent to Which the 24 Chief Financial Officers Act Agencies Addressed Key Privacy Practices in Policies and Procedures	75
Appendix IV	Survey Administered to the 24 Chief Financial Officers Act Agencies	79
Appendix V	Comments from the Department of Commerce	91
Appendix VI	Comments from the Department of Defense	92
Appendix VII	Comments from the Department of Education	94

Appendix VIII	Comments from the Department of Energy	96
Appendix IX	Comments from the Department of Health and Human Services	99
Appendix X	Comments from the Department of Homeland Security	101
Appendix XI	Comments from the Department of the Interior	106
Appendix XII	Comments from the Department of State	107
Appendix XIII	Comments from the Department of Veterans Affairs	109
Appendix XIV	Comments from the Environmental Protection Agency	111
Appendix XV	Comments from the General Services Administration	113
Appendix XVI	Comments from the National Aeronautics and Space Administration	115
Appendix XVII	Comments from the Nuclear Regulatory Commission	117
Appendix XVIII	Comments from the Small Business Administration	119
Appendix XIX	Comments from the Social Security Administration	121

Appendix XX	Comments from the U.S. Agency for International Development	122
Appendix XXI	Comments from the Office of Personnel Management	125
Appendix XXII	GAO Contacts and Staff Acknowledgments	130

Tables

Table 1: Key Practices for Establishing a Program for Ensuring Privacy Protections	10
Table 2: Officials and Offices with Overall Privacy Responsibilities at the 24 Chief Financial Officers Act of 1990 Agencies	17
Table 3: Extent to Which the 24 Chief Financial Officers Act Agencies Addressed Key Privacy Compliance Activities	75
Table 4: Extent to Which the 24 Chief Financial Officers Act Agencies Addressed Key Privacy Coordination Activities	76
Table 5: Extent to Which the 24 Chief Financial Officers Act Agencies Addressed Key Privacy Risk Management Activities	77

Figures

Figure 1: Extent to Which the 24 Chief Financial Officers Act of 1990 Agencies Addressed Key Practices for Establishing a Privacy Program	20
Figure 2: Number of 24 Chief Financial Officers Act of 1990 Agencies Reporting Challenges in Implementing Privacy Programs	29
Figure 3: Number of the 24 Chief Financial Officers Act of 1990 Agencies Reporting that Privacy Impact Assessments Were Generally Beneficial	39

Abbreviations

CFO Act	Chief Financial Officers Act of 1990
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
DOT	Department of Transportation
EPA	Environmental Protection Agency
FISMA	Federal Information Security Modernization Act of 2014
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OCIO	Office of the CIO
OIRA	Office of Information and Regulatory Affairs
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIA	privacy impact assessment
PII	personally identifiable information
SAOP	senior agency official for privacy
SBA	Small Business Administration
SORN	system of records notice
SP	special publication
SSA	Social Security Administration
USAID	U.S. Agency for International Development
USDA	Department of Agriculture
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



September 22, 2022

Congressional Requesters

Federal agencies collect and process large amounts of personally identifiable information (PII) that is used for various government programs. 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. Federal agencies may collect PII to determine eligibility for participating in certain programs or receiving benefits, such as health insurance or student loans. Agencies may also collect PII during law enforcement investigations or for research or statistical purposes. Protecting the privacy of individuals requires agencies to carefully consider any collection of PII and ensure that they collect only the minimum necessary to carry out their missions. Further, agencies must ensure that any PII they collect, store, or process is protected from unauthorized access, tampering, or loss.

The protection of personal privacy has become a more significant issue in recent years with the advent of new technologies and the proliferation of personal information. The increasingly sophisticated ways in which the federal government obtains and uses PII have the potential to assist in performing critical functions, such as helping to detect and prevent terrorist threats and enhancing online interactions with the public. However, these technological developments can also pose challenges in ensuring the protection of privacy. Recognizing these challenges, we expanded our information security high-risk area in 2015 to include protecting the privacy of PII.¹

Office of Management and Budget (OMB) guidance requires agencies to establish programs to ensure the privacy of the PII they collect, process, and share. This includes designating a senior agency official for privacy (SAOP) with responsibility for developing, implementing, and maintaining privacy protections and managing privacy risks at the agency, among other things. In addition, agencies are required to conduct privacy impact

¹See most recently GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, [GAO-21-119SP](#) (Washington, D.C.: Mar. 2, 2021) and *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, [GAO-21-288](#) (Washington, D.C.: Mar. 24, 2021). We have designated information security as a government-wide high-risk area since 1997.

assessments (PIA) to analyze how personal information is collected, stored, shared, and managed in a federal system.

You asked us to examine federal agencies' privacy programs, including the roles and responsibilities of senior privacy officials in reviewing and approving privacy protections. Accordingly, this report examines (1) the extent to which agencies have established privacy programs for ensuring privacy protections for agency programs; (2) the challenges agencies reported experiencing in implementing their privacy programs; (3) reported benefits and limitations in agencies' use of privacy impact assessments (PIAs); and (4) the extent to which agencies have senior leadership dedicated to privacy issues.

In conducting this engagement, we focused on the 24 Chief Financial Officers Act of 1990 (CFO Act) agencies.² To address the first objective, we reviewed relevant privacy laws, including the Privacy Act of 1974 and the E-Government Act of 2002. We also reviewed federal privacy guidance, including OMB Circular A-130, and National Institute of Standards and Technology (NIST) Special Publication 800-37, among others. From these documents, we identified key practices for establishing privacy programs for ensuring privacy protections. We selected practices that address the general requirements of a privacy program and lay the foundation for ensuring compliance with applicable privacy requirements, coordinating with other key agency functions, and managing privacy risks. We then assessed the extent to which the 24 CFO Act agencies have established programs for ensuring privacy protections in accordance with these key practices. To do so, we collected and analyzed agency policies and procedures, and interviewed relevant agency officials.

Regarding the second objective, we identified potential challenges that agencies may face in implementing their privacy programs, based on our initial agency interviews, prior GAO work, and other background research

²The CFO Act, 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 CFO 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.

on federal privacy programs. We then administered a survey to privacy officials at the 24 CFO Act agencies asking them to identify which of the potential challenges, or any other challenges, they have experienced in implementing their privacy programs and what factors contributed to them. We analyzed the results of this survey to identify the number of agencies citing each specific challenge, as well as common contributing factors. Finally, we obtained OMB Office of Information and Regulatory Affairs (OIRA) privacy branch staff's perspectives on these challenges, including information on any government-wide efforts planned or under way that may address the identified challenges.

To address the third objective, we identified potential benefits and limitations of PIAs by interviewing selected experts from non-CFO Act federal agencies, the researcher community, and privacy advocacy organizations. We selected these experts based on their prior work relating to federal agencies' use of PIAs. We also administered a survey to the 24 CFO Act agencies to identify any benefits and limitations they experienced in their use of PIAs, and what factors contributed to them. We analyzed the information collected to identify the number of agencies and experts reporting specific benefits and limitations of PIAs, as well as any contributing factors. Finally, we obtained OMB OIRA privacy branch staff's perspectives on the agency- and expert-reported benefits and limitations of PIAs. This included information on any government-wide efforts planned or under way that may address limitations identified in agencies' use of PIAs.

For our fourth objective, we reviewed OMB guidance on the role of the SAOP, and reviewed agency policies and procedures to determine which official had been designated SAOP. We also determined if the SAOP had delegated privacy-related responsibilities to other agency officials. Further, we interviewed privacy officials at agencies with a chief privacy officer or other senior privacy official established by law. We also discussed the SAOP role with privacy branch staff from OIRA. See appendix I for a more detailed discussion of our objectives, scope, and methodology.

We conducted this performance audit from March 2021 to September 2022 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

The federal government collects and uses personal information, including PII, in increasingly sophisticated ways. For example, the Department of Commerce's Census Bureau processes PII on over a hundred million households across the country to produce data products, such as the apportionment of congressional seats and redistricting data, as part of the decennial census. The government's reliance on IT to collect, store, and transmit this sensitive information has also grown. Consequently, vulnerabilities arising from agencies' increased dependence on IT can result in the compromise of sensitive personal information, such as inappropriate use, modification, or disclosure. For example, insufficient policies, procedures, and technical controls for limiting employee and contractor access to systems containing PII can put that information at increased risk of compromise.

In addition, privacy risks are created by the increasing amounts of data that agencies and other organizations collect, as well as new techniques available for analyzing them. For example, advances in technology, such as new search technology and data analytics software, have made it easier for individuals and organizations to correlate information and track it across large and numerous databases. In addition, lower data storage costs have made it less expensive to store vast amounts of data. Moreover, ubiquitous internet and cellular connectivity make it easier to track individuals by allowing easy access to information pinpointing their locations.

The federal government continues to face challenges in protecting privacy and sensitive data. Information security incidents, many involving PII, continue to affect federal agencies. For example, federal agencies reported 30,819 incidents to the Cybersecurity and Infrastructure Security Agency in fiscal year 2020, representing an 8% increase from fiscal year 2019 when agencies reported 28,581 incidents. Agencies reported the following examples of privacy incidents involving breaches or potential breaches of PII in fiscal year 2020:

-
- On September 4, 2020, the Department of Defense (DOD) reported a major incident³ at the Defense Manpower Data Center after an analyst mistakenly uploaded an incorrect dataset for delivery to a Navy civilian employee. The dataset included PII such as names, Social Security numbers, dates of birth, home addresses, and personnel information. An estimated 300,000 people were potentially affected.
 - On January 10, 2020, the Department of Justice (DOJ) reported a major incident at the United States Marshals Service after an intrusion was detected in the Detention Services Network system. PII such as names, addresses, dates of birth, Social Security numbers, Federal Bureau of Investigation numbers, and alien numbers of current and former prisoners were successfully electronically exfiltrated.⁴ An estimated 387,000 people were potentially affected.
 - On October 25, 2019, the Department of Homeland Security (DHS) reported a major incident at the Federal Emergency Management Agency that involved possible oversharing of PII data with a third-party vendor. The PII data included names, home addresses, phone numbers, e-mail addresses, and several non-PII elements related to disaster aid. An estimated 307,000 individuals were potentially affected.

³OMB defines a major incident as one that is either (1) likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people or (2) a breach that involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. OMB adds that while agencies should assess each breach on a case-by-case basis to determine whether the breach meets the definition of a major incident, its guidance requires a determination of major incident for any unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to the PII of 100,000 or more people. See OMB Memorandum 20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements* (Washington, D.C.: Nov. 19, 2019).

⁴Exfiltration is the unauthorized transfer of information from a system.

Federal Law and Policy Establish Requirements for Protecting PII and Establishing Agency Privacy Programs

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 and ensuring privacy protections for agency programs.⁵ These include the following laws and guidance, among others:

- **Privacy Act of 1974.** The act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records.⁶ It requires agencies to issue system of records notices (SORN) to notify the public when they establish or make changes to a system of records. SORNs are to 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 PIA for each system.⁷ This assessment is an analysis of how personal information is collected, stored, shared, and managed in a federal system. Agencies must conduct a PIA before developing or procuring IT that collects, maintains, or disseminates information that is in an identifiable form. A PIA must also be performed before initiating any new data collections involving identifiable information that will be collected, maintained, or disseminated using IT if the same questions or reporting requirements are imposed on ten or more people.
- **OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act.*** This 2003

⁵The discussion 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 (HIPAA), 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 (FERPA), 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.

⁶Privacy 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).

⁷E-Government Act of 2002, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921 (Dec. 17, 2002).

memorandum provides guidance on implementing the privacy provisions of the E-Government Act.⁸ According to this guidance, the purpose of a PIA is to: (1) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. The guidance discusses when agencies should conduct or update a PIA, and what elements are to be included, such as what information is being collected and how it will be used and shared. The guidance also discusses what privacy risks the agency has identified and the steps it has taken to mitigate those risks. In addition, the guidance notes that, in general, PIAs should be made available on agencies' public websites with some exceptions, such as when doing so would reveal classified or other sensitive information.

- **Executive Order 13719, *Establishment of the Federal Privacy Council*.** This 2016 executive order directed OMB to issue a revised policy on the role and designation of the senior agency officials for privacy (SAOP). The revised policy includes guidance on the SAOP responsibilities at their agencies, required level of expertise, adequate level of resources, and other matters. It further directed the head of each agency to designate or re-designate an SAOP with the experience and skills necessary to manage an agency-wide privacy program, consistent with OMB's guidance. Further, the order established the Federal Privacy Council as the principal interagency forum to improve the government privacy practices of agencies and entities acting on their behalf.⁹
- **OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy*.** As directed by Executive Order 13719, OMB issued this guidance in September 2016 to clarify and update the role of the agency SAOP.¹⁰ In particular, it describes the position, expertise, and authority the SAOP should have, and it provides details on the SAOP's responsibilities. It notes that the SAOP should have a central leadership role at the agency with visibility into agency

⁸Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Washington, D.C.: Sept. 26, 2003).

⁹The White House, *Establishment of the Federal Privacy Council*, Executive Order 13719 (Washington, D.C.: Feb. 9, 2016).

¹⁰OMB Memorandum M-16-24: *Role and Designation of Senior Agency Officials for Privacy* (Washington, D.C.: Sept. 15, 2016).

operations and a position high enough to regularly engage with senior leadership. It also states that the SAOP should have the skills, knowledge, and expertise to lead the agency's privacy program and the necessary authority to lead the program and carry out privacy-related functions.

- **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.¹¹ The appendices to this circular include responsibilities for protecting federal information resources and managing PII. In particular, appendix II outlines some of the general responsibilities for federal agencies managing information resources that involve PII and summarizes the key privacy requirements for managing those resources. These responsibilities include developing, implementing, documenting, maintaining, and overseeing agency-wide privacy programs that include people, processes, and technologies, among others.

In addition to laws and guidance focusing specifically on PII, agencies are subject to laws and guidance governing the protection of information and information systems, which includes implementing privacy protections. For example:

- **Federal Information Security Modernization Act of 2014 (FISMA).** The act is intended to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets, as well as the effective oversight of information security risks.¹² The act requires each agency to develop, document, and implement an agency-wide information security program. Further, FISMA gives NIST responsibility for developing standards for categorizing information and information systems, security requirements for information and systems, and guidelines for detection and handling of

¹¹OMB Circular A-130, *Managing Information as a Strategic Resource* (Washington, D.C.: July 2016).

¹²The Federal Information Security Modernization Act of 2014 (FISMA 2014) Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

security incidents. Several of these standards and guidance address privacy and the management of PII.

- **NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.** This document provides a catalog of security and privacy controls for systems and organizations. While previous revisions of this publication included a separate appendix detailing specific privacy controls, revision 5, issued in September 2020, aims to fully integrate privacy controls into the security control catalog, creating a consolidated and unified set of controls.¹³
- **NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.** This document describes the NIST Risk Management Framework and provides guidelines for applying the framework to information systems and organizations. The framework provides a disciplined, structured, and flexible process for managing security and privacy risk. This process includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. The risk management framework includes activities to prepare organizations to execute the framework at appropriate risk management levels.¹⁴

Federal Guidance Includes Key Practices for Establishing Privacy Programs

OMB and NIST guidance include key practices for establishing programs for ensuring privacy protections for agency programs.¹⁵ Specifically, these include activities that lay the foundation for programs to develop and evaluate privacy policy, manage privacy risks, and ensure compliance with applicable privacy requirements. The key practices we used to assess agencies' programs are listed in table 1 and described in more detail below.

¹³NIST SP 800-53, Revision 5: *Security and Privacy Controls for Information Systems and Organizations* (Gaithersburg, Md.: September 2020).

¹⁴NIST 800-37, Revision 2: *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (Gaithersburg, Md.: December 2018).

¹⁵This guidance includes OMB A-130 and M-16-24; and NIST 800-37, Rev. 2.

Table 1: Key Practices for Establishing a Program for Ensuring Privacy Protections

Key practice	Description
<i>Document privacy compliance activities</i>	
Develop system of records notices	Agencies are required to comply with the requirements of the Privacy Act of 1974 and ensure that system of records notices are published, revised, and rescinded, as required.
Develop privacy impact assessments	Agencies are required to conduct privacy impact assessments in accordance with the E-Government Act of 2002.
Develop and maintain a privacy program plan	Agencies are required to develop and maintain a privacy program plan that provides an overview of the agency's privacy program. The plan should also include the program management and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.
<i>Ensure coordination between privacy and other programs or functions</i>	
Coordination with information security program	Agencies should ensure that the senior agency official for privacy (SAOP) and the agency's privacy personnel closely coordinate specifically with agency officials responsible for information security.
Coordination with IT budget and acquisition activities	The SAOP is responsible for reviewing in IT capital investment plans and budgetary requests to ensure privacy requirements and associated controls are explicitly identified and included with respect to any IT resources that will involve personally identifiable information (PII).
Coordination with workforce planning activities	The SAOP should be involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy.
Coordination with incident response activities	The SAOP should be notified of privacy-related incidents in accordance with procedures issued by the Office of Management and Budget.
<i>Implement a risk management framework to manage privacy risks</i>	
Develop a privacy risk management strategy	Agencies should establish a risk management strategy for the organization that includes a determination of privacy risk tolerance.
Authorize information systems containing PII	Agencies should ensure the involvement of the SAOP or other key privacy officials in the categorization, control selection, control assessment, and authorization of agency information systems with PII.
Develop a privacy continuous monitoring strategy	As part of an agency's risk management process, the appropriate privacy official is to develop and maintain a written strategy for monitoring privacy controls on an ongoing basis.

Source: GAO analysis of OMB and NIST guidance. | GAO-22-105065

Document Privacy Compliance Activities

- **Develop SORNs.** Agencies are to comply with the requirements of the Privacy Act of 1974 and ensure that system of records notices (SORN) are published, revised, and rescinded, as required.¹⁶ SORNs are to 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.

¹⁶OMB A-130, app. II.

Ensure Coordination between
Privacy and Other Programs or
Functions

- **Develop PIAs.** Agencies are required to conduct PIAs in accordance with the E-Government Act of 2002.¹⁷ A PIA is an analysis of how PII is handled to ensure that handling conforms to applicable privacy requirements. A PIA also determines the privacy risks associated with an information system or activity, and evaluates ways to mitigate privacy risks.
- **Develop and maintain a privacy program plan.** OMB guidance states that agencies are required to develop and maintain a privacy program plan.¹⁸ The plan should provide an overview of the agency's privacy program, including, a description of the structure of the privacy program, the role of the SAOP and other privacy officials and staff. The plan should also outline the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.
- **Coordinate with information security program.** OMB guidance states that agencies should ensure that the SAOP and the agency's privacy personnel closely coordinate specifically with the agency chief information officer, senior agency information security officer, and other agency offices and officials, as appropriate.¹⁹ This includes taking a coordinated approach to identifying and managing security and privacy risks and complying with applicable requirements.
- **Coordinate with IT budget and acquisition activities.** OMB guidance states that the SAOP should review IT capital investment plans and budgetary requests to ensure that privacy requirements and associated privacy controls, as well as any associated costs, are explicitly identified. The SAOP should review these plans for any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.²⁰
- **Coordinate with workforce planning activities.** According to OMB, agencies shall ensure that the SAOP is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy.²¹ The SAOP, along with other senior leaders, should develop and maintain a workforce planning

¹⁷Pub. L. No. 107-347, § 208, 116 Stat. at 2921; OMB A-130, app. II.

¹⁸OMB A-130, app. II.

¹⁹OMB A-130, app. II.

²⁰OMB A-130, app. II.

²¹OMB A-130, app. II.

Manage Privacy Risks

process. This process should ensure that the agency can anticipate and respond to changing mission requirements, maintain workforce skills in a rapidly developing IT environment, and recruit and retain the talent needed to accomplish the mission.

- **Coordinate with incident response activities.** OMB guidance states that agencies are to maintain formal incident management and response policies and capabilities. This includes ensuring that privacy-related incidents are reported to the SAOP and defining roles and responsibilities to ensure the oversight and coordination of privacy incident response activities.²²
- **Develop a privacy risk management strategy.** According to NIST guidance, agencies should establish a risk management strategy for the organization incorporating privacy risk that includes, among other things, a statement of the agency's risk tolerance.²³
- **Authorize information systems containing PII.** OMB and NIST guidance note that the SAOP or other privacy official should be involved in agency activities for authorizing information systems that include PII.²⁴ This includes the following:
 - Review and approve the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.
 - Designate which privacy controls the agency will treat as program management, common, information system-specific, and hybrid controls.
 - Identify privacy control assessment methodologies and metrics, conduct the assessment and document the results.
 - Review authorization packages for information system that involves PII to ensure compliance with applicable privacy requirements and manage privacy risks, prior to system authorization.
- **Develop a privacy continuous monitoring strategy.** OMB guidance states that, as part of an agency's risk management process, the

²²OMB A-130, app. II.

²³NIST SP 800-37, Rev. 2. Risk tolerance is the level of risk or degree of uncertainty that is acceptable to organizations.

²⁴OMB A-130, app. II; NIST SP 800-37, Rev. 2.

appropriate privacy official is to develop and maintain a written privacy continuous monitoring strategy.²⁵ The strategy should catalog the available privacy controls implemented at the agency across the agency risk management tiers. Further, it should ensure that the controls are effectively monitored on an ongoing basis, at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.

OMB Oversees Executive Branch Privacy Policy and Information Sharing

OMB's OIRA provides oversight of executive branch privacy policy and is responsible for, among other things, providing assistance to federal agencies on privacy matters, developing federal privacy policy, and overseeing implementation of privacy policy by federal agencies. This includes issuing memoranda that provide privacy-related guidance to agencies. In addition, each year, OMB issues guidance instructing each SAOP to review the administration of the agency's privacy program and report compliance data to OMB. Lastly, OIRA's Privacy Branch Chief also serves as the chair of the Federal Privacy Council.

The Federal Privacy Council, as noted above, was established by Executive Order 13719 and serves as the principal interagency forum to improve the privacy practices of agencies and entities acting on their behalf. The council aims to support interagency efforts to protect privacy and provide expertise and assistance to agencies and expand the skill and career development opportunities of agency privacy professionals. It also allows agencies to share lessons learned and best practices and promotes collaboration between and among agency privacy professionals. The council's membership consists of senior privacy officials from across the executive branch. It also has multiple committees addressing topics such as agency implementation and privacy workforce, as well as working groups on several topics, including risk management. The council also makes available resources on its website such as a privacy "law library" and a SORN dashboard.²⁶

²⁵OMB A-130, app. II.

²⁶These resources are located at the Federal Privacy Council's website, <https://www.fpc.gov>.

Prior GAO Work Has Highlighted the Need for Additional Actions to Protect Privacy

We have previously identified actions that need to be taken to better protect sensitive personal data held by federal agencies, highlighting the importance of fully establishing programs for ensuring privacy protections. For example:

- In December 2021, we reported that although selected DHS components addressed most of the key privacy control activities for overseeing contractor-operated systems, gaps existed in their compliance with these activities.²⁷ These included identifying and addressing gaps in privacy compliance, administering role-based privacy training, evaluating proposed new instances of PII sharing in contractor-operated systems, and documenting incident remediation activities. We made seven recommendations to DHS components to improve their oversight of contractors' privacy controls and remediation of incidents. DHS concurred with the recommendations and outlined steps planned or taken to address them. As of May 2022, DHS had not implemented any of the recommendations.
- In September 2020, we reported that Customs and Border Protection had taken steps to incorporate some privacy principles in its facial recognition technology program. These steps included publishing the legislative authorities used to implement its program, but the agency had not consistently provided complete information in privacy notices or ensured notices were posted and visible to travelers.²⁸ We made five recommendations to the agency to address these limitations. DHS concurred with the recommendations and, as of May 2022, had implemented two of them.
- We reported in September 2020 that the Department of Housing and Urban Development (HUD) was not effectively protecting sensitive information exchanged with external entities.²⁹ We made five recommendations to HUD to fully implement leading practices and fully identify the extent to which sensitive information is shared with external entities. HUD did not agree or disagree with the

²⁷GAO, *DHS Privacy: Selected Component Agencies Generally Provided Oversight of Contractors, but Further Actions Are Needed to Address Gaps*, [GAO-22-104144](#) (Washington, D.C.: Dec. 16, 2021).

²⁸GAO, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, [GAO-20-568](#) (Washington, D.C.: Sept. 2, 2020).

²⁹GAO, *Information Security and Privacy: HUD Needs a Major Effort to Protect Data Shared with External Entities*, [GAO-20-431](#) (Washington, D.C.: Sept. 21, 2020).

recommendations, but described actions intended to address them. As of May 2022, HUD had implemented four of the five recommendations.

- We reported in September 2018 that the office of Federal Student Aid exercised minimal oversight of certain lenders' protection of borrower data. We made six recommendations to the agency to ensure that its oversight of non-school partners addressed key practices for ensuring the protection of PII.³⁰ Federal Student Aid concurred with three of the recommendations, partially concurred with two, and did not concur with one. As of May 2022, the agency had implemented two of the six recommendations.
- In August 2018, we reported on actions taken by the consumer reporting company Equifax and by federal agencies in response to a breach at Equifax resulting in attackers accessing personal information of at least 145.5 million individuals.³¹ Equifax's investigation of the breach identified four major factors, and it reported that it took steps to mitigate these factors and attempted to identify and notify individuals whose information was accessed. In addition, three major federal customers that used Equifax's identity verification services—Internal Revenue Service, Social Security Administration (SSA), and the U.S. Postal Service—conducted assessments of the company's security controls. The assessments identified several lower-level technical concerns that Equifax was directed to address. The agencies also adjusted their contracts with Equifax, such as modifying notification requirements for future data breaches. In addition, the Bureau of Consumer Financial Protection and the Federal Trade Commission, which have regulatory and enforcement authority over consumer reporting agencies such as Equifax, initiated an investigation into the breach and Equifax's response in September 2017. We did not make any recommendations in this report.

Gaps Exist in Agency Policies for Ensuring Privacy Protections

The 24 CFO Act agencies established privacy programs with a variety of organizational placements and structures. In addition, agencies varied in the extent to which they established policies and procedures for ensuring privacy protections. Without incorporating key practices into their policies

³⁰GAO, *Cybersecurity: Office of Federal Student Aid Should Take Additional Steps to Oversee Non-School Partners' Protection of Borrower Information*, [GAO-18-518](#) (Washington, D.C.: Sept. 17, 2018).

³¹GAO, *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*, [GAO-18-559](#) (Washington, D.C.: Aug. 30, 2018).

and procedures, agencies will have less assurance that they are consistently and effectively implementing privacy protections.

Agencies Established Privacy Programs with Varying Organizational Placement and Structure

As previously mentioned, OMB guidance requires that agencies develop, implement, document, maintain, and oversee agency-wide privacy programs that include people, processes, and technologies. They are also to designate an SAOP who has agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risks. OMB guidance further states that the SAOP should serve in a central leadership position at the agency. The SAOP should also have visibility into relevant agency operations and be positioned highly enough within the agency to regularly engage with other agency leadership, including the head of the agency.

In accordance with this guidance, all of the 24 selected agencies established a privacy program and designated an SAOP who has overall responsibility for the program. These responsibilities include developing and implementing privacy policies, ensuring compliance with privacy requirements, and managing privacy risks.

Half of the agencies positioned their privacy program within the Office of the Chief Information Officer (CIO) and designated either the CIO or Deputy CIO as the SAOP. The remaining 12 agencies located their privacy programs in a variety of other offices, or as stand-alone privacy offices, and designated various other officials as SAOP. For example, one agency designated its Chief Administrative Officer as SAOP, and placed the privacy program in that official's office. Another placed the privacy program within the Office of the General Counsel and designated the General Counsel as SAOP.

Although the SAOP retains responsibility and accountability for the agency's privacy program, OMB guidance provides for the delegation of privacy functions to other qualified agency personnel.³² It further notes that agencies shall consider establishing privacy programs and privacy officials at sub-agencies, components, or programs. Accordingly, the majority of agencies (21 of 24) have delegated much of the day-to-day oversight of their privacy programs to an official other than the SAOP, such as a chief privacy officer (CPO). In addition, depending on an agency's size or structure, it may have a more centralized privacy program, or a decentralized one, with privacy programs and staff at the component or program level. Table 2 shows, for the 24 agencies, the

³²OMB M-16-24.

designated SAOP, responsible privacy office, and whether the agency's privacy program is centralized or decentralized.

Table 2: Officials and Offices with Overall Privacy Responsibilities at the 24 Chief Financial Officers Act of 1990 Agencies

Agency	Official designated as Senior Agency Official for Privacy	Responsible office	Structure (centralized vs. decentralized)^a
U.S. Department of Agriculture	Chief Information Officer (CIO)	Privacy Office, within the Office of the CIO (OCIO)	Decentralized
Department of Commerce	Director of Privacy and Open Government (Office of the Secretary)	The Office of Privacy and Open Government, within the Office of the Secretary	Decentralized
Department of Defense	Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency	Privacy, Civil Liberties, and Freedom of Information Act Directorate	Decentralized
Department of Education	Director of the Student Privacy Policy Office	Student Privacy Policy Office	Centralized
Department of Energy	CIO	Privacy and Records Management Office, within the Office of the CIO	Decentralized
Department of Health and Human Services	CIO	Office of Privacy and Information Management, within the Office of Information Security, OCIO	Decentralized
Department of Homeland Security	Chief Privacy Officer	Privacy Office	Decentralized
Department of Housing and Urban Development	Chief Administrative Officer	Privacy Program within the Office of the Chief Administrative Officer	Decentralized
Department of the Interior	CIO	Privacy Office, within the Cybersecurity Division in the OCIO	Decentralized
Department of Justice	Chief Privacy and Civil Liberties Officer	Deputy Attorney General office	Decentralized
Department of Labor	Deputy Assistant Secretary for Operations (Office of the Assistant Secretary for Administration and Management)	Standards and Guidance Branch under the Division of Information Security Policy & Planning in the Cybersecurity Directorate within the OCIO	Decentralized
Department of State	Deputy Assistant Secretary for Global Information Services	Privacy Office within the Bureau of Administration	Centralized
Department of Transportation	Deputy CIO	Privacy Office within the OCIO	Decentralized
Department of the Treasury	Assistant Secretary for Management	Office of Privacy, Transparency, and Records within the Office of Management	Decentralized
Department of Veterans Affairs	CIO	Office of Information Security, Office of Information Technology	Decentralized
Environmental Protection Agency	CIO	Privacy Program, OCIO	Decentralized

Agency	Official designated as Senior Agency Official for Privacy	Responsible office	Structure (centralized vs. decentralized) ^a
General Services Administration	Deputy CIO	OCIO	Centralized
National Aeronautics and Space Administration	CIO	Cybersecurity and Privacy Division, OCIO	Decentralized
National Science Foundation	CIO	Division of Information Systems	Centralized
Nuclear Regulatory Commission	Deputy CIO	Cybersecurity Branch, Government and Enterprise Management Services Division, OCIO	Centralized
Office of Personnel Management	Chief Privacy Officer	Office of Privacy and Information Management	Centralized
Small Business Administration	CIO	Information Security Division, OCIO	Centralized
Social Security Administration	General Counsel	Office of Privacy and Disclosure, Office of General Counsel	Centralized
U.S. Agency for International Development	Acting Deputy Administrator	Information Assurance Division, OCIO, Bureau for Management	Decentralized

Source: GAO analysis of agency data. | GAO-22-105065

^aFor the purposes of this report, a centralized structure is one in which privacy staff are concentrated at the agency or department level. A decentralized structure is one in which agency components have their own privacy staff (e.g., component Chief Privacy Officers) who are responsible for implementing requirements.

At most agencies, the official designated as the SAOP primarily has non-privacy roles and responsibilities, such as serving as the agency’s CIO, Chief Administrative Officer, or in another role. Accordingly, these agencies delegate much of the day-to-day oversight of their privacy program to another dedicated official.³³ For example, at the U.S. Agency for International Development (USAID), the SAOP has overall responsibility and accountability for ensuring the agency’s implementation of privacy protections, including full compliance with federal laws, regulations, and policies relating to privacy. However, the CPO provides oversight and guidance for privacy policy and procedures, compliance

³³OMB guidance notes that at the discretion of the SAOP and consistent with applicable law, other qualified agency personnel may perform privacy functions that are assigned to the SAOP. In addition, agencies shall consider establishing privacy programs and privacy officials at sub-agencies, components, or programs where there is a need for privacy leadership in support of the SAOP. In all cases, however, the SAOP shall retain responsibility and accountability for the agency’s privacy program, including privacy functions performed by officials at sub-agencies, components, or programs. See OMB-M-16-24.

activities, and the effectiveness of the agency-wide privacy program. The CPO also ensures that privacy requirements are incorporated into each stage of the information lifecycle.

Agencies also may have more centralized or decentralized privacy programs depending on their size and structure. That is, privacy management and compliance activities might be carried on primarily through the agency- or department-level privacy program, or they may delegate implementation to component or bureau privacy officials. Some agencies (e.g., smaller ones) give the agency-level privacy program primary responsibility for ensuring that privacy requirements are met and privacy protections are implemented at the agency. For example, at the National Science Foundation (NSF), the agency Privacy Lead is responsible for working directly with system owners to incorporate privacy requirements and best practices. The Privacy Lead is also to ensure that privacy-related NIST controls are built into new systems and assist system owners with conducting PIAs.

By contrast, some agencies (e.g., larger or more decentralized agencies) delegate the implementation of privacy activities to component privacy officials or programs. These agencies may have component-level senior privacy officials or component CPOs who are responsible for coordinating with program offices and other component functions to ensure the implementation of privacy policy and requirements. For example, the Department of Defense (DOD) has Senior Component Officials for Privacy and component Privacy and Civil Liberties Officers further responsible for the day-to-day management and implementation of the DOD privacy program. These component-level activities include, for example, establishing component-specific privacy policy and working directly with system owners or program managers to develop privacy compliance documentation.

Agencies Implemented Some but Not All Key Practices for Ensuring Privacy Protections

The 24 selected agencies established privacy programs with authority and responsibility for ensuring privacy protections for agency programs. However, these programs did not fully address selected key practices identified by federal guidance (and discussed previously) for ensuring that privacy protections are incorporated into agency programs and activities. Specifically, agency policies and procedures mostly addressed privacy compliance activities, had some gaps in addressing coordination between privacy and other agency functions, and had the most gaps in addressing risk management activities. Figure 1 shows the number of agencies that addressed, partially addressed, or did not address these selected practices. (Additional details on the extent to which the agencies addressed these practices are in appendix III.)

Figure 1: Extent to Which the 24 Chief Financial Officers Act of 1990 Agencies Addressed Key Practices for Establishing a Privacy Program

Privacy compliance activities

Establish system of records notice policies



Establish privacy impact assessment policies



Develop privacy program plan



Coordination between privacy and other programs or functions

Ensure coordination with information security



Ensure coordination with IT budget and acquisition



Ensure coordination with workforce management



Ensure coordination with incident response



Risk management framework to manage privacy risks

Develop a privacy risk management strategy



Incorporate privacy in system authorization steps

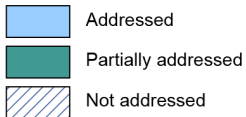


Develop a privacy continuous monitoring strategy



0 4 8 12 16 20 24

Number of agencies



Source: GAO analysis of agency information. | GAO-22-105065

Agencies Generally Documented Privacy Compliance Activities

As discussed previously, fundamental privacy compliance activities include developing SORNs and PIAs and documenting the activities of the agency's program in a privacy program plan. Agencies generally documented fundamental privacy compliance activities by developing policies and procedures for SORNs and PIAs, as well as developing plans that provide an overview of the privacy programs, with a few exceptions.

- **Develop SORNs.** Twenty-two of 24 agencies fully documented policies and procedures for ensuring the creation, review, and publication of SORNs.³⁴ For example, whenever a Department of Labor organization proposes to establish a new system of records or significantly revise an existing one, the program manager is to notify the Labor Privacy Act Officer who will provide assistance in preparing a SORN using the prescribed format. The officer will also coordinate its review and approval within Labor and submit it for evaluation by OMB and Congress and for publication in the Federal Register.

In contrast, two agencies (the Department of Education and the Office of Personnel Management (OPM)) had not fully documented these activities, or their policies were out of date. Specifically, Education's SORN procedures were out of date in that they did not accurately reflect the current structure of the privacy program or address guidance provided since the directives were approved. In addition, OPM had not fully documented its process for developing, reviewing, and approving SORNs.

OPM and Education privacy officials stated that they intend to update their policies, although they did not provide specific time frames for doing so. Until these policies are updated, agencies will have less assurance that SORNs are being developed in a timely manner, which is essential for informing the public about agencies' use of PII.

- **Develop PIAs.** All 24 agencies fully documented their policies and procedures for creating, reviewing, and updating PIAs. For example, the General Services Administration (GSA) defines policies and procedures for developing and maintaining privacy threshold assessments and PIAs. The policies and procedures include role and

³⁴These agencies were the Departments of Agriculture, Commerce, Defense, 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; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

responsibilities for completing these documents, as well as specifying who is responsible for reviewing, approving, and updating them, and at what frequency. This document states that under the direction of the SAOP, the CPO is responsible for evaluating the privacy threshold assessments and PIAs for completeness of privacy related information and approving them for publication.

- **Develop privacy program plan.** Twenty-three agencies fully developed a privacy program plan or equivalent policy or plan that identifies the role of key privacy officials, describes the structure of the privacy program, and documents program management and common privacy controls.³⁵ For example, the NSF Privacy Program Plan provides an overview of the agency's privacy program and describes the structure of the privacy program and the resources dedicated to the privacy program. The plan also describes the role of the SAOP and other privacy staff, the strategic goals and objectives of the program, and program management and common controls in place for meeting privacy requirements and managing privacy risks.

One agency (the Department of Agriculture (USDA)) developed plans but did not fully document program management or common privacy controls, as called for by OMB guidance. USDA's Privacy Program plan referenced the need to document these controls, but officials did not provide documentation of the controls. Without a privacy plan that documents program-management or common privacy controls, agencies have less assurance that privacy protections are consistently implemented across their organization and that privacy risks are effectively managed.

Agencies Did Not Always Define Processes for Coordination between Privacy Program and Other Key Functions

As discussed previously, OMB guidance calls for agency privacy programs to coordinate with other key functions, including information security, IT budget and acquisition, workforce planning, and incident response. The 24 agencies have taken steps to ensure coordination between privacy programs and other key programs and activities, including information security, budget and acquisition, workforce management, and incident response. However, agencies have not always

³⁵These agencies were the Departments of 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.

fully defined policies or processes for such coordination, to ensure that privacy considerations are effectively addressed.

- **Coordinate with information security program.** Almost all agencies (22) have fully defined policies and processes for ensuring that SAOP and other agency privacy personnel coordinate with the agency's CIO, Chief Information Security Officer (CISO), and other staff responsible for information security activities.³⁶ This coordination may include co-locating the privacy office and information security functions within the agency CIO office or convening councils or working groups to facilitate discussion, analysis, and policy review. For example, USDA established a Privacy Council, which is a standing committee, whose membership includes mission area and agency Privacy Officers, and other personnel designated by the agency, staff offices, and CIOs. The Privacy Council meets monthly and provides a venue for the discussion, analysis, and review of policy, procedures, and programs.

In contrast, two agencies (OPM and the Social Security Administration (SSA)) had not fully defined processes for coordination between the privacy and information security programs. According to OPM privacy officials, the office is working to formalize some of the processes and still needs to have the proper policies and procedures in place. The same officials added that they engage in regular meetings with OCIO staff regarding coordination with information security, though these processes have not been formalized. Similarly, while SSA policy included high-level statements regarding coordination between privacy and security, the policy did not elaborate on how this was to occur. Without clearly defining processes for coordination with information security officials, these agencies may not be able to consistently consider and incorporate key privacy considerations in security activities.

- **Coordinate with budget and acquisition activities.** Sixteen agencies have fully defined the role of the SAOP or other privacy officials in reviewing IT budgetary requests and capital investment plans to ensure privacy requirements and associated controls are

³⁶These agencies were the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, and Veterans Affairs, the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Small Business Administration, and U.S. Agency for International Development.

explicitly identified with respect to any IT resources that involve PII.³⁷ Specifically, the SAOP or other privacy officials may sit on the agency's investment review board to provide input on prospective IT programs. For example, Commerce's CIO serves as the chair of the Commerce Information Technology Review Board and the SAOP is a principal member of the board. The board is part of the department's investment review process and focuses on new or re-competed acquisitions required to support major investments and non-major investments with life-cycle costs at or above \$10 million.

In contrast, six agencies (USDA, Department of the Treasury, Department of Veterans Affairs (VA), GSA, SSA, and the U.S. Agency for International Development (USAID) partially defined and documented a process for the involvement of privacy officials in reviewing budget requests, while two agencies (Department of Housing and Urban Development (HUD) and Department of Labor) did not address this in policy.

Officials from USDA, HUD, Labor, Treasury, GSA, SSA, and USAID described ways in which privacy officials may be involved in reviewing and approving budget requests; however, they did not provide documentation that outlined the details of these review processes. One agency, VA, stated that it planned to update their policies and procedures to define and document the role of the SAOP or other privacy officials in these activities, but did not provide time frames for doing so. Until agencies fully define and document these processes, they may not be able to ensure privacy requirements and associated controls are explicitly identified and included with respect to any IT resources that will involve PII.

- **Coordinate with workforce management activities.** Eleven agencies defined policies and processes to ensure that the SAOP or other privacy officials are involved in assessing and addressing the hiring, training, and professional development needs of the agency's workforce with respect to privacy.³⁸ For example, at the Department of

³⁷These agencies were the Departments of Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Justice, Interior, State, and Transportation; the Environmental Protection Agency, National Aeronautics and Space Administration, Nuclear Regulatory Commission, National Science Foundation, Office of Personnel Management, and the Small Business Administration.

³⁸These agencies were the Departments Commerce, Education, Homeland Security, Housing and Urban Development, Interior, Justice, and State; the U.S. Agency for International Development; Environmental Protection Agency; National Aeronautics and Space Administration; and the National Science Foundation.

Education, the SAOP coordinates with the CIO and Chief Human Capital Officer to maintain and enhance workforce needs. They do so by, among other things, maintaining a current workforce planning process, recruiting and retaining privacy and IT professionals, developing a set of competency requirements for staff, and ensuring managers are aware of flexible hiring authorities plan.

The remaining 13 agencies (USDA, DOD, Energy, Health and Human Services (HHS), Labor, Transportation (DOT), Treasury, VA, GSA, Nuclear Regulatory Commission (NRC), OPM, Small Business Administration (SBA), and SSA) had not fully defined or documented processes for privacy workforce management. Three agencies (DOD, Energy, and GSA) noted that they were revising existing guidance or considering doing so, but did not provide timeframes for doing so. Further, nine agencies (USDA, HHS, DOT, Treasury, VA, NRC, OPM, SBA, and SSA) described processes for workforce planning but did not provide documentation of the role of the SAOP or other privacy officials in those processes. Lastly, one agency, Labor, acknowledged that the SAOP plays a minimal role in workforce planning. Without involvement from the SAOP or other privacy officials, agencies will be limited in their ability to identify staffing needs and ensure a well-qualified privacy workforce.

- **Coordinate with incident response activities.** All 24 agencies have defined roles and responsibilities for the SAOP and other privacy officials with respect to responding to privacy incidents, including breaches of PII. They each have policies or procedures that specify when the SAOP or other privacy officials must be notified when an incident or breach occurs and define the roles and responsibilities of privacy officials in responding to breaches. For example, at DHS, the SAOP is responsible for coordinating with the CIO and CISO to provide guidance and respond to privacy incidents and breaches of PII. Additionally, when first made aware of a privacy incident, the SAOP serves as the senior DHS official responsible for oversight of privacy incident management and leads the Breach Response Team. The SAOP also works with each component's privacy officers to make sure privacy-related incidents are properly reported and mitigated.

Agencies Varied in Incorporating Privacy into Risk Management Processes

As discussed previously, agencies should establish a risk management framework that incorporates privacy risks. This includes establishing an organization-wide risk management strategy that includes privacy, defining the role of the SAOP or other privacy officials in the steps for managing risks to information systems, and establishing a privacy continuous monitoring strategy. However, agencies varied in the extent to

which they incorporated privacy into their risk management processes. Specifically,

- **Develop a privacy risk management strategy.** Ten agencies developed a privacy risk management strategy or incorporated privacy into a broader cybersecurity risk management strategy.³⁹ For example, VA's privacy risk management strategic plan discusses the department's privacy risk tolerance and considerations for setting specific risk tolerance levels at various organizational tiers.⁴⁰ It also describes how VA identifies, assesses, and responds to privacy risks, among other things.

The remaining 14 agencies (USDA, Commerce, DOD, Energy, DHS, HUD, Interior, DOJ, State, DOT, Treasury, the National Aeronautics and Space Administration (NASA), OPM, and USAID) did not fully develop a risk management strategy that addresses strategic decisions regarding privacy, including a determination of the agency's risk tolerance. One agency, Commerce, stated that it planned to develop a strategy and finalize it in the third quarter of fiscal year 2022. Four agencies (USDA, DOD, Interior, and State) stated that they were planning to or considering developing such a strategy, but did not provide a firm time frame for doing so. Nine agencies (Energy, DHS, HUD, DOJ, DOT, Treasury, NASA, OPM, and USAID) stated that they used other policies or tools to manage privacy risks; however, the policies provided did not constitute a strategy that addresses considerations such as risk tolerance. Without an explicit strategy for managing privacy risk that includes a determination of risk tolerance, agencies will have less assurance that they are managing privacy risks within acceptable thresholds.

- **Authorize information systems with PII.** Twelve agencies defined the role of the SAOP or other officials in risk management steps for authorizing information systems with PII.⁴¹ For example, DOJ requires its Chief Privacy and Civil Liberties Officer, or a duly authorized representative, to review and approve the security categorization of information systems and identify methodologies and metrics for

³⁹These agencies were Education, HHS, DOL, VA, the Environmental Protection Agency, GSA, NSF, NRC, SBA, and SSA.

⁴⁰As defined by NIST, risk tolerance is the level of risk or degree of uncertainty that is acceptable to organizations.

⁴¹These agencies were Commerce, DOD, Education, HHS, HUD, Interior, DOJ, DOT, EPA, NSF, SBA, and USAID.

privacy control assessments. The official is also to review authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

However, eight agencies (USDA, DHS, State, Treasury, VA, GSA, NRC, and SSA) partially defined and documented the roles of privacy officials in carrying out these steps, while four (Energy, Labor, NASA, and OPM) did not explicitly define these roles in policy or procedure. Specifically, agencies did not always explicitly require the SAOP or other privacy officials to review and approve system categorizations, oversee control assessments, or review authorization packages.

Five agencies (Energy, State, Treasury, OPM, and SSA) noted that they were planning to revise their existing guidance to clarify the role of privacy officials in the risk management process or were considering doing so, but did not provide time frames for doing so. Six other agencies (USDA, DHS, VA, GSA, NASA, and NRC) noted that they had processes in place for involving privacy in each step; however, the involvement of privacy officials was not always documented in the agencies' policies and procedures. One agency, Labor, acknowledged that the SAOP did not play a role in the authorization process. Without fully documenting the roles of privacy officials in authorizing information systems with PII, agency privacy programs will be hindered in ensuring that privacy protections are adequately incorporated into those systems.

- **Continuous monitoring.** Fourteen of 24 agencies have developed a privacy continuous monitoring strategy.⁴² For example, HHS developed a privacy continuous monitoring strategy that applies to all of its IT systems that collect, process, maintain, share, and dispose of PII. This strategy includes, among other things, a catalog of privacy controls and specified minimum frequencies for assessing the controls. It also notes that operating divisions and system owners may require more frequent assessments in accordance with their risk tolerance.

The remaining 10 agencies (USDA, DOD, DOJ, DHS, HUD, State, Treasury, VA, Environmental Protection Agency (EPA), and OPM) had not fully developed such a strategy. Specifically, four agencies (USDA, HUD, State, and OPM) had not developed a privacy continuous monitoring strategy while six agencies (DOD, DHS, DOJ, Treasury, VA, and EPA) had developed a strategy but it lacked

⁴²These agencies were Commerce, Education, Energy, HHS, DOI, DOL, DOT, GSA, NASA, NSF, NRC, SSA, SBA, and USAID.

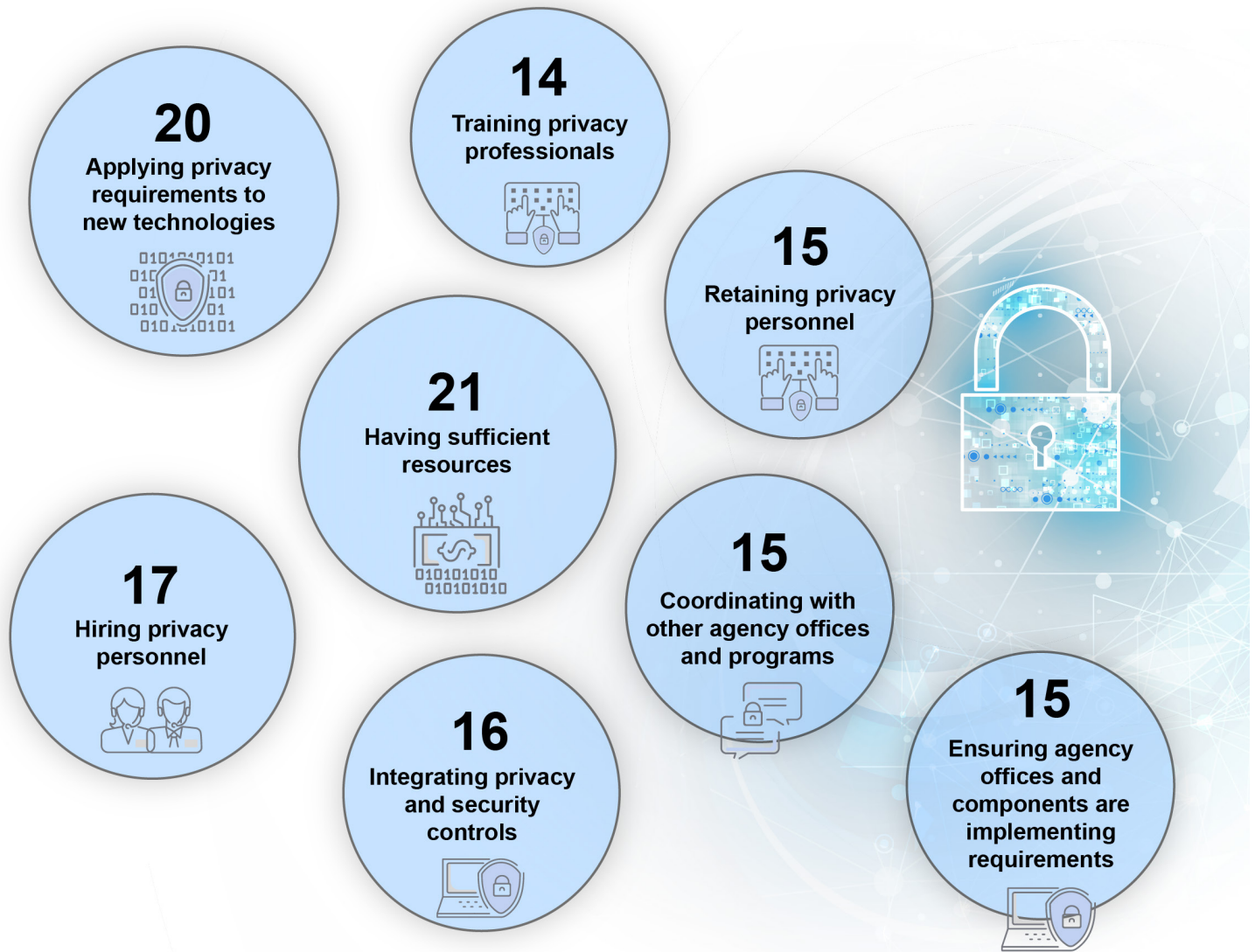
important elements, such as defining the frequency at which controls were to be assessed.

Of these 10 agencies, five (USDA, DOD, HUD, DOJ, and State) noted that they were in the process of fully developing a strategy or planned to, but did not provide a time frame for doing so. Three other agencies (DHS, Treasury, and OPM) noted that they relied on other tools, such as compliance tracking tools and the regular review of privacy threshold assessments and PIAs. However, these approaches did not constitute a comprehensive strategy for assessing privacy controls at a defined frequency. One agency, VA, had established a strategy, but had not included all elements, such as cataloging its privacy controls; the agency planned to complete this activity in fiscal year 2023. Another agency, EPA, provided an information security continuous monitoring strategy, but it did not specifically address privacy controls. Without a documented privacy continuous monitoring strategy that addresses how controls are to be assessed and at what frequency, agencies may lack ongoing awareness of the state of their privacy controls, which is necessary to support decisions for adequately protecting PII.

Agencies Identified Various Challenges Facing Their Privacy Programs

Privacy officials at all the 24 CFO Act agencies reported experiencing challenges in implementing their privacy programs. Agencies most cited challenges related to a lack of sufficient resources and applying privacy requirements to new and emerging technologies. Figure 2 shows the challenges most frequently identified and the number of agencies reporting each challenge, which are discussed in more detail below.

Figure 2: Number of 24 Chief Financial Officers Act of 1990 Agencies Reporting Challenges in Implementing Privacy Programs



Source: GAO analysis of agency survey responses; images: Thitichaya/stock.adobe.com, marinashevchenko/stock.adobe.com. | GAO-22-105065

Having Sufficient Resources

The Federal Privacy Council emphasizes that privacy programs should have the resources needed to manage federal information resources that involve PII. Further, OMB guidance states that agencies are to identify and plan for the financial, human, information, and infrastructural

resources that are necessary to carry out the privacy-related functions described in law and OMB policies.⁴³

Twenty-one of 24 agencies reported that having sufficient resources to complete privacy-related work is a challenge. Nine of these 21 agencies specified the lack of resources as being short staffed, while five of 21 agencies cited lack of funding, and four of 21 stated that privacy officials have multiple duties, which makes completing privacy-related work challenging. For example:

- SSA privacy officials stated that the onset of the COVID-19 pandemic shifted workload priorities and required them to re-allocate many of their resources to ensure continuity of operations. As a result, strategic initiatives such as revising templates and processes to align with NIST Special Publication 800-53 Revision 5 and other privacy-related efforts have not been implemented as quickly as anticipated.
- DHS privacy officials stated that providing sufficient subject matter expertise is a challenge, given that the Privacy Office has oversight of all the department's operational components, as well as DHS Headquarters offices. The officials explained that providing this expertise is a challenge given the staffing issues the office and other component privacy offices have encountered. This has been especially prevalent over the course of the last 2 years with the number of different programs/systems that have been developed due to the COVID-19 pandemic.
- EPA privacy officials also cited staffing shortages, stating that two key privacy program personnel left the agency in 2021. Officials added that they are actively working to backfill these vacancies, but it has been challenging to complete all privacy-related work.

Applying Privacy Requirements to New Technologies

OMB notes that as federal agencies take advantage of emerging information technologies and services, they must also apply the principles and practices of risk management, information security, and privacy to the acquisition and use of those technologies and services. To take advantage of these technologies, agencies must be able to adapt efficiently and effectively to apply privacy requirements.

Twenty of 24 agencies reported applying privacy requirements to new and emerging technologies as a challenge. Thirteen of these 20 agencies

⁴³OMB-M-16-24.

stated that this was due to lack of federal guidance for newer technologies such as cloud services⁴⁴ and artificial intelligence (AI)⁴⁵ technologies, or a lack of knowledge and expertise for applying privacy requirements to these technologies. For example:

- USAID privacy officials stated that applying privacy requirements to new and emerging technologies has been a challenge because the Privacy Act was enacted long before technological advancements, such as AI, machine learning,⁴⁶ and smart wearable technology.⁴⁷ They further noted that the amount of PII data collected and processed by new technologies has grown exponentially. The officials stated that they must consider whether non-PII becomes PII when combined with other data elements collected or acquired to facilitate the development of AI policy and procedures. Further, they noted applying requirements, such as determining whether an IT system or process constitutes a system of records under the Privacy Act has also been a challenge.
- Treasury privacy officials stated that finding and retaining subject matter experts, refining privacy policies, and conducting the necessary analyses to evaluate emerging technologies has been a challenge. They added that outdated federal guidance and uncertain vulnerabilities that accompany emerging technology also make it difficult to determine effectiveness of measures to apply privacy requirements.
- Interior privacy officials stated that there is a need for a better understanding of new and emerging technologies. They added that there are questions surrounding how the technologies will be used, how data will be used, and the separate and overlapping roles and responsibilities, to fully evaluate the potential privacy implications.

⁴⁴As defined by NIST, cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released.

⁴⁵While the term AI has a range of meanings, it can be defined as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.

⁴⁶Machine learning is a field of artificial intelligence (AI) in which software learns from data to perform a task.

⁴⁷This includes devices, such as fitness trackers, smart watches, or smart glasses, that collect personal data using sensors, analyze the data, and communicate information to the consumer.

Further, they stated that additional government-wide education, training, and collaboration would facilitate awareness of privacy considerations and emergent privacy risks. This could include privacy, security, and acquisition roles and requirements for AI, cloud service providers, and other new technologies.

Hiring Privacy Personnel

As the Federal Privacy Council and OPM have noted, to protect privacy, each agency needs experienced and educated privacy professionals.⁴⁸ They further state that privacy is a multidisciplinary field that includes skills and expertise in such varied areas such as law, IT, and cybersecurity.

Seventeen of 24 agencies reported hiring personnel to fill key privacy positions as a challenge. Ten of these 17 agencies stated that there is a lack of qualified candidates to fill privacy positions. For example:

- DHS privacy officials stated that the Privacy Office is facing critical hiring needs, with 35 percent of positions vacant. They further noted the office has struggled to fill these vacancies in part due to a severe shortage of qualified candidates applying for their job postings.
- DOJ privacy officials stated that there is heavy demand in the private sector for attorneys and analysts with privacy-related knowledge, skills, and experience. Officials explained that personnel with the appropriate skillset and who are willing to earn U.S. government salaries are difficult to find.
- Treasury privacy officials stated that approval to hire and fill any position is a long process, particularly positions that require specialized privacy knowledge or a security clearance. Officials added that privacy offices in different federal agencies often compete for a small pool of experienced privacy professionals. Treasury sometimes loses privacy personnel to other agencies that have established positions with seemingly similar responsibilities, but at higher grade levels.

Integrating Privacy and Security Controls

NIST emphasizes the need for close collaboration between cybersecurity and privacy programs to select and implement the appropriate controls for information systems processing PII. NIST further notes that a unified and collaborative approach provides greater visibility into the implementation

⁴⁸Federal Privacy Council and U.S. Office of Personnel Management, *Toolkit for Recruiting, Hiring, and Retaining Privacy Professionals in the Federal Government* (January 2017).

of security and privacy controls which will promote more informed, risk-based authorization decisions.

Sixteen of 24 agencies reported integrating privacy and security controls as it relates to the transition to NIST SP 800-53, Revision 5, as a challenge.⁴⁹ Four of the 16 agencies found this to be a challenge due to the increased work needed to adapt their processes and workflow to the new requirements. For example:

- NASA privacy officials stated that this is a challenge because the change requires significant effort to move existing plans to revision 5. As a result, this takes time and resources to implement on top of the time required to learn and understand the revision 5 controls.
- USAID privacy officials explained that they have struggled with updating their tool for meeting data protection compliance requirements, because NIST's revised guidance for assessing the implementation of the security and privacy controls in Revision 5 of SP 800-53⁵⁰ was not final at this time. They noted that in the interim, USAID planned to use a Revision 5-compliant spreadsheet to ensure compliance until the tool is updated and available for use.

Ensuring Agency Offices and Components Are Implementing Privacy Requirements

The Federal Privacy Council notes that agencies must cultivate privacy awareness among all employees of an agency. This includes ensuring awareness and accountability for complying with applicable privacy requirements and managing privacy risks.

Fifteen of 24 agencies reported that ensuring that program offices and/or agency components are aware of and implementing privacy requirements is a challenge. Six of the 15 agencies stated this was due to the large size of their agency and organizational structure. For example:

- DOT privacy officials stated that there are times when program offices are unaware of the need to implement privacy requirements, and may proceed without doing so, until they are referred to the Privacy Officer by someone familiar with the requirements. They pointed out that one

⁴⁹While the previous revision of this publication included a separate appendix detailing specific privacy controls, Revision 5, issued in September 2020, aims to fully integrate privacy controls into the security control catalog, creating a consolidated and unified set of controls.

⁵⁰National Institute of Standards and Technology 800-53A, Revision 5: *Assessing Security and Privacy Controls in Information Systems and Organizations* (Gaithersburg, Md.: January 2022), provides NIST's guidance for assessing the implementation of security and privacy controls.

example is program offices being unaware of the need for privacy assessments for information collections.

- DOD privacy officials stated that some components report that it is a challenge to ensure implementation of privacy requirements internally. Officials explained that this can be due to various factors, such as the size and scope of the component, a failure to consider privacy during early phases of a project, and a lack of awareness of what privacy requirements are.
- State privacy officials noted that the Privacy Office is centralized in that that privacy officers are not distributed throughout the agency in each bureau, but rather reside in a centralized location overseeing all bureaus. This limits the office's visibility and communication with the department's large global footprint domestically and overseas.

Coordinating with Other Agency Offices and Programs

OMB requires coordination between an agency's privacy program and other key activities. This is important because privacy-related activities may be carried out by personnel in multiple offices and at different organizational levels of the agency.

Fifteen of 24 agencies reported that coordinating with other agency offices and programs has been a challenge, primarily because of the cross-cutting nature of privacy, which requires input from multiple agency offices and components. Six of these 15 agencies stated that resource limitations make it difficult to coordinate privacy requirements fully and completely to the level desired. For example:

- VA privacy officials stated that coordination has been a challenge due to the decentralized structure of the VA Privacy program. In addition, program/system managers are often laser-focused on the effort at hand with respect to implementation or deployment of systems and may not be as focused on privacy considerations.
- Labor privacy officials stated that they have experienced challenges in coordinating privacy requirements, given their cross-cutting nature. They added that portions of the privacy program reside in OCIO, the Office of Solicitor, and each component, and in many instances these are collateral duties and compete with other priorities.
- Treasury privacy officials noted that bureau and departmental privacy personnel regularly interact with information security, human capital, and budget personnel, but resource constraints do limit the degree of interaction envisioned in new requirements from Congress and OMB. They also stated many of the existing privacy requirements are dated and require updates to reflect changes in technology and shifts in how

information is collected, stored, and managed in the federal government.

Retaining Privacy Personnel

As the Federal Privacy Council and OPM have noted, to protect privacy, each agency needs experienced and educated privacy professionals.⁵¹ They further state that privacy is a multidisciplinary field that may require skills and expertise in such varied areas such as law, IT, and cybersecurity.

Fifteen of 24 agencies reported that retaining privacy personnel with needed skills and expertise is a challenge. Seven of these 15 stated this was a challenge due to personnel leaving for other opportunities with higher salaries and/or promotion opportunities. For example:

- DOD privacy officials reported that although many components do not report a challenge in this area, some components do report high turnover in privacy positions. They stated reasons for high turnover include combination of privacy responsibilities with other duties, such as FOIA, realignment, or normal rotations. This can undercut the strength of the component's privacy program due to a need to continuously hire and retrain.
- OPM privacy officials stated that lack of promotion opportunity can impede retention, leading to privacy staff leaving for other opportunities elsewhere. They added that, as a response to this, the agency created career ladders within available privacy vacancies to provide a career development path, which they anticipate, will benefit both the individuals and the agency.

Training Privacy Professionals

OMB and the Federal Privacy Council note that agencies need a well-trained privacy workforce, as well as providing appropriate training to the broader agency workforces. This includes developing, maintaining, and providing agency-wide privacy awareness and training programs for all employees and contractors, as well as specialized, role-based training for privacy professionals in the agency.

Fourteen of 24 agencies reported training of privacy professionals as a challenge. Three of these 14 agencies stated that the Federal Privacy

⁵¹Federal Privacy Council and U.S. Office of Personnel Management, *Toolkit for Recruiting, Hiring, and Retaining Privacy Professionals in the Federal Government* (January 2017).

Council boot camps⁵² have limited capacity, and therefore agencies can only send a limited number of staff to these training sessions. For example:

- HHS officials stated that while the Federal Privacy Council offers a robust, biannual federal-wide privacy training course for all new privacy professionals, their capacity is strictly limited and that HHS operating divisions have repeatedly been denied entrance due to these constraints. In addition, the training is open only to federal employees (and not to contractors).
- Department of State privacy officials stated that there are limited training opportunities specifically for privacy analysts. Privacy training is also available through the International Association of Privacy Professionals,⁵³ but it tends to cover non-government specific privacy laws. Additionally, officials stated that privacy training beyond introductory training is not available for more seasoned staff.
- Treasury privacy officials stated that annual privacy awareness training is effective for a period after the training is completed, but sufficient resources do not always exist to conduct further privacy awareness campaigns throughout the year. They also stated that updating annual training and mid-year privacy awareness campaigns are costly and their development is time-consuming. They added that one possible solution is for agencies to share existing annual privacy awareness training so it can be used by other agencies to allow agencies to update/refresh other agencies' annual training without the expense of creating it from scratch.

Challenges May Be Exacerbated by a Lack of Information Sharing

As noted previously, the privacy branch within OIRA is responsible for oversight of executive branch privacy implementation, including issuing policy and other guidance as appropriate. Further, the Federal Privacy Council, led by OMB, provides resources to agencies and a mechanism for collaboration and information sharing.

⁵²The Federal Privacy Council's Privacy Boot Camp is an 8-week program designed to provide foundational knowledge of Federal privacy laws and policies to federal personnel at all levels who are new to privacy roles. It serves as a central, standardized training resource for the executive branch. This program is held in the spring and fall of each year, is offered free of charge by the Federal Privacy Council and is open to executive branch employees.

⁵³Founded in 2000, the International Association of Privacy Professionals is a not-for-profit organization that is intended to help define, promote, and improve the privacy profession globally.

In discussing the challenges identified by agencies, OMB staff from OIRA's privacy branch noted that they would continue to issue policy through circulars and memoranda as appropriate. However, the same OMB staff did not identify specific initiatives under way to address the challenges related to applying privacy protections to new and emerging technologies. Agencies specifically noted that a lack of knowledge and expertise of how to apply privacy requirements to these technologies contributed to the challenge.

The staff added that OMB relies on the Federal Privacy Council and broader privacy community to identify implementation issues and challenges, and it works through its leadership of the council to facilitate development and sharing of best practices to address them. This includes activities through the council, its committees and work groups, as well as through communities of practice.

We agree that the Federal Privacy Council could provide a useful forum for sharing knowledge and expertise among agencies about applying privacy requirements to new technologies. However, OIRA privacy branch staff did not identify any such initiatives planned or under way. In particular, sharing strategies and best practices for applying privacy requirements to new technologies and integrating privacy and security requirements could assist agencies in addressing these challenges. Promoting such information sharing, through the Federal Privacy and Council and its subcommittees and communities of practice, could assist agencies in meeting the challenges they have identified, in turn strengthening their privacy programs.

Agencies and Experts Identified Benefits and Limitations of Privacy Impact Assessments

The 24 CFO Act agencies, as well as selected privacy experts, identified benefits to PIAs that included managing privacy risks, informing the public about agencies' handling of PII, and affecting the design of systems, among others. However, they also cited factors that may limit PIAs' effectiveness. These included that agencies do not always initiate PIAs early in the development of a program or system, privacy programs are not always aware of all agency systems requiring a PIA, and privacy programs may struggle to hold agency staff accountable for completing PIAs.

Benefits of Privacy Impact Assessments Include Managing Risks and Informing the Public

As previously discussed, the E-Government Act of 2002 requires agencies to conduct PIAs that analyze how personally identifiable information is collected, stored, shared, and managed in a federal

system.⁵⁴ Specifically, according to OMB guidance, the purpose of a PIA is to:

- ensure handling of PII conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and
- examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

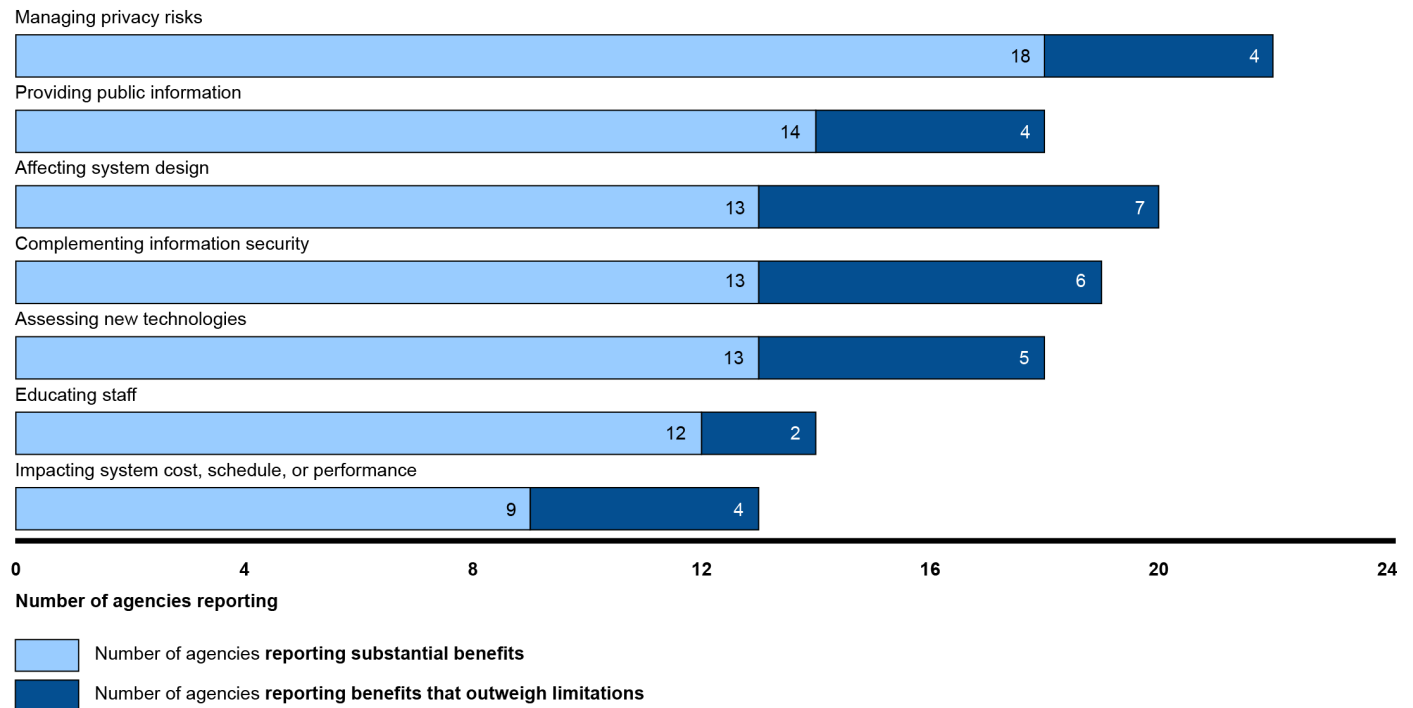
OMB guidance also states that PIAs should be made publicly available, except to the extent that publication would raise security concerns or reveal classified or sensitive information.⁵⁵

In their survey responses, the 24 CFO Act agencies identified benefits in agencies' use of PIAs to meet central goals regarding identifying and mitigating privacy risks and notifying the public about how PII is collected, used, and safeguarded. Specifically, many of the agencies reported that PIAs were generally beneficial for managing privacy risks, providing public information, and affecting system design. ("Generally beneficial" includes agencies whose survey responses indicated that PIAs had "significant benefits" or "benefits that outweigh limitations" for the specified purposes.) Most agencies also reported that PIAs had additional benefits in areas such as complementing information security activities; assessing new technologies; educating staff; and impacting system cost, schedule, or performance. Figure 3 shows the number of the 24 agencies who reported that PIAs are generally beneficial for specific purposes. More detail on the identified benefits is provided following the figure.

⁵⁴E-Government Act of 2002, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921 (Dec. 17, 2002).

⁵⁵The E-Government Act directs OMB to develop policies and guidelines for agencies on the conduct of privacy impact assessments; oversee the implementation of the privacy impact assessment process throughout the government; and require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form. OMB has issued PIA guidance in OMB Memorandum M-03-22 and OMB Circular A-130.

Figure 3: Number of the 24 Chief Financial Officers Act of 1990 Agencies Reporting that Privacy Impact Assessments Were Generally Beneficial



Source: GAO analysis of agency survey responses. | GAO-22-105065

Note: “Generally beneficial” includes agencies who responded that PIAs had “significant benefits” or “benefits that outweigh limitations” for the specified purposes.

- Managing privacy risks:** Twenty-two of 24 CFO Act agencies reported that their use of PIAs are generally beneficial for managing privacy risks. For example, one agency responded that documenting privacy risks and how to mitigate those risks, as well as having an independent senior agency official sign off on those risks and mitigation strategies, is extremely important. In addition, some agencies reported supplemental ways PIAs help them manage privacy risks. For example, four agencies explicitly stated that PIAs help ensure compliance with other privacy-related laws and regulations such as the Privacy Act.

Privacy experts also stated that the process of developing PIAs can help identify and mitigate privacy risks that may have otherwise gone undetected or unconsidered. For example, two experts described PIAs as a “speed bump” that can prevent agencies from making a

privacy-adverse decision without proper consideration. Another expert noted that developing PIAs compels stakeholders to consider privacy risks, even when privacy is not their primary responsibility, and can help inculcate a culture of privacy awareness.

- **Providing information to the public:** Eighteen of 24 agencies reported that PIAs are generally beneficial for informing the public about agencies' handling of PII. For example, one agency noted that PIAs increase transparency and public trust in agency handling of PII. Another agency specified that PIAs allow interested members of the public to learn about the agency's systems. A third agency noted that PIAs support open government.

Privacy experts agreed that publishing PIAs provides useful information to the public. For example, one expert explained that PIAs may often be the only public source of information that sufficiently describe an agency system or a particular collection of PII. Another expert noted that PIAs may be most helpful to advocacy groups and media organizations, who can then present the content to the general public.

- **Affecting system design:** Twenty of 24 agencies reported that PIAs are generally beneficial for affecting system design. For example, one agency noted that the completion of a PIA requires a more thorough examination of the system to ensure privacy is being managed appropriately, thereby helping ensure privacy considerations are considered in the design and of programs and systems. Officials at another agency stated that staff participating in the development of a PIA become more aware of relevant privacy concerns during security assessments and the system authorization process. They emphasized that the questions asked during the development of a PIA are designed to instruct, inform, and determine privacy risks early in the development stage of a program.

Thirteen agencies also noted that involving the privacy program early in a system's life cycle helps ensure that the PIA can have an impact on system design. For example, one agency reported that if a privacy staffer is involved in the design and planning phase of a system, PIAs are more likely to reflect privacy considerations. Privacy experts also stated that PIAs can benefit a system's design by, for example, forcing stakeholders to consider requirements beyond information security—such as purpose limitation and data minimization.

- **Complementing information security activities:** Nineteen of 24 agencies reported that PIAs are generally beneficial in complementing

information security activities. Five agencies specified that PIAs are generally part of a system's authorization to operate package, and that the package requires collaboration with the information security team. Privacy experts we spoke with also noted that PIAs can provide a public-facing discussion of security practices and that the overall integration of privacy and security is beneficial.

- **Assessing risks of new technologies:** Eighteen of 24 agencies reported that PIAs are generally beneficial with respect to addressing new technologies. Specifically, 16 agencies reported that their current PIA policies, processes, and templates are flexible enough to cover new and emerging technologies, such as robotic process automation⁵⁶ and artificial intelligence. As an example, one agency official stated that, while new technologies will require an analysis of privacy implications, the type of information considered to be PII does not change. Officials at two other agencies stated that their PIA process helps increase engagement with technical experts in program offices when assessing new technologies' privacy risks.
- **Educating agency staff about privacy:** Fourteen of 24 agencies reported that PIAs are generally beneficial for educating new staff about privacy issues and requirements. Thirteen agencies specified that the development of a PIA raises awareness of privacy issues for staff involved in the process. For example, one agency noted that PIAs require collaboration between component staff and the privacy office, enabling broader perspectives and highlighting where additional privacy education is necessary. Privacy experts also mentioned this benefit, noting, for example, that repeated exposure to the privacy program through the development of PIAs can lead to a change in culture and increased awareness.
- **Impacting system cost, schedule, and performance:** Thirteen of 24 agencies reported that PIAs are generally beneficial for impacting system cost, schedule, or performance. For example, one agency noted that PIAs help identify needed system upgrades and changes based on what kind of information the system contains. In addition, nine agencies specified that early initiation of PIAs helps avoid negative impacts to cost and schedule, such as by minimizing delays and work stoppages that may occur in the event appropriate privacy controls were not effectively implemented.

⁵⁶Robotic process automation is the use of software scripts to perform tasks as an automated process that no longer requires the use of human input.

Limitations May Hinder Effectiveness of Privacy Impact Assessments

Although CFO Act agencies and experts identified significant benefits of PIAs, they also identified limitations in ensuring that (1) PIAs are initiated early enough to impact system design decisions, (2) privacy offices are aware of all systems that may require a PIA, and (3) privacy offices are able to hold agency staff accountable for completing PIAs.

- **PIAs are not always initiated early in system development.** Only six of 24 agencies reported that they “always” initiate PIAs sufficiently early to affect program or system design decisions, while 18 agencies reported that they “sometimes” initiate PIAs sufficiently early. For example, one agency stated that PIAs are frequently done after the program or system is mostly or wholly complete. An official at another agency noted that while their typical practice is to initiate a PIA at least 90 days prior to the system’s authorization to operate, there may be occasions where a system needs to be implemented more quickly. One other agency official noted that the timing of PIAs was uneven among its components, and that components department-level privacy staff work with on a regular basis are more likely to initiate privacy conversations early.

As noted above, agencies stressed that the early initiation of PIAs is important for realizing benefits such as affecting significant program and system design decisions. Similarly, experts we spoke to stated that it is not rare for the initiation of a PIA to occur after significant program decisions have been made. In these cases, they noted, PIAs generally describe the program “as is” rather than being able to affect the direction or design of the program. Multiple experts stated that forcing early discussions with privacy and other stakeholders would be their top priority for improving the quality and effectiveness of PIAs.

- **Agency privacy programs may not be aware of all systems that require a PIA.** Twelve agencies said they were sometimes aware of all such systems and one agency said they were never aware of all such systems. For example, five agencies explained that privacy programs may not be aware of systems or tools an agency uses that collect PII when those systems do not go through a process, such as an authorization to operate, that triggers a PIA. The agencies cited examples of IT that may not go through such a process as cloud-based⁵⁷ offerings and existing technology that gets repurposed. In addition, officials at two agencies stated that their components vary in

⁵⁷As noted above, cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released.

how engaged they are with agency privacy programs, and another noted that the department-level privacy program relies on offices and components to report IT that may involve PII. Further, one agency noted that their privacy offices may have limited visibility into the activities of program offices and the offices may only become aware of systems after they have already been developed.

We have previously found that agency privacy programs may not be aware of all systems that require a PIA when the system is deployed by a business unit without notifying the privacy program. Specifically, in June of 2021 we found that 13 of 14 agencies did not have awareness of what non-federal facial recognition systems were being used by employees and thus had not fully assessed potential privacy risks of using those systems.⁵⁸

- **Privacy programs may not be able to hold program offices or system owners accountable for completing PIAs.** Most agencies reported that they were not always able to hold program offices accountable for timely initiation of PIAs. Specifically, 12 stated that they were sometimes able to hold staff accountable and one agency said they were never able to hold staff accountable. For example, one agency noted that component privacy offices may lack influence or be unable to hold other program offices accountable, and that local policies and procedures that may not adequately require PIA completion at the correct stage of the process. Another agency stated that department policy may not have accountability mechanisms, while another reported that program staff may not perceive the value of completing PIAs. Finally, one agency pointed to the high volume of PIAs as contributing to the difficulty of holding staff accountable.

Experts also expressed concerns that agency privacy programs are unable to hold program offices accountable for drafting and approving PIAs. Experts pointed to an apparent lack of substantive enforcement mechanisms if a program does not develop a PIA, and identified examples of systems with significant privacy impacts operating for years without an accurate PIA or any PIA.

Agencies and Experts Identified Resources That Could Enhance Benefits of PIAs

Agencies and experts also identified tools and resources that could help improve PIAs. They noted that templates or guidance for creating PIAs for different types of IT systems or procurements could help lighten the burden on agencies and increase government transparency:

⁵⁸GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, [GAO-21-518](#) (Washington, D.C.: June 3, 2021).

-
- Seven agencies stated that additional sharing of completed PIAs and best practices could assist agencies in completing their PIAs. For example, one agency expressed a need for guidance on roles and responsibilities for conducting PIAs for agency systems, shared services, cloud services, web applications, grant systems, etc. to address growing complexities and challenges. Another agency expressed a desire for training or sharing of best practices from agencies with expertise in developing PIAs. Three agencies noted that a more standardized template or PIA form would be useful for ensuring that PIAs contain consistent types of information. One agency suggested that having a centralized repository of agency PIAs could make them more accessible.
 - Privacy experts, particularly from government, agreed that sharing example PIAs, templates for different types of systems, and expertise would be helpful. Another expert pointed out that sharing has been helpful at reducing unnecessary duplication in countries where PIAs are more widespread. Other experts noted that a central government website for PIAs could increase transparency and make it easier for interested members of the public to access PIAs relevant to their needs or interests. They noted that it can be difficult for interested members of the public to track agency activities when PIAs are posted on disparate websites across agencies.

In discussing these matters, OIRA privacy branch staff did not identify any specific steps planned or under way to provide such additional resources. Specifically, OIRA staff stated that while they encourage the sharing of agency expertise and best practices, for which the Federal Privacy Council provides a ready forum, a PIA is not a “check-the-box” or “one-size-fits-all” compliance tool. Rather, they stated that developing a PIA requires that SAOPs work closely with program managers, information system owners, and other relevant agency officials. They added that a PIA is a living document that agencies are required to update when changes to the information technology, agency practices, or other factors alter the privacy risks.

However, given the proliferation of technology and data collection with privacy implications, encouraging additional sharing of information and resources could help agencies implement more efficient and effective PIA processes. It could assist them in identifying approaches to common types of systems while still allowing them to focus appropriate attention and resources on unique, high-value, or particularly sensitive resources.

Most Senior Agency Privacy Officials Do Not Have Privacy as Their Primary Assigned Duty

We have previously reported that the single most important element of successful government improvement initiatives—such as strategic efforts to address major challenges—is the demonstrated commitment of top leaders.⁵⁹ Recognizing new challenges in ensuring privacy, in 2016, Executive Order 13719 required agencies to designate or re-designate a Senior Agency Official for Privacy with the experience and skills necessary to manage an agency-wide privacy program. OMB’s guidance on implementing this requirement, issued in 2016, was intended to help ensure that agencies were able to meet such new challenges arising from innovations in technology and advancements in information analytics that have led to the ability to collect, process, maintain, and disseminate an unprecedented amount of PII.⁶⁰

Toward that end, OMB specified that the SAOP was intended to serve in a senior leadership position in the agency and be positioned high enough within the agency to regularly engage with other agency leadership, including the head of the agency. Further, the SAOP was expected to have the necessary skills, knowledge, and expertise to lead and direct the agency’s privacy program and carry out the privacy-related functions described in law and OMB policies. Finally, the SAOP was to have the necessary authority at the agency to lead and direct the agency’s privacy program and carry out the privacy-related functions described in law and OMB policies.

As noted above, all 24 agencies have designated an SAOP, as required by OMB guidance. However, a key factor that likely contributed to agency shortcomings and challenges in implementing their privacy programs is that most SAOPs are not focused on privacy as their primary—or one of their primary—duties.

Specifically, half of the agencies designated their CIO or Deputy CIO as SAOP. However, as we have previously reported, CIOs in particular are also tasked with carrying out numerous functions in key IT areas, including leadership and accountability, strategic planning, workforce, budgeting, investment management, and information security. Moreover,

⁵⁹GAO, *Government Performance: GPRM Modernization Act Provides Opportunities to Help Address Fiscal, Performance, and Management Challenges*, [GAO-11-466T](#) (Washington, D.C.: Mar. 16, 2011).

⁶⁰OMB M-16-24.

we found that agency CIOs were not always effective in carrying out these assigned duties and faced various challenges in doing so.⁶¹

Other designated SAOPs included officials such as the agency Chief Administrative Officer, Deputy Assistant Secretary for Operations, Deputy Assistant Secretary for Global Information Services, Assistant Secretary for Management, General Counsel, and Acting Deputy Administrator. By contrast, few agencies had assigned the role of SAOP to an official whose primary duties were privacy-related.

Officials with primary duties other than privacy are unlikely to spend a majority of their time focused on privacy, and, as we found, agencies generally delegated operational aspects of their privacy programs to less-senior officials. This makes it less likely that SAOPs will focus their attention on privacy in discussions with other senior agency leaders. For example, OMB guidance notes that agencies should recognize that privacy and security are independent and separate disciplines and that, while privacy and security require coordination, they often raise distinct concerns and require different expertise and different approaches.

A senior official dedicated to privacy could be better positioned to ensure that key elements of a privacy program are fully implemented and challenges are addressed. As noted above, gaps we identified in agency policies and procedures often related to areas that highlighted the cross-cutting nature of privacy and the need for an agency's privacy program to coordinate with other senior officials, such as the CIO, CISO, or Chief Human Capital Officer. Moreover, the challenges reported by agencies involved, among others, marshalling resources, ensuring an adequate workforce, ensuring that agency programs comply with requirements, and coordinating with other agency programs and functions. Such an official could be better positioned to ensure a consistent focus on privacy at the level of senior leadership, facilitate cross-agency coordination, and elevate the importance of privacy:

- **Ensure consistent focus on privacy:** A senior-level official with primarily privacy-related duties could help ensure a consistent focus on privacy. For example, OMB staff from OIRA's privacy branch suggested that codifying the role of the senior agency privacy official in statute as a CPO (analogous to a CIO or Chief Data Officer) would support privacy programs' development. They stated that a codified

⁶¹GAO, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*, [GAO-18-93](#) (Washington, D.C.: Aug. 02, 2018).

CPO role would help support agencies in obtaining more resources, hiring more staff, and having a senior privacy official focus solely on privacy, rather than having multiple roles within the agency and various other responsibilities. Further, privacy officials at DOJ, where the Chief Privacy and Civil Liberties Officer is required by law,⁶² stated that it is essential for a senior official to have privacy responsibilities and only those responsibilities, as well as the relevant knowledge, skills, and expertise.

- **Facilitate cross-agency coordination:** As discussed previously, many agencies had not fully developed policies and procedures for ensuring coordination between privacy and other key agency functions. A senior-level official with primarily privacy-related duties could better facilitate cross-agency coordination. For example, OIRA privacy branch staff stated that a CPO codified in statute at a level comparable to a CIO or other senior executive would empower these officials to develop more mature privacy programs with robust cross-agency relationships, processes, and technology. Similarly, two agencies with a statutory, senior-level CPO (DHS and DOJ), had generally established comprehensive policies for complying with privacy requirements and ensuring coordination with other key agency activities, such as budget review and workforce planning. In addition, DHS privacy officials stated that having the CPO at the department level with sufficient authority is important for ensuring cohesion in cases where components have their own privacy programs. In addition, in February 2021, a member of the Federal Privacy and Civil

⁶²Specifically, DHS and DOJ are statutorily required to have a chief privacy officer responsible for leading their privacy programs. The Homeland Security Act of 2002, as amended, creates the Chief Privacy Officer at DHS with responsibilities to ensure privacy and transparency in government are implemented throughout the department. 6 U.S.C. § 142. In addition, the Violence Against Women and Department of Justice Reauthorization Act of 2005, as amended, required the Attorney General to designate a senior official in the DOJ to assume primary responsibility for privacy policy. Pub. L. No. 109-162, § 1174, 119 Stat. 2960, 3124 (Jan. 5, 2006). In 2006, the DOJ created the position of the Chief Privacy and Civil Liberties Officer in the Office of the Deputy Attorney General and subsequently established the Office of Privacy and Civil Liberties to support the duties and responsibilities of the Chief Privacy and Civil Liberties Officer.

Liberties Oversight Board⁶³ published an article advocating for agencies to have CPOs as full-time dedicated officials reporting to the heads of their respective agencies.⁶⁴ Such officials, he argued, should be empowered with authority to oversee and address all privacy issues across the agency, including the power to investigate and enforce compliance.

- **Elevate the importance of privacy:** As noted previously, we have identified protecting the privacy of PII as a government-wide high-risk issue since 2015. A senior-level official with primary responsibility for privacy could help elevate the importance of privacy at an agency and help ensure that it receives sufficient attention from agency top leadership. OIRA privacy branch officials stated that statutory status of CPOs would strengthen agency privacy programs by ensuring that the senior privacy officials have a seat at the table alongside other statutory officials with responsibilities related to agency data governance, such as CIOs. They added that such a role would help ensure that privacy programs are able to address identified challenges, including resources, hiring and retaining staff, and ensuring privacy awareness and coordination across agencies. DHS privacy officials emphasized that the DHS CPO reports directly to the DHS Secretary (as opposed to a chief of staff or deputy secretary), and that having direct access to the department head makes a critical difference in how privacy is perceived and the importance it is given. The aforementioned privacy expert also maintained that by creating and elevating the CPO role, agency heads will better ensure privacy issues are seen, heard, and prioritized, thereby increasing the likelihood that they are handled appropriately and consistently across the federal government.

Establishing such a role in statute could help ensure more consistent implementation of privacy programs across the government by elevating the visibility of privacy and establishing top-level leadership commitment.

⁶³Originally established in the Executive Office of the President by the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1061, 118 Stat. 3638, 3684 (Dec. 17, 2004), the Privacy and Civil Liberties Oversight Board was made an independent agency within the Executive Branch by the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 801, 121 Stat. 266, 352 (Aug. 3, 2007). The bipartisan, five-member Board is appointed by the President and confirmed by the Senate. The Board's mission is to ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties.

⁶⁴Travis LeBlanc, "It is time for federal chief privacy officers," The Hill (Feb. 12, 2021), accessed Mar. 15, 2022, <https://thehill.com/blogs/congress-blog/politics/538571-it-is-time-for-federal-chief-privacy-officers?rl=1>.

In addition, appropriately empowered leadership could help address challenges agencies identified. This particularly includes challenges related to ensuring adequate resources, prioritizing the hiring and retention of privacy staff, and coordinating with other agency programs to make sure that privacy is fully considered in key activities and that agency staff are effectively trained and fully aware of their responsibilities related to privacy. Such empowered leadership could also help ensure that agency privacy programs are fully implementing key practices, as well as improving the effectiveness and consistency of PIAs, by, for example, ensuring that privacy programs are aware of all systems with PII and that staff are held accountable for completing PIAs. Without such dedicated senior-level leadership, agencies could continue to struggle to fully implement key privacy practices and address the challenges they have identified.

Conclusions

The large amount of PII collected by federal agencies, along with the increasing sophistication of technology, highlights the importance of strong programs for ensuring privacy protections. Such programs are especially critical when considering recent breaches involving PII that have affected hundreds of thousands of people.

The 24 CFO Act agencies have established privacy programs with overall responsibility for privacy policy, compliance, and risk management. However, the agencies have not fully established policies and procedures for implementing certain key practices. These include cross-agency activities such as reviewing IT budget proposals, workforce planning, and managing risks to IT systems that contain PII. Without fully establishing these elements of the privacy programs, agencies will have less assurance that they are consistently and effectively implementing privacy protections.

The 24 agencies identified several challenges in implementing their privacy programs. Among these are a lack of sufficient resources, especially enough privacy staff with the skills needed to carry out their duties, as well as challenges in effective cross-agency coordination and accountability for implementing privacy requirements. Agencies also identified challenges with applying privacy protections to new technologies, integrating privacy and security requirements, and using federal guidance. While OIRA privacy branch officials did not identify specific efforts planned or under way, additional information sharing, via the Federal Privacy Council or another channel, could help agencies address some of these challenges.

Both agencies and privacy experts identified benefits of privacy impact assessments—particularly in managing privacy risks and providing important information to the public about agencies’ use and management of PII. However, agencies indicated limitations in their ability to ensure that PIAs are initiated in a timely manner, that all systems with PII receive PIAs, and that staff are held accountable for completing them. Empowered privacy leadership could help ensure that PIAs are prioritized and completed for all agency systems with PII. Lastly, although OIRA privacy branch officials did not identify specific efforts planned or under way, opportunities exist for additional information sharing among agencies regarding best practices on PIAs.

Addressing key privacy program practices, program challenges, and privacy impact assessment effectiveness requires significant leadership commitment at agencies. However, most agencies lack senior-level leadership solely focused on privacy, who can marshal resources and elevate the visibility of the privacy program to ensure effective coordination across the organization. While agencies have designated Senior Agency Officials for Privacy, these officials generally have other demanding responsibilities, leading them to delegate many of the duties to other staff. Establishing a statutory CPO position for agencies that lack one could provide the strong leadership needed to meet these challenges and to ensure more consistent implementation of agencies’ privacy programs.

Matter for Congressional Consideration

Congress should consider legislation to designate a senior privacy official, such as a chief privacy officer, at agencies that currently lack such a position. This position should have privacy as its primary duty, the organizational placement necessary to coordinate with other agency functions and senior leaders, and the authority to ensure that privacy requirements are implemented and privacy concerns are elevated to the head of the agency.

Recommendations for Executive Action

We are making the following two recommendations to OMB:

The Director of OMB should take steps to promote, through the Federal Privacy Council or other channels, sharing of information and best practices to help agencies address challenges identified in this report, including the application of privacy requirements and risk management to new and emerging technologies and integrating security and privacy controls. (Recommendation 1)

The Director of OMB should take steps to promote, through the Federal Privacy Council or other channels, the sharing of information, best

practices, and other resources related to conducting privacy impact assessments. (Recommendation 2)

We are also making a total of 62 recommendations to 23 of the 24 Chief Financial Officers Act agencies in our review to fully address key practices in their privacy policies and procedures. These recommendations are in appendix II.

Agency Comments and Our Evaluation

We requested comments on a draft of this report from OMB and the 24 CFO Act agencies included in our review. All the agencies provided responses, as discussed below.

In email comments received on August 15, 2022, subject matter experts from OMB's Office of Information and Regulatory Affairs stated that they agreed with the two recommendations. They further noted that they would continue to work through the Federal Privacy Council and other channels to work toward implementing the recommendations.

In addition, the staff from OMB stated that they see codification in statute of a senior privacy official position, such as a Chief Privacy Officer, in federal agencies as a key step in addressing the specific issues that were the focus of our report. They also see it as essential to ensuring that agency privacy programs can successfully carry out the host of other critical responsibilities associated with managing personally identifiable information, for which SAOPs are responsible.

Of the 24 CFO Act agencies, 19 agencies (USDA, Commerce, DOD, Education, Energy, HHS, DHS, DOI, DOL, State, DOT, VA, EPA, GSA, NASA, NRC, SBA, SSA, and USAID) concurred with our recommendations. In addition, one agency (OPM) partially concurred with our recommendations; one agency (DOJ) did not concur with our recommendations; and one agency (HUD) provided comments but did not state whether it agreed or disagreed with our recommendations. Lastly, two agencies (Treasury and NSF) stated that they had no comments on the report. Multiple agencies also provided technical comments, which we incorporated as appropriate.

The following 19 agencies concurred with our recommendations and, in several cases, described steps planned or under way to address them:

- The Department of Agriculture's Audit Liaison Official provided comments via email on July 29, 2022, which stated that the department generally agreed with the findings and recommendations in the report.

-
- The Department of Commerce sent written comments stating that it agreed with our recommendation and planned to develop a formal action plan upon issuance of the final report. Commerce's comments are reprinted in appendix V.
 - The Department of Defense sent written comments stating that it concurred with our recommendations and would take steps to address them. DOD's comments are reprinted in appendix VI.
 - The Department of Education provided written comments which stated that it concurred with our recommendation and described plans under way to address it. In particular, the department noted that it has already begun updating existing privacy policies, including those related to compliance with the Privacy Act, as well as those establishing and administering the privacy program. Education's comments are reprinted in appendix VII.
 - The Department of Energy sent written comments which stated that the department concurred with our recommendations. It further described planned actions to implement them and estimated completion dates. For example, the department noted that it plans to update the duties of privacy officials with respect to workforce planning, integrate privacy into its risk profile process, and update its privacy program order to address privacy officials' roles in key risk management steps. DOE's comments are reprinted in appendix VIII.
 - The Department of Health and Human Services provided written comments on the report and stated that it concurred with our recommendation. The department further described actions planned to address the recommendation. Specifically, it intends to address the recommendation in an update to its Policy for Information Security and Privacy Protection. HHS's comments are reprinted in appendix IX.
 - The Department of Homeland Security sent written comments stating that the department concurred with our recommendations. It further described planned actions to implement them and estimated completion dates. For example, DHS stated that it intends to incorporate risk tolerance into its privacy risk management tools; review and update policies and instructions that advance and reinforce privacy policies, procedures, and programs across the enterprise; and fully establish a privacy continuous monitoring strategy. DHS's comments are reprinted in appendix X.
 - The Department of the Interior provided written comments in which it stated that it concurred with our recommendation. Interior's comments are reprinted in appendix XI.

-
- The Department of Labor’s Audit Liaison sent comments via email on July 20, 2022, which stated that the department concurred with our recommendations and would take steps to address them.
 - The Department of State provided written comments, which stated that it concurred with our recommendations, and described plans under way to address them. Specifically, it noted that the privacy program will work with other relevant bureaus within the department to implement the recommendations. The comments are reprinted in appendix XII.
 - The Department of Transportation’s Deputy Director, Audit Relations and Program Improvement, provided comments via email on July 14, 2022, which stated that the department concurred with our recommendations.
 - The Department of Veterans Affairs provided written comments, which stated that the department concurred with our recommendations. In addition, VA stated that it had already taken action to implement our recommendation to fully establish its privacy continuous monitoring strategy and requested closure of the recommendation. We will work with the department to verify completion of these actions. VA’s comments are reprinted in appendix XIII.
 - The Environmental Protection Agency provided written comments, stating that the agency concurred with our recommendation. The comments further described actions planned to address the recommendation, along with an estimated completion date. In particular, EPA stated that it intends to update its Information Security Continuous Monitoring plan by February 17, 2023, to include the privacy control continuous monitoring requirements. EPA’s comments are reprinted in appendix XIV.
 - The General Services Administration provided written comments, stating that the agency agrees with the recommendations and is developing a plan to address them. GSA’s comments are reprinted in appendix XV.
 - The National Aeronautics and Space Administration provided written comments stating that the agency concurred with our recommendations. The comments further describe actions planned to address the comments and estimated completion dates. Specifically, the agency stated that the recommendations will be addressed in existing policy documents and estimated that these efforts would be completed in December 2022. NASA’s comments are reprinted in appendix XVI.

-
- The Nuclear Regulatory Commission provided written comments stating the agency concurred with our recommendations and describing actions planned to address them. In particular, the agency stated that it plans to revise the appropriate policies and procedures to address the recommendations. NRC's comments are reprinted in appendix XVII.
 - The Small Business Administration provided written comments stating that the agency concurred with our recommendation. SBA's comments are reprinted in appendix XVIII.
 - The Social Security Administration provided written comments stating that the agency agreed with our recommendations. SSA's comments are reprinted in appendix XIX.
 - The U.S. Agency for International Development provided written comments stating that the agency agreed with our recommendations. The comments described actions planned or under way to address the recommendations, along with estimated completion dates. For example, the agency stated that it plans to include the SAOP's input as a voting member of the agency's Information Technology Steering Subcommittee and plans to update the agency's risk appetite statement to acknowledge the overlap between privacy and cybersecurity risks. USAID's comments are reprinted in appendix XX.

In email comments received on August 2, 2022, the Department of Housing and Urban Development's Chief Privacy Officer did not state whether they agreed or disagreed with our recommendations, but generally agreed with our report.

Two agencies—DOJ and OPM—either did not concur with our recommendations, or partially concurred. Their comments and our response are summarized below:

In an email received on August 1, 2022, an Assistant Director from the Department of Justice's Audit Liaison Group transmitted the department's comments. In these comments, the department stated that it did not concur with our two recommendations. Specifically, the comments stated that the department does not concur with the recommendation to incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance. The comments noted that DOJ's cybersecurity program order defines minimum cybersecurity and privacy requirements for all DOJ components, personnel, and information systems that process, store, or transmit DOJ information. The comments further stated that the order describes how DOJ identifies, assesses, and

responds to privacy risks. In addition, DOJ's comments stated that the department's Cyber Security Assessment and Management tool captures security and privacy control assessment status and incorporates privacy into department-wide risk management. This is to include a determination of risk tolerance based on the system categorization and assigned risk levels.

However, documentation provided by DOJ, including the cybersecurity program order, does not explicitly discuss the department's approach to determining privacy risk tolerance, including, for example, factors to be considered and acceptable amounts of risk (e.g., thresholds). As NIST guidance notes, risk tolerance affects all parts of the organization's risk management process, having a direct impact on the risk management decisions made by senior leaders or executives throughout the organization and providing important constraints on those decisions. Explicitly defining its approach to risk tolerance would help DOJ ensure that privacy risk management is implemented consistently across the department and based on clear statements of the acceptable amount of risk. Accordingly, we continue to believe that our recommendation is warranted.

DOJ also did not concur with the recommendation to establish a time frame and fully develop and document a privacy continuous monitoring strategy. The comments stated that DOJ's privacy continuous monitoring Strategy is documented in both the department's *Information Security and Privacy Continuous Monitoring Strategy* and the its *Security and Privacy Assessment and Authorization Handbook*. Specifically, the comments stated that DOJ components must assess all security and privacy controls employed by an information system during initial authorization and assess a subset of controls during continuous monitoring on an ongoing basis.

However, documents provided by DOJ—including its *Continuous Monitoring Strategy, Assessment and Authorization Handbook*, and a plan for moving to revision 5 of NIST Special Publication 800-53—do not specify the frequency with which the department plans to assess each privacy control at the various risk management tiers. OMB guidance notes that agencies should develop a written privacy continuous monitoring strategy that catalogs the available privacy controls implemented at the agency across the risk management tiers and assigns an assessment frequency to each control. Accordingly, we continue to believe that our recommendation is warranted.

The Office of Personnel Management provided written comments (reprinted in appendix XXI) in which it partially concurred with four of our

recommendations and did not concur with two recommendations. Specifically:

- OPM partially concurred with our recommendation to establish a time frame for updating the agency's policy for creating, reviewing, and publishing system of records notices, and make these updates. The agency noted that it concurs with the concept that fully documented processes for creating, reviewing, and publishing SORNs are beneficial. However, it did not concur with the implication that OPM has no process in place and is impeding publication of SORNs. OPM described the process it follows for creating, reviewing, and publishing SORNs, while acknowledging that more fully documenting guidance and process regarding SORNs will benefit OPM. OPM added that it is committed to reviewing and updating any outdated SORN guidance by the close of fiscal year 2023.

We acknowledge that a lack of fully documented processes does not necessarily prevent an agency from developing, reviewing, and publishing SORNs. However, we continue to believe that documenting up-to-date policies and procedures can help ensure consistent processes. If appropriately implemented, OPM's plans to update its guidance should address the intent of our recommendation.

- OPM also partially concurred with our recommendation to define and document procedures for coordination between privacy and information security functions. In particular, the agency described activities that it undertakes which include coordination between privacy and information security. These include participation in the agency's Investment Review Board and Risk Management Council, as well as meetings to discuss issues affecting information security and privacy. However, the agency also noted that during fiscal year 2023 it will evaluate the need for increased documentation of the coordination between the privacy and security functions.

We acknowledge that such coordination as OPM described can occur in the absence of formal, documented policies and procedures. However, such policies and procedures can help ensure that coordination continues on a regular and consistent basis, including when changes in staff or other changes occur at an agency. Accordingly, we continue to believe that our recommendation is warranted.

- OPM partially concurred with our recommendation to establish a time frame for fully defining the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system

categorizations, overseeing privacy control assessments, and reviewing authorization packages, and document these roles. In particular, OPM stated that the privacy team is involved in various activities related to this process. The agency further noted that the privacy and security teams are currently examining roles and responsibilities with respect to the controls and their selection and evaluation. The agency added that it is evaluating with OCIO colleagues whether and how to better document this and the appropriate time frame for doing so.

As noted above, without fully documenting the roles of privacy officials in authorizing information systems with PII, agency privacy programs will be hindered in ensuring that privacy protections are adequately incorporated into those systems. In reviewing OPM's policies and procedures, we found that existing guidance preceded the establishment of the privacy program as a stand-alone office separate from the Office of the CIO. Thus, these policies and procedures did not reflect the agency's current operating environment. Accordingly, we continue to believe that the agency should document the specific roles that privacy officials are to play in this process, as called for by OMB guidance, and that our recommendation is warranted.

- OPM partially concurred with our recommendation to fully develop and document a privacy continuous monitoring strategy. Specifically, the agency stated that it has a current continuous monitoring strategy in place which provides a comprehensive view of each system, including privacy controls, at a defined frequency. OPM added that as it moves to implement NIST 800-53 rev. 5, it will further evaluate its approach to privacy continuous monitoring and review the need for more comprehensive documentation by the end of fiscal year 2023.

OPM did provide information on its approach to privacy continuous monitoring, noting that it relies on privacy threshold assessments and privacy impact assessments. In addition, OPM officials noted that the agency addresses continuous monitoring through a variety of activities, not only for security and systems controls issues, but also at the management and program level. However, OPM did not document a privacy continuous monitoring strategy that identifies controls at the various risk management tiers (organizational, program, system level) and types (program management, common, hybrid, system) and identifies how they will be monitored and at what frequency, as called for by OMB guidance. Accordingly, we continue to believe that our recommendation is warranted.

-
- OPM did not concur with our recommendation to fully define and document a policy and process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. In particular, the agency noted that OPM's SAOP is a member of the Senior Executive Service and the office head for the Office of Privacy and Information Management, the central OPM office that houses OPM's centralized privacy program. The agency further noted that the SAOP is responsible for evaluating the hiring, training, and professional development needs of the office generally and the privacy program specifically. OPM added that the agency provided evidence to support the fact that the SAOP is responsible for meeting the hiring needs of the agency regarding privacy. Further, OPM described activities the privacy office had undertaken, both on its own and in coordination with the Office of the CIO, to address hiring needs.

We acknowledge that OPM has taken actions in this area. However, our concern is that OPM has not formalized the role of the SAOP in addressing hiring, training, and professional development needs with respect to privacy. As OPM noted, it did provide evidence of such involvement; this consisted of a January 2020 memo from the Director of the Privacy Office to the OPM Director outlining strategic workforce needs for the Office of Privacy and Information Management. However, OPM had not formalized this role in a policy that would require SAOP involvement on a regular, ongoing basis. Formalizing this role in policy would strengthen the privacy program's ability to advocate for the skilled and qualified staff it needs on an ongoing basis. Accordingly, we continue to believe that our recommendation is warranted.

- Finally, OPM did not concur with our recommendation to incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance. In particular, the agency stated that the Senior Agency Official for Privacy has been a member of the OPM Risk Management Council, the OPM body that identifies, evaluates, and works to mitigate enterprise-wide risk, since approximately 2017. OPM added that the council's risk registers consistently address privacy risks at the enterprise level, and the privacy team address risk at a program level through Privacy Threshold Analyses and Privacy Impact Assessments.

While we acknowledge the benefits of having an agency's SAOP participate in an agency-level risk management council, this does not

replace the need for a documented risk management strategy in which the agency explicitly frames its approach to privacy risk. As NIST guidance notes, the risk management strategy guides and informs risk-based decisions including how security and privacy risk is framed, assessed, responded to, and monitored. This includes an explicit discussion of the agency's risk tolerance. Accordingly, we continue to believe that our recommendation is warranted.

Finally, two agencies stated that they had no comment on the report. In email comments received on July 28, 2022, the Director of Privacy and Civil Liberties at the Department of the Treasury stated that the department had no comments on the report. Similarly, in email comments received on July 25, 2022, the Policy, Audit, and Enterprise Risk Management analyst from NSF stated that the agency had no comments on the report. We did not make any recommendations to NSF.

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

If you or your staff have any questions about this report, please contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov, or Marisol Cruz Cain at (202) 512-5017 or cruzcaim@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix XXII.



Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity



Marisol Cruz Cain
Director, Information Technology and Cybersecurity

List of Requesters

The Honorable Gary C. Peters

Chairman

The Honorable Rob Portman

Ranking Member

Committee on Homeland Security and Governmental Affairs

United States Senate

The Honorable Ron Johnson

Ranking Member

Permanent Subcommittee on Investigations

Committee on Homeland Security and Governmental Affairs

United States Senate

Appendix I: Objectives, Scope, and Methodology

The objectives of this report were to examine:

1. The extent to which agencies have established privacy programs with authority and responsibility for ensuring privacy protections for agency programs.
2. Challenges agencies have reported experiencing in implementing their privacy programs, and what, if any, government-wide initiatives are under way to address them.
3. Reported benefits and limitations in agencies' use of privacy impact assessments (PIAs).
4. The extent to which agencies have senior leadership dedicated to privacy issues.

In conducting this engagement, we focused on the 24 Chief Financial Officers Act of 1990 (CFO Act) agencies.¹

For the first objective, we identified key practices for establishing privacy programs based on a review and analysis of federal laws, policy, and guidance. We reviewed laws including the Privacy Act of 1974 and the E-Government Act of 2002, as well as Executive Order 13719: *Establishment of the Federal Privacy Council*. Guidance we reviewed included the Office of Management and Budget's (OMB) M-16-24: *Role and Designation of Senior Agency Officials for Privacy*, Circular A-130: *Managing Information as a Strategic Resource*, and National Institute of Standards and Technology (NIST) Special Publication 800-37. Because our objective was focused on establishing agency privacy programs, we selected practices that address the general requirements of a privacy program outlined in OMB A-130, appendix II. These requirements lay the foundation for comprehensive privacy programs that develop and evaluate privacy policy, manage privacy risks, and ensure compliance with applicable privacy requirements. We also included requirements from

¹The CFO Act, 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 CFO 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.

the other elements of a privacy program that overlap with the general requirements and are directly related to senior agency official for privacy (SAOP) involvement in managing privacy risks per the requirements laid out in OMB M-16-24.

We then assessed the extent to which the 24 CFO Act agencies have established programs for ensuring privacy protections in accordance with these practices. To do so, we collected and analyzed agency documentation, including policies and procedures, and interviewed relevant agency officials. Specifically, for each practice we determined if the agency met, partially met, or did not meet each key practice based on the information collected. We considered a practice to be met if the evidence provided addressed all elements of the practice, partially met if it addressed one or more element, and not met if the evidence did not address any of the elements. After an initial determination, a second analyst reviewed the assessment for concurrence on the ratings and evidence used to support them. In cases where two analysts reached different assessments, they discussed the analysis to resolve any differences. We followed up with the agencies to collect and analyze additional information as appropriate.

As part of this assessment, we determined, among other things, if agencies have an organizational structure, roles, responsibilities, etc. for their privacy programs; how agencies identify and analyze privacy risks; how they have defined their programs in policy; and how information is shared among key agency stakeholders (e.g., department- or agency-level oversight of component privacy activities).

For the second objective, we identified potential challenges agency may face in implementing their privacy programs based on initial discussions with the 24 agencies and OMB Office of Information and Regulatory Affairs (OIRA) staff, as well as prior GAO work and other background research on federal privacy programs. These potential challenges included recruiting, developing, and retaining qualified staff, among others. We then administered a survey to privacy officials at the 24 agencies asking them to identify which of the potential challenges they have experienced and what factors contribute to them, as well as to identify any other challenges they have experienced. We developed this survey in collaboration with our methodologist, and the survey underwent internal peer review as well as three pre-tests with knowledgeable federal privacy professionals who fit the general profile of agency officials that would be responding to our survey. (The survey questions we asked are reproduced in appendix IV.)

We analyzed the results of this survey to identify the number of agencies citing each specific challenge and performed a content analysis to identify common factors contributing to the challenges. After an initial assessment, a second analyst reviewed and provided concurrence on the content analysis. Any discrepancies were resolved through discussion between the two analysts. Finally, we obtained OMB OIRA privacy branch staff perspectives on these challenges, including any government-wide efforts planned or under way that may address the identified challenges.

For the third objective, we identified potential benefits and limitations of PIAs by conducting group discussions and interviews with selected experts from federal agencies, academia, and privacy advocacy organizations. We selected these experts based on their experience with or prior work relating to federal agencies' use of PIAs. After selecting the experts, we held two group discussions via videoconference, each with a mix of experts from federal agencies, academia, and privacy advocacy organizations.²

- For the federal agencies, we solicited the participation of agency privacy officials through coordination with the Federal Privacy Councils, asking for SAOPs or other senior privacy officials from non-CFO Act agencies (i.e., agencies not within the scope of our audit). Four agency officials agreed to participate.
- For academics and researchers, we identified professional researchers who had published on or otherwise demonstrated expertise in federal agencies' use of PIAs. Of the academics/researchers we identified, two agreed to participate in our group discussions, and a third spoke to us via an individual videoconference interview.
- For privacy advocacy organizations, we focused on U.S.-based privacy advocacy organizations that frequently engage with federal privacy policy and practice and limited our outreach to those who had work directly relating to or demonstrating familiarity with U.S. agencies' PIAs. Four experts from privacy advocacy organizations agreed to participate in our group discussions.

²We held a separate interview with one of the experts who did not attend the group discussions.

Eleven experts participated in these discussions, including the following:³

- Hannah Bergman, Chief Privacy Officer, National Archives and Records Administration
- Roger Clarke, Xamax Consultancy Pty Ltd, UNSW Law, ANU Computer Science
- Sophia Cope, Senior Staff Attorney, Electronic Frontier Foundation
- John Davisson, Director of Litigation and Senior Counsel, Electronic Privacy Information Center
- Rachel Finn, Director – Data Protection and Cyber-risk Services / Head of Irish Operations, Trilateral Research
- Hugh Handeyside, Senior Staff Attorney, American Civil Liberties Union National Security Project
- Dana Jackson, Administrative Law Attorney, Export-Import Bank
- Deirdre K. Mulligan, Professor, School of Information; Co-Director, Algorithmic Fairness & Opacity Group; Faculty Director, Berkeley Center for Law and Technology; University of California, Berkeley
- Fon Muttamara, Chief Privacy Officer, U.S. Merit Systems Protection Board
- Mike O'Rourke, Chief Privacy Officer, U.S. International Trade Commission

We analyzed the discussion transcripts to identify common themes discussed by and key statements of the experts. To complete this analysis, we developed a list of themes characterizing expert statements, converted the themes into codes, and then coded the transcript based on the consensus of multiple analysts. Because experts were generating and discussing ideas as part of a free-flowing group discussion, the number of times a concept was or was not repeated does not necessarily indicate the level of consensus on that concept. Throughout the report, we use the term “experts” to refer to more than one expert.

Based on the information collected from these experts, along with prior GAO reports and other background research, we developed and administered a survey to the 24 CFO Act agencies. The survey was to determine which benefits and limitations they have experienced in their use of PIAs, such as for assessing privacy risks and communicating information to the public, as well as questions about the processes used to conduct PIAs. We developed this survey in collaboration with our GAO methodologist, and the survey underwent internal peer review as well as three pre-tests with knowledgeable federal privacy professionals who fit

³We gave experts who participated the option of remaining anonymous and some chose to do so.

the general profile of agency officials that would be responding to our survey. All 24 agencies responded to the survey. (The survey questions we asked and a summary of the responses are reproduced in appendix IV.)

We analyzed the information collected to identify the number of agencies reporting specific benefits and limitations of PIAs, as well as providing specific responses to the questions about the PIA process. We performed a content analysis of the agencies' responses to identify common themes or factors related to the benefits and limitations. After an initial assessment, a second analyst reviewed and provided concurrence on the content analysis. Any discrepancies were resolved through discussion between the two analysts. Finally, we obtained OMB OIRA privacy branch staff's perspectives on the agency- and expert-reported benefits and limitations of PIAs, including any government-wide efforts planned or under way that may address limitations identified in agencies' use of PIAs.

For our fourth objective, we reviewed OMB guidance on the role of the SAOP, and reviewed agency policies and procedures to determine which official had been designated SAOP. We also determined if the SAOP had delegated privacy-related responsibilities to other agency officials. Further, we interviewed privacy officials at agencies with a chief privacy officer or other senior privacy official established by law. We also discussed the SAOP role with privacy branch staff from OIRA.

We conducted this performance audit from March 2021 to September 2022 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: Recommendations to Departments and Agencies

We are making a total of 62 recommendations to 23 of the 24 Chief Financial Officers Act agencies.

We are making the following six recommendations to the Department of Agriculture:

- The Secretary of Agriculture should document program management controls and common privacy controls in place or planned for meeting applicable requirements and managing risks. (Recommendation 3)
- The Secretary of Agriculture should fully define and document a process for ensuring that the senior agency official for privacy, or other designated privacy official, reviews IT capital investment plans and budgetary requests. (Recommendation 4)
- The Secretary of Agriculture should fully define and document a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. (Recommendation 5)
- The Secretary of Agriculture should establish a time frame for incorporating privacy into an organization-wide risk management strategy that includes a determination of risk tolerance, and develop and document this strategy. (Recommendation 6)
- The Secretary of Agriculture should fully define and document the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages, and document these roles. (Recommendation 7)
- The Secretary of Agriculture should establish a time frame for fully developing a privacy continuous monitoring strategy, and develop and document this strategy. (Recommendation 8)

We are making one recommendation to the Department of Commerce:

- The Secretary of Commerce should ensure that its organization-wide risk management strategy includes key elements, including a determination of privacy risk tolerance. (Recommendation 9)

We are making the following three recommendations to the Department of Defense:

- The Secretary of Defense should establish a time frame for fully defining a process to ensure that the senior agency official for privacy

or other designated senior privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy, and document this process. (Recommendation 10)

- The Secretary of Defense should establish a time frame for incorporating privacy into an organization-wide risk management strategy that includes a determination of risk tolerance, and develop and document this strategy. (Recommendation 11)
- The Secretary of Defense should establish a time frame for fully developing a privacy continuous monitoring strategy, and develop and document this strategy. (Recommendation 12)

We are making one recommendation to the Department of Education:

- The Secretary of Education should establish a time frame for updating the department's policies for creating, reviewing, and publishing system of records notices, and make these updates. (Recommendation 13)

We are making the following three recommendations to the Department of Energy:

- The Secretary of Energy should establish a time frame for fully defining a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy, and document this process. (Recommendation 14)
- The Secretary of Energy should incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance. (Recommendation 15)
- The Secretary of Energy should establish a time frame for fully defining the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages, and document these roles. (Recommendation 16)

We are making one recommendation to the Department of Health and Human Services:

- The Secretary of Health and Human Services should fully define and document a process for ensuring that the senior agency official for

privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. (Recommendation 17)

We are making the following three recommendations to the Department of Homeland Security:

- The Secretary of Homeland Security should incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance. (Recommendation 18)
- The Secretary of Homeland Security should fully define and document the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages. (Recommendation 19)
- The Secretary of Homeland Security should fully develop and document a privacy continuous monitoring strategy. (Recommendation 20)

We are making the following three recommendations to the Department of Housing and Urban Development:

- The Secretary of Housing and Urban Development should fully define and document a process for ensuring that the senior agency official for privacy, or other designated privacy official, reviews IT capital investment plans and budgetary requests. (Recommendation 21)
- The Secretary of Housing and Urban Development should incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance. (Recommendation 22)
- The Secretary of Housing and Urban Development should establish a time frame for fully developing a privacy continuous monitoring strategy, and develop and document this strategy. (Recommendation 23)

We are making one recommendation to the Department of the Interior:

- The Secretary of the Interior should establish a time frame for incorporating privacy into an organization-wide risk management strategy that includes a determination of risk tolerance, and develop and document this strategy. (Recommendation 24)

We are making the following two recommendations to the Department of Justice:

- The Attorney General should incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance. (Recommendation 25)
- The Attorney General should establish a time frame and fully develop and document a privacy continuous monitoring strategy. (Recommendation 26)

We are making the following three recommendations to the Department of Labor:

- The Secretary of Labor should fully define and document a process for ensuring that the senior agency official for privacy, or other designated privacy official, reviews IT capital investment plans and budgetary requests. (Recommendation 27)
- The Secretary of Labor should fully define and document a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. (Recommendation 28)
- The Secretary of Labor should fully define and document the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages. (Recommendation 29)

We are making the following three recommendations to the Department of State:

- The Secretary of State should establish a time frame for incorporating privacy into an organization-wide risk management strategy that includes a determination of risk tolerance, and develop and document this strategy. (Recommendation 30)
- The Secretary of State should establish a time frames for fully defining and the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages, and document these roles. (Recommendation 31)
- The Secretary of State should establish a time frame for fully developing a privacy continuous monitoring strategy, and develop and document this strategy. (Recommendation 32)

We are making the following two recommendations to the Department of Transportation:

- The Secretary of Transportation should fully define and document a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. (Recommendation 33)
- The Secretary of Transportation should incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance. (Recommendation 34)

We are making the following five recommendations to the Department of the Treasury:

- The Secretary of the Treasury should fully define and document a process for ensuring that the senior agency official for privacy, or other designated privacy official, reviews IT capital investment plans and budgetary requests. (Recommendation 35)
- The Secretary of the Treasury should fully define and document a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. (Recommendation 36)
- The Secretary of the Treasury should incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance. (Recommendation 37)
- The Secretary of the Treasury should establish a time frame for fully defining the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages, and document these roles. (Recommendation 38)
- The Secretary of the Treasury should fully develop and document a privacy continuous monitoring strategy. (Recommendation 39)

We are making the following four recommendations to the Department of Veterans Affairs:

- The Secretary of Veterans Affairs should establish a time frame for defining a process for ensuring that the senior agency official for

privacy, or other designated privacy official, reviews IT capital investment plans and budgetary requests, and document this process. (Recommendation 40)

- The Secretary of Veterans Affairs should fully define and document a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. (Recommendation 41)
- The Secretary of Veterans Affairs should fully define and document the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages, and document these roles. (Recommendation 42)
- The Secretary of Veterans Affairs should ensure that its privacy continuous monitoring strategy includes a catalog of privacy controls and defines the frequency at which they are to be assessed. (Recommendation 43)

We are making one recommendation to the Environmental Protection Agency (EPA):

- The Administrator of EPA should fully develop and document a privacy continuous monitoring strategy. (Recommendation 44)

We are making the following three recommendations to the General Services Administration (GSA):

- The Administrator of GSA should fully define and document a process for ensuring that the senior agency official for privacy, or other designated privacy official, reviews IT capital investment plans and budgetary requests. (Recommendation 45)
- The Administrator of GSA should establish a time frame for fully defining a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy, and document that process. (Recommendation 46)
- The Administrator of GSA should fully define and document the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages. (Recommendation 47)

We are making the following two recommendations to the National Aeronautics and Space Administration (NASA):

- The Administrator of NASA should incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance. (Recommendation 48)
- The Administrator of NASA should fully define and document the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages. (Recommendation 49)

We are making the following two recommendations to the Nuclear Regulatory Commission (NRC):

- The Chairman of NRC should fully define and document a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. (Recommendation 50)
- The Chairman of NRC should fully define and document the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages. (Recommendation 51)

We are making the following six recommendations to the Office of Personnel Management (OPM):

- The Director of OPM should establish a time frame for updating the agency's policy for creating, reviewing, and publishing system of records notices, and make these updates. (Recommendation 52)
- The Director of OPM should define and document procedures for coordination between privacy and information security functions. (Recommendation 53)
- The Director of OPM should fully define and document a policy and process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. (Recommendation 54)

- The Director of OPM should incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance. (Recommendation 55)
- The Director of OPM should establish a time frame for fully defining the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages, and document these roles. (Recommendation 56)
- The Director of OPM should fully develop and document a privacy continuous monitoring strategy. (Recommendation 57)

We are making one recommendation to the Small Business Administration (SBA):

- The Administrator of SBA should fully define and document a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. (Recommendation 58)

We are making the following four recommendations to the Social Security Administration (SSA):

- The Commissioner of SSA should define and document procedures for coordination between privacy and information security functions. (Recommendation 59)
- The Commissioner of SSA should fully define and document a process for ensuring that the senior agency official for privacy, or other designated privacy official, reviews IT capital investment plans and budgetary requests to ensure privacy requirements and associated controls are explicitly identified and included with respect to any IT resources that will involve PII. (Recommendation 60)
- The Commissioner of SSA should fully define and document a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. (Recommendation 61)
- The Commissioner of SSA should establish a time frame for fully defining the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and

reviewing authorization packages, and document these roles.
(Recommendation 62)

We are making two recommendations to the U.S. Agency for International Development (USAID):

- The Administrator of USAID should fully define and document a process for ensuring that the senior agency official for privacy, or other designated privacy official, reviews IT capital investment plans and budgetary requests. (Recommendation 63)
- The Administrator of USAID should incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance. (Recommendation 64)

Appendix III: Details on the Extent to Which the 24 Chief Financial Officers Act Agencies Addressed Key Privacy Practices in Policies and Procedures

The following tables provide details on the extent to which the 24 agencies' policies and procedures addressed key practices related to privacy compliance activities, coordination between privacy and other programs or functions, and risk management activities.

Table 3: Extent to Which the 24 Chief Financial Officers Act Agencies Addressed Key Privacy Compliance Activities

Agency	System of records notice	Privacy impact assessment	Privacy program plan
Agriculture	●	●	◐
Commerce	●	●	●
Defense	●	●	●
Education	◐	●	●
Energy	●	●	●
Health and Human Services	●	●	●
Homeland Security	●	●	●
Housing and Urban Development	●	●	●
Interior	●	●	●
Justice	●	●	●
Labor	●	●	●
State	●	●	●
Transportation	●	●	●
Treasury	●	●	●
Veterans Affairs	●	●	●
Environmental Protection Agency	●	●	●
General Services Administration	●	●	●
National Aeronautics and Space Administration	●	●	●
National Science Foundation	●	●	●
Nuclear Regulatory Commission	●	●	●
Office of Personnel Management	◐	●	●

**Appendix III: Details on the Extent to Which the
24 Chief Financial Officers Act Agencies
Addressed Key Privacy Practices in Policies
and Procedures**

Agency	System of records notice	Privacy impact assessment	Privacy program plan
Small Business Administration	●	●	●
Social Security Administration	●	●	●
U.S. Agency for International Development	●	●	●

Legend: ● = Addressed ◐ = Partially addressed ○ = Not addressed

Source: GAO analysis of agency information. | GAO-22-105065

Table 4: Extent to Which the 24 Chief Financial Officers Act Agencies Addressed Key Privacy Coordination Activities

Agency	Coordination with information security	IT budget review	Workforce management	Incident response
Agriculture	●	◐	◐	●
Commerce	●	●	●	●
Defense	●	●	◐	●
Education	●	●	●	●
Energy	●	●	◐	●
Health and Human Services	●	●	◐	●
Homeland Security	●	●	●	●
Housing and Urban Development	●	○	●	●
Interior	●	●	●	●
Justice	●	●	●	●
Labor	●	○	○	●
State	●	●	●	●
Transportation	●	●	◐	●
Treasury	●	◐	◐	●
Veterans Affairs	●	◐	◐	●
Environmental Protection Agency	●	●	●	●
General Services Administration	●	◐	◐	●

**Appendix III: Details on the Extent to Which the
24 Chief Financial Officers Act Agencies
Addressed Key Privacy Practices in Policies
and Procedures**

Agency	Coordination with information security	IT budget review	Workforce management	Incident response
National Aeronautics and Space Administration	●	●	●	●
National Science Foundation	●	●	●	●
Nuclear Regulatory Commission	●	●	◐	●
Office of Personnel Management	◐	●	◐	●
Small Business Administration	●	●	◐	●
Social Security Administration	◐	◐	◐	●
U.S. Agency for International Development	●	◐	●	●

Legend: ● = Addressed ◐ = Partially addressed ○ = Not addressed

Source: GAO analysis of agency information. | GAO-22-105065

Table 5: Extent to Which the 24 Chief Financial Officers Act Agencies Addressed Key Privacy Risk Management Activities

Agency	Risk management strategy	Risk management steps	Continuous monitoring
Agriculture	○	◐	○
Commerce	○	●	●
Defense	○	●	◐
Education	●	●	●
Energy	○	○	●
Health and Human Services	●	●	●
Homeland Security	○	◐	◐
Housing and Urban Development	○	●	○
Interior	○	●	●
Justice	○	●	◐
Labor	●	○	●
State	○	◐	○

**Appendix III: Details on the Extent to Which the
24 Chief Financial Officers Act Agencies
Addressed Key Privacy Practices in Policies
and Procedures**

Agency	Risk management strategy	Risk management steps	Continuous monitoring
Transportation	○	●	●
Treasury	○	◐	◐
Veterans Affairs	●	◐	◐
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	●	◐	●
U.S. Agency for International Development	○	●	●

Legend: ● = Addressed ◐ = Partially addressed ○ = Not addressed

Source: GAO analysis of agency information. | GAO-22-105065

Appendix IV: Survey Administered to the 24 Chief Financial Officers Act Agencies

We administered a survey to the 24 Chief Financial Officers Act agencies to solicit privacy officials' views on challenges they faced in implementing their privacy program. The following identifies the survey questions that we administered and the aggregated results from the responses under each question. All 24 agencies responded to the survey. Answers to open-ended questions are not displayed below for brevity and to limit the possibility of identification of individual agencies.

Survey on Federal Agency Privacy Programs

The purpose of this set of questions is to gather information from the 24 Chief Financial Officers Act agencies about aspects of their privacy programs. The sections of this questionnaire cover (1) issues agencies may have experienced in establishing privacy policies and procedures, (2) challenges agencies may have in implementing the privacy programs, and (3) benefits and limitations of privacy impact assessments (PIA).

We believe that the official(s) responsible for day-to-day oversight of privacy program activities, in consultation with other staff as needed, are best positioned to answer the questions for your agency. We estimate that completing this survey should take approximately one hour. If you feel that providing supporting documentation would help answer any of the questions, please feel free to include that as an attachment.

Section I: Establishing Policies and Procedures

During our ongoing analysis of agencies' privacy policies and procedures, we have identified areas where agencies may not have documented policies or processes that address key OMB requirements in circular A-130. We wanted to get a better picture of how agencies are addressing each of these requirements and if there is an issue with documenting those procedures.

Please describe your agency's process for:

1. Ensuring senior agency official for privacy (SAOP) review of IT budget documents to ensure that privacy requirements (and associated privacy controls), as well as any associated costs, are explicitly identified and included. **(Note – open ended text responses deliberately omitted)**
2. Ensuring that the SAOP is involved in addressing the hiring, training, and professional development needs of the agency with respect to privacy. **(Note – open ended text responses deliberately omitted)**
3. Fully defining the role of privacy officials in categorizing systems with PII, selecting and assessing privacy controls, and reviewing authorization packages. **(Note – open ended text responses deliberately omitted)**

Section II: Challenges

4. Based on our prior work and conversations with agency officials, we have identified the following list of challenges agencies may face in implementing their privacy programs. For each challenge, please indicate whether or not it is a challenge for your agency. If you answered "yes," please explain what factors make it a challenge.
 - a) Coordinating with other internal agency offices and programs (e.g., information security, human capital, budget) to address privacy requirements

Yes, has been a challenge
 No, has not been a challenge

Number of Responses

Yes	15
No	9

If yes, please explain.

(Note – open ended text responses deliberately omitted)

- b) Ensuring that program offices and/or agency components are aware of and implementing privacy requirements

- Yes, has been a challenge
 No, has not been a challenge

Number of Responses

Yes	15
No	9

If yes, please explain.

(Note – open ended text responses deliberately omitted)

- c) Hiring personnel to fill key privacy positions

- Yes, has been a challenge
 No, has not been a challenge

Number of Responses

Yes	17
No	7

If yes, please explain.

(Note – open ended text responses deliberately omitted)

- d) Retaining privacy personnel with needed skills and expertise

- Yes, has been a challenge
 No, has not been a challenge

Number of Responses

Yes	15
No	9

If yes, please explain.

(Note – open ended text responses deliberately omitted)

e) Training of privacy staff or contractors

- Yes, has been a challenge
- No, has not been a challenge

Number of Responses

Yes	14
No	10

If yes, please explain.

(Note – open ended text responses deliberately omitted)

f) Using federal guidance, such as from NIST and/or OMB, for privacy programs

- Yes, has been a challenge
- No, has not been a challenge

Number of Responses

Yes	9
No	15

If yes, please explain.

(Note – open ended text responses deliberately omitted)

g) Integrating privacy and security controls as it relates to the transition to NIST 800-53 Revision 5

- Yes, has been a challenge
- No, has not been a challenge

Number of Responses

Yes	16
No	8

If yes, please explain.

(Note – open ended text responses deliberately omitted)

- h) Applying privacy requirements to new and emerging technologies (e.g., artificial intelligence, cloud services)

- Yes, has been a challenge
 No, has not been a challenge

Number of Responses

Yes	20
No	4

If yes, please explain.

(Note – open ended text responses deliberately omitted)

- i) Having sufficient resources to complete privacy-related work

- Yes, has been a challenge
 No, has not been a challenge

Number of Responses

Yes	21
No	3

If yes, please explain.

(Note – open ended text responses deliberately omitted)

5. Please describe any additional challenges in implementing your privacy program that were not listed above.

(Note – open ended text responses deliberately omitted)

6. Given the challenges, if any, that your agency faces, what suggestions do you have for government-wide initiatives that OMB could undertake to address the identified challenges?

(Note – open ended text responses deliberately omitted)

Section III: Privacy Impact Assessments

Based on our research and discussion with experts from government and non-governmental organizations, we have identified the following

**Appendix IV: Survey Administered to the 24
Chief Financial Officers Act Agencies**

potential uses of privacy impact assessments (PIA). For each statement below, please indicate whether each potential use of PIAs **at your agency** generally has substantial benefits, benefits that somewhat outweigh the limitations, equal benefits and limitations, limitations that somewhat outweigh the benefits, or substantial limitations. In addition, please explain your reasons for each answer, describing any specific benefits and/or limitations.

The Use of PIAs for (...a-h..) have...	Substantial benefits	Benefits that somewhat outweigh the limitations	Equal benefits and limitations	Limitations that somewhat outweigh the benefits	Substantial limitations
a) Providing information to the public about agency programs or systems and how they collect, use, and protect PII	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Number of responses	
Substantial benefits	14
Benefits that somewhat outweigh limitations	4
Equal benefits and limitations	5
Limitations that somewhat outweigh benefits	1
Substantial limitations	0

**Please describe the reason for your answer:
(Note – open ended text responses deliberately omitted)**

b) Managing programs' and systems' privacy risks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

Number of responses	
Substantial benefits	18
Benefits that somewhat outweigh limitations	4
Equal benefits and limitations	1
Limitations that somewhat outweigh benefits	0
Substantial limitations	1

**Appendix IV: Survey Administered to the 24
Chief Financial Officers Act Agencies**

Please describe the reason for your answer:

(Note – open ended text responses deliberately omitted)

**c) Educating agency staff about the
importance of privacy**

Number of responses

Substantial benefits	12
Benefits that somewhat outweigh limitations	2
Equal benefits and limitations	7
Limitations that somewhat outweigh benefits	1
Substantial limitations	2

Please describe the reason for your answer:

(Note – open ended text responses deliberately omitted)

**d) Ensuring that privacy considerations
are taken into account in the design of
programs and systems**

**Appendix IV: Survey Administered to the 24
Chief Financial Officers Act Agencies**

Number of responses

Substantial benefits	13
Benefits that somewhat outweigh limitations	7
Equal benefits and limitations	1
Limitations that somewhat outweigh benefits	1
Substantial limitations	2

Please describe the reason for your answer:

(Note – open ended text responses deliberately omitted)

**e) Addressing privacy issues raised by
new and emerging technologies**

f)

Number of responses

Substantial benefits	13
Benefits that somewhat outweigh limitations	5
Equal benefits and limitations	3
Limitations that somewhat outweigh benefits	1
Substantial limitations	2

Please describe the reason for your answer:

(Note – open ended text responses deliberately omitted)

**g) Complementing information security
activities**

Number of responses

Substantial benefits	13
Benefits that somewhat outweigh limitations	6
Equal benefits and limitations	3
Limitations that somewhat outweigh benefits	0
Substantial limitations	1
N.A.	1

**Appendix IV: Survey Administered to the 24
Chief Financial Officers Act Agencies**

Please describe the reason for your answer:

(Note – open ended text responses deliberately omitted)

h) Covering privacy risks to individuals that may emerge even if no data is collected (e.g. physical privacy)

Number of responses

Substantial benefits	7
Benefits that somewhat outweigh limitations	2
Equal benefits and limitations	2
Limitations that somewhat outweigh benefits	3
Substantial limitations	4
N.A.	4

Please describe the reason for your answer:

(Note – open ended text responses deliberately omitted)

h) Impacting programs' cost, schedule, and/or performance

Number of responses

Substantial benefits	9
Benefits that somewhat outweigh limitations	4
Equal benefits and limitations	6
Limitations that somewhat outweigh benefits	2
Substantial limitations	2
N.A.	1

Please describe the reason for your answer:

(Note – open ended text responses deliberately omitted)

7. Please describe any other benefits you have experienced in your agency's use of PIAs.
(Note – open ended text responses deliberately omitted)

8. Please describe any other limitations you have experienced in your agency's use of PIAs

(Note – open ended text responses deliberately omitted)

9. The following questions pertain to the process of developing and maintaining PIAs and guidance or other tools that might assist your agency's efforts. For each question, please answer "always," "sometimes," "never," or "don't know" and elaborate on your response.

	Always	Sometimes	Never	Don't know
a) Are PIAs at your agency initiated early enough in the development of a program or system to affect decisions about such things as the information to be collected and how a program or system is designed?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Number of responses

Always	6
Sometimes	18
Never	0
Don't know	0

Please describe the reason for your answer:

(Note – open ended text responses deliberately omitted)

b) Are you made aware of all systems or tools at your agency that may require a PIA, including general support systems, systems owned and operated by a third party, web applications, or other tools?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--	--------------------------	--------------------------	--------------------------	--------------------------

Appendix IV: Survey Administered to the 24 Chief Financial Officers Act Agencies

Number of responses

Always	11
Sometimes	12
Never	1
Don't know	0

Please describe the reason for your answer:

(Note – open ended text responses deliberately omitted)

-
- c) Are PIAs at your agency updated frequently enough to reflect changes to a system and the current state of privacy risks?
-

Number of responses

Always	14
Sometimes	10
Never	0
Don't know	0

Please describe the reason for your answer:

(Note – open ended text responses deliberately omitted)

-
- d) Are PIA requirements and guidance appropriate for systems of different types (e.g., standard communication tools, major database systems), sensitivity (e.g., basic contact information, sensitive medical data), or risk levels (e.g., different risks to different communities)?
-

Number of responses

Always	12
Sometimes	10
Never	1
Don't know	1

Please describe the reason for your answer:

(Note – open ended text responses deliberately omitted)

**Appendix IV: Survey Administered to the 24
Chief Financial Officers Act Agencies**

e) **Is the privacy program able to hold agency staff accountable for conducting PIAs in a timely manner?**

Always	11
Sometimes	12
Never	1
Don't know	0

Please describe the reason for your answer:

(Note – open ended text responses deliberately omitted)

f) **Is the agency as a whole held accountable by external oversight bodies for conducting PIAs in a timely manner?**

Number of responses

Always	13
Sometimes	6
Never	4
Don't know	1

Please describe the reason for your answer:

(Note – open ended text responses deliberately omitted)

10. What additional government-wide guidance or tools, if any, would assist your agency in conducting PIAs? **(Note – open ended text responses deliberately omitted)**

Appendix V: Comments from the Department of Commerce



UNITED STATES DEPARTMENT OF COMMERCE
Office of the Acting Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

August 11, 2022

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC20548

Marisol Cruz Cain
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC20548

Dear Ms. Franks and Ms. Cruz Cain:

Thank you for the opportunity to respond to the GAO draft report entitled *Privacy: Dedicated Leadership Can Improve Programs and Address Challenges (GAO-22-105065)*.

The Department agrees with GAO's recommendation that Commerce should ensure that its organization-wide risk management strategy includes key elements, including a determination of privacy risk tolerance. We will prepare a formal action plan upon issuance of GAO's final report.

If you have any questions, please contact MaryAnn Mausser, Department GAO Audit Liaison, at (202) 482-8120 or mmausser@doc.gov.

Sincerely,

JEREMY
PELTER

Digitally signed by
JEREMY PELTER
Date: 2022.08.11
17:04:26 -0400

Jeremy Pelter

Acting Chief Financial Officer and
Assistant Secretary for Administration

Appendix VI: Comments from the Department of Defense



ASSISTANT TO THE SECRETARY OF DEFENSE FOR
PRIVACY, CIVIL LIBERTIES, AND TRANSPARENCY
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

Ms. Jennifer R. Franks
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Franks,

This is the Department of Defense (DoD) response to the GAO Draft Report GAO-105065, "PRIVACY: Dedicated Leadership Can Improve Programs and Address Challenges," dated June 30, 2022."

Attached is DoD's response to the subject report. My point of contact is Cynthia Stanley, who can be reached at cynthia.b.stanley2.civ@mail.mil and via telephone at (703) 268-6782.

Sincerely,

CHUNG, JOO.Y. Digitally signed by
CHUNG, JOO.Y. 1512306507
Date: 2022.07.22 15:12:21
+04'00'
.1512306507

Joo Y. Chung

**GAO DRAFT REPORT DATED JUNE 30, 2022
GAO-105065 (GAO CODE 105065)**

“PRIVACY: Dedicated Leadership Can Improve Programs and Address Challenges”

**DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION**

FIRST GAO RECOMMENDATION FOR DoD: The Secretary of Defense should establish a time frame for fully defining a process to ensure that the Senior Agency Official for Privacy (SAOP) or other designated senior privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy, and document this process. (Recommendation 10)

DoD RESPONSE: Concur. DoD will establish a time frame for fully defining a process to ensure the Agency’s SAOP (and other senior privacy officials as appropriate) are involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy, and document this process. A time frame with appropriate milestones for completion will be created.

SECOND GAO RECOMMENDATION FOR DoD: The Secretary of Defense should establish a time frame for incorporating privacy into an organization-wide risk management strategy that includes a determination of risk tolerance, and develop and document this strategy. (Recommendation 11)

DoD RESPONSE: Concur. DoD will establish a time frame to incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance, and develop and document this strategy. A time frame with appropriate milestones for completion will be created.

THIRD GAO RECOMMENDATION FOR DoD: The Secretary of Defense should establish a time frame for fully developing a privacy continuous monitoring strategy, and develop and document this strategy. (Recommendation 12)

DoD RESPONSE: Concur. DoD will establish a time frame for fully developing a privacy continuous monitoring strategy, and develop and document this strategy. A time frame with appropriate milestones for completion will be created.

Appendix VII: Comments from the Department of Education



UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF PLANNING, EVALUATION AND POLICY DEVELOPMENT

July 29, 2022

Ms. Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity

Ms. Marisol Cruz Cain
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Franks and Ms. Cain:

On behalf of the U.S. Department of Education (Department), I write in response to the draft Government Accountability Office (GAO) report, *Privacy: Dedicated Leadership Can Improve Programs and Address Challenges (GAO-22-105065)*. As the Assistant Secretary of the Office of Planning, Evaluation and Policy Development (OPEPD), I am specifically responding to the one recommendation made to the Department.

The Department appreciates the opportunity to respond to this GAO draft report, which examined the privacy programs of the 24 Chief Financial Officer (CFO) Act agencies, specifically (1) the extent to which agencies have established programs for ensuring privacy protections; (2) challenges agencies reported experiencing in implementing their privacy programs; (3) reported benefits and limitations in agencies' use of privacy impact assessments; and (4) the extent to which agencies have senior leadership dedicated to privacy issues. In this multi-agency study, GAO makes 65 recommendations for selected agencies, including one specific to the Department.

The Department agrees with GAO that the protection of personal privacy has become a more significant issue in recent years with the advent of new technologies and the proliferation of personal information, and that Federal agencies must ensure that any personally identifiable information (PII) they collect, store, or process is protected from unauthorized access, tampering, or loss. This issue was a contributing factor when the Department centralized privacy functions and created the Student Privacy Policy Office (SPPO) within OPEPD. The SPPO director serves as the Department's Chief Privacy Officer and Senior Agency Official for Privacy, leading the Department's efforts to protect privacy including the enforcement of student privacy laws, the development and evaluation of privacy policy, and the management of privacy risks. Our response to the one recommendation to the Department in the GAO draft report is below.

400 MARYLAND AVE., S.W. WASHINGTON, D.C. 20202-2110

The Department of Education's mission is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access.

**Appendix VII: Comments from the Department
of Education**

Page 2 – Ms. Franks/Ms. Crain

Recommendation 13: The Secretary of Education should establish a time frame for updating the department's policies for creating, reviewing, and publishing system of records notices, and make these updates.

Response 13:

The Department concurs with this recommendation. The Department has already begun updating existing privacy policies, including those related to compliance with the Privacy Act, as well as those establishing and administering the privacy program. The Department is also working to develop a timeline for the development and completion of these policies. Final governance documentation will be consistent with Office of Management and Budget (OMB) Circular A-108, and accurately reflect the Department's current processes, as well as the current structure of the privacy program.

Again, thank you for the chance to respond to the recommendations outlined in this draft GAO report. If you need further information, please contact Kevin Herms, Director of SPPO, at 202-453-7038 or kevin.herms@ed.gov.

Sincerely,



Roberto Rodriguez
Assistant Secretary
Office of Planning, Evaluation and Policy
Development

Appendix VIII: Comments from the Department of Energy



Department of Energy

Washington, DC 20585

August 10, 2022

Marisol Cruz Cain
Director of Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Cain:

The Department of Energy (DOE or Department) appreciates the opportunity to provide a response to the Government Accountability Office's (GAO) Draft report titled, *Privacy: Dedicated Leadership Can Improve Programs and Address Challenges* (GAO-22-105065). DOE concurs with each of the 3 recommendations listed in the report. DOE plans to implement the following activities as described in the enclosure.

GAO should direct any questions to Ken Hunt, Deputy Chief Information Officer for Enterprise Records Management, Privacy & Compliance Office of the Chief Information Officer, at 202-586-8695 or via e-mail Ken.Hunt@hq.doe.gov.

Sincerely,

A handwritten signature in black ink, appearing to read "Ann Dunkin".

Ann Dunkin
Chief Information Officer

Enclosure

MANAGEMENT RESPONSE
GAO Draft Report, 22-105065

Privacy: Dedicated Leadership Can Improve Programs and Address Challenges

Recommendation 15: The Secretary of Energy should establish a time frame for fully defining a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy, and document this process.

Management Response: Concur

- Action Plan for the recommendation: DOE Order 206.1 addresses the responsibility of Heads of Departmental Elements to maintain a privacy program and to appoint qualified officials to run the program within the Departmental Element. The Order also addresses the privacy program officials' responsibilities. These duties will be updated when the work to update and reissue the Order is completed. In addition, the Senior Agency Official for Privacy and the Chief Privacy Officer will consult with the Human Capital Office to provide best practices outlining the skill sets and professional development recommendations for privacy professionals at DOE and its management and operating contractors.
- DOE will also continue to support the Federal Privacy Council's continued virtual training opportunities, to ensure broad participation of privacy professionals across the DOE Enterprise.

Estimated Completion Date: By June 30, 2023

Recommendation 16: The Secretary of Energy should incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance.

Management Response: Concur

- Action Plan for the recommendation: The Senior Agency Official for Privacy and the Chief Privacy Officer will work with the DOE Cybersecurity community to integrate privacy into the Department's Risk Profile process. This issue will also be addressed through updates to Departmental directives and orders for both privacy and cybersecurity, both of which are currently being revised.

Estimated Completion Date: By October 31, 2023

Recommendation 17: The Secretary of Energy should establish a time frame for fully defining the role of the Senior Agency Official for Privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, reviewing authorization packages, and documenting these roles.

**Appendix VIII: Comments from the Department
of Energy**

Management Response: Concur

- Action Plan for the recommendation: The Office of the Chief Information Officer is in the process of updating DOE Order 206.1, DOE Privacy Program. The updated order will include documenting and defining the role of the SAOP in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages. The program will also review whether additional delegations are needed to empower the SAOP to perform the relevant functions.

Estimated Completion Date: By June 30, 2023

Appendix IX: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

August 1, 2022

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Franks:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, **"PRIVACY: Dedicated Leadership Can Improve Programs and Address Challenges"** (GAO-22-105065).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Melanie Anne Egorin

Melanie Anne Egorin, PhD
Assistant Secretary for Legislation

Attachment

**GENERAL COMMENTS FROM THE DEPARTMENT OF
HEALTH & HUMAN SERVICES ON THE GOVERNMENT
ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED —
PRIVACY Dedicated Leadership Can Improve Programs and
Address Challenges (GAO-22-105065)**

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

General Comments

Recommendation 19

The Secretary of Health and Human Services should fully define and document a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy.

HHS Response

HHS Concurs with GAO's recommendation.

In the next iteration of the HHS Policy for Information Security and Privacy Protection (IS2P), HHS will define and document the responsibility and process of the Senior Agency Official for Privacy (SAOP) in the hiring, training, and professional development needs of the agency with respect to Privacy.

Appendix X: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

August 5, 2022

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Marisol Cruz Cain
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-22-105065, "PRIVACY: Dedicated Leadership Can Improve Programs and Address Challenges"

Dear Mses. Franks and Cruz Cain:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO's recognition of the Department's efforts to protect privacy through its policies and procedures for key privacy activities, the establishment of privacy impact assessment policies, and ensuring coordination with other key functions, including information security, Information Technology (IT) budget and acquisition, workforce planning, and incident response. DHS remains committed to accomplishing its mission while embedding and enforcing privacy protections and transparency in all Departmental activities.

The draft report contained 67 recommendations, including three for DHS with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments under a separate cover for GAO's consideration.

**Appendix X: Comments from the Department
of Homeland Security**

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future

Sincerely,

**JIM H
CRUMPACKER**

Digitally signed by JIM H
CRUMPACKER
Date: 2022.08.05 07:30:08 -04'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Enclosure

**Enclosure: Management Response to Recommendations
Contained in GAO-22-105065**

GAO recommended that the Secretary of Homeland Security:

Recommendation 20: Incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance.

Response: Concur. Pursuant to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5, “Security and Privacy Controls for Information Systems and Organizations,” dated September 2020¹, the DHS Privacy Office (PRIV) previously incorporated privacy into an organization-wide risk management strategy through specific privacy controls. Specifically, NIST SP 800-53 provides a catalog of security and privacy controls for all U.S. federal information systems, and on January 23, 2014, PRIV implemented Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) templates for DHS-wide use based on these controls. For example, the System Privacy Plans developed for each DHS system are based on the catalog of privacy controls in NIST SP 800-53 and document privacy controls in place for each system, as appropriate.

PRIV also implemented other privacy best practices in accordance with the Department’s Fair Information Practice Principles (FIPPs)², which are the framework for privacy policy at DHS, and provide the foundational principles for privacy policy and guideposts for their implementation throughout the Department. The FIPPs are the basis of the privacy compliance policies and procedures governing the use of personally identifiable information (PII). Accordingly, all DHS programs are analyzed based on the FIPPs, as established in DHS Memorandum 2008-01, “Privacy Policy Guidance Memorandum,” dated December 29, 2008.³ For example, DHS provides transparency and notice to an individual regarding the collection, use, dissemination, and maintenance of PII through Privacy Act Statements and PIAs published on our website. Another DHS best practice, according to the FIPPs, is within data minimization, as DHS only collects PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retains PII for as long as necessary to fulfill the specified purpose(s). For example, pursuant to DHS Instruction 262-16-001, “DHS Privacy Compliance Instruction on the Collection Use Retention and Dissemination Personally Identifiable Information,” dated May 4, 2022, DHS has minimized the use of social security numbers and instructed programs to

¹ <https://doi.org/10.6028/NIST.SP.800-53r5>

² <https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles>

³ https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

**Appendix X: Comments from the Department
of Homeland Security**

only collect and retain the minimum amount of information necessary to accomplish their mission.⁴

However, PRIV recognizes that the determination of risk tolerance is not specifically addressed on the PTA and PIA templates and PRIV's Compliance Team will review the templates to determine how best to address this information, as appropriate. Estimated Completion Date (ECD): January 31, 2023.

Recommendation 21: Fully define and document the role of the senior agency official for privacy, or other designated privacy official, in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages.

Response: Concur. As the senior agency privacy official in DHS, the Chief Privacy Officer (CPO) is the Department's senior-level official with primarily privacy-related duties who ensures consistent focus on privacy concerns. The CPO is currently responsible and accountable for ensuring compliance with applicable privacy requirements, and managing privacy risks by reviewing and approving the categorization of information systems. The CPO also assesses privacy risks for all DHS IT systems, technologies, rulemakings, programs, pilot projects, information collections and forms that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

In addition, the CPO is responsible for providing guidance and mitigation strategies by reviewing and approving all DHS Component privacy compliance documentation, such as PIAs, System of Records Notices, and periodic policy reviews. PRIV also further defines the roles and responsibilities of the CPO by providing support to Component privacy programs through program oversight, specialized training, and centralized focus for professional development as it pertains to privacy.

PRIV will continue to fully define the CPO's role as the designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments and reviewing authorization packages for information systems that involve PII prior to system authorization, as described in DHS Instruction 047-01-001, "Privacy Policy and Compliance," dated July 25, 2011.⁵ Through engagements with DHS Components, and based upon changes to law, the CPO will review and update policies and instructions that advance and reinforce privacy policies, procedures, and programs across the enterprise, as appropriate. For example, most recently the CPO issued an updated DHS Instruction

⁴ <https://www.dhs.gov/publication/collection-use-retention-and-dissemination-personally-identifiable-information>

⁵ <https://www.dhs.gov/publication/privacy-policy-and-compliance-instruction-047-01-001>

262-16-001 based upon Executive Order 13993, “Executive Order on the Revision of Civil Immigration Enforcement Policies and Priorities,” dated January 20, 2021.⁶

Recommendation 22: Fully develop and document a privacy continuous monitoring strategy.

Response: Concur. PRIV will continue efforts already underway to address key elements of a privacy continuous monitoring strategy, pursuant to DHS Instruction 047-01-001. With respect to overall privacy program management, for example, in October 2019, PRIV developed an internal compliance document tracking system known as PRIVCATS. This system tracks the privacy compliance of all Departmental systems and programs and ensures these systems maintain compliance with DHS Directive 047-01, “Privacy Policy and Compliance,” dated July 7, 2011,⁷ and DHS Instruction 047-01-001, “Privacy Policy and Compliance,” dated July 25, 2011.⁸ Specifically, PRIVCATS allows PRIV to track important dates to ensure continual monitoring of systems, additional compliance requirements (e.g., pending PIAs), and metrics. The system also enables PRIV to create robust reporting to track trends in subject areas, privacy risks, and production for all the PRIV’s IT systems that collect, process, maintain, share, and dispose of PII.

PRIV plans to implement a continuous monitoring strategy through the requirements of DHS Directive 047-01 and Instruction 047-01-001 and the functionality provided by PRIVCATS. As DHS Directive 047-01 and DHS Instruction 047-01-001 require that program/system privacy compliance documentation be updated every three years or when changes occur, PRIV believes that tracking these updates via PRIVCATS enables PRIV to continually monitor developments and any privacy impacts to DHS programs and systems. With the development of PRIVCATS, PRIV is able to track updates to programs/systems to ensure compliance with the DHS policies. For example, PRIVCATS can track when programs/systems are approaching the three-year requirement for their privacy compliance documentation to be updated.

PRIV is currently considering ways to implement a thorough continuous monitoring strategy through more advance tracking features within PRIVCATS to improve awareness on the current state of the PRIV’s privacy controls and compliance documentation. Accordingly, PRIV will fully develop its privacy continuous monitoring strategy through multiple phases of implementation via PRIVCATS, and will identify improvements to PRIVCATS and best practices to ensure compliance with DHS policies. ECD: January 31, 2023.

⁶ <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-the-revision-of-civil-immigration-enforcement-policies-and-priorities/>

⁷ <https://www.dhs.gov/publication/privacy-policy-and-compliance-directive-047-01>

⁸ <https://www.dhs.gov/publication/privacy-policy-and-compliance-instruction-047-01-001>

Appendix XI: Comments from the Department of the Interior



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

Jennifer R. Franks
Director, Information Technology Acquisition Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Marisol Cruz Cain
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Franks and Ms. Cruz Cain:

Thank you for providing the U.S. Department of the Interior (Department) the opportunity to review and comment on the draft Government Accountability Office (GAO) report titled, *PRIVACY: Dedicated Leadership Can Improve Programs and Address Challenges* (GAO-22-105065). We appreciate GAO's review of the Department's Privacy Program.

The GAO issued several recommendations to multiple agencies, including one to the Department to address its finding. Below is a summary of actions planned to implement the recommendation.

Recommendation 26: The Secretary of Interior should establish a time frame for incorporating privacy into an organization-wide risk management strategy that includes a determination of risk tolerance and develop and document this strategy.

Response: Concur. The Department will establish a time frame to incorporate privacy into its Enterprise Risk Management Strategy, to include privacy roles, requirements for identifying and assessing privacy risks, and a determination of risk tolerance.

If you have any questions or need additional information, please contact Deborah (June) Hartley, Acting Chief Information Officer and Acting Senior Agency Official for Privacy, at june_hartley@ios.doi.gov.

Sincerely,

JOAN
MOONEY

Joan M. Mooney
Principal Deputy Assistant Secretary
Exercising the Delegated Authority of the Assistant
Secretary - Policy, Management and Budget

Digitally signed by JOAN
MOONEY
Date: 2022.08.05
13:20:55 -04'00'

Appendix XII: Comments from the Department of State



United States Department of State
Comptroller
Washington, DC 20520

AUG 11 2022

Thomas Melito
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Mr. Melito:

We appreciate the opportunity to review your draft report, "PRIVACY: Dedicated Leadership Can Improve Programs and Address Challenges" GAO Job Code 105065.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

Sincerely,

A handwritten signature in blue ink, appearing to read "William B. Davisson".

William B. Davisson (Acting)

Enclosure:

As stated

cc: GAO – Marisol Cruz Cain
A – Alaina Teplitz
OIG - Norman Brown

Department of State Comments on GAO Draft Report

**Privacy: Dedicated Leadership Can Improve Programs and Address
Challenges**
(GAO-22-105065, GAO Code 105065)

Thank you for the opportunity to comment on the GAO draft report, "*Privacy: Dedicated Leadership Can Improve Programs and Address Challenges.*"

Recommendation 32: The Secretary of State should establish a time frame for incorporating privacy into an organization-wide risk management strategy that includes a determination of risk tolerance and develop and document this strategy.

Response: The Department of State concurs with this recommendation and will work with the Bureau of Administration and the Bureau of Information Resource Management to establish a time frame for fully incorporating privacy into the Department's risk management strategy, including a determination of risk tolerance, and develop and document this strategy.

Recommendation 33: The Secretary of State should establish a time frame for fully defining the role of the Senior Agency Official for Privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages, and document these roles.

Response: The Department of State concurs with this recommendation and will work with the Bureau of Administration and the Bureau of Information Resource Management to establish a time frame to fully define and document the role of the Senior Agency Official for Privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages.

Recommendation 34: The Secretary of State should establish a time frame for fully developing a privacy continuous monitoring strategy, and develop and document this strategy.

Response: The Department of State concurs with this recommendation and will work with the Bureau of Administration and the Bureau of Information Resource Management to establish a time frame to fully develop a privacy continuous monitoring strategy and develop and document this strategy.

Appendix XIII: Comments from the Department of Veterans Affairs



DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON

August 5, 2022

Ms. Jennifer R. Franks
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Franks:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report: ***PRIVACY: Dedicated Leadership Can Improve Programs and Address Challenges*** (GAO-22-105065).

The enclosure contains the action plan to address the draft report recommendations. VA appreciates the opportunity to comment on your draft report.

Sincerely,

A handwritten signature in black ink that reads "Tanya J. Bradsher".

Tanya Bradsher
Chief of Staff

Enclosure

Enclosure

Department of Veterans Affairs (VA) Comments to
The Government Accountability Office (GAO) Draft Report
***PRIVACY: Dedicated Leadership Can Improve Programs
and Address Challenges***
(GAO-22-105065)

Recommendation 1: The Secretary of Veterans Affairs should establish a time frame for defining a process for ensuring that the senior agency official for privacy, or other designated privacy official, reviews IT capital investment plans and budgetary requests, and document this process.

VA Comment: Concur. VA agrees with the GAO conclusions and concurs with its recommendation to the Department. VA will provide the actions to be taken to address the GAO draft report recommendation in the 180-day update to the final report.

Recommendation 2: The Secretary of Veterans Affairs should fully define and document a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy.

VA Comment: Concur. VA agrees with GAO's conclusions and concurs with its recommendation to the Department. VA will provide the actions to be taken to address the GAO draft report recommendation in the 180-day update to the final report.

Recommendation 3: The Secretary of Veterans Affairs should fully define and document the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages, and document these roles.

VA Comment: Concur. VA agrees with GAO's conclusions and concurs with its recommendation to the Department. VA will provide the actions to be taken to address the GAO draft report recommendation in the 180-day update to the final report.

Recommendation 4: The Secretary of Veterans Affairs should ensure that its privacy continuous monitoring strategy includes a catalog of privacy controls and defines the frequency at which they are to be assessed.

VA Comment: Concur. The Department has taken action to ensure VA's privacy continuous monitoring (PCM) strategy includes a catalog of privacy controls and defines the frequency at which they are to be assessed. VA's Chief Privacy Officer signed the VA PCM strategy on February 16, 2022, (Attachment A). VA updated the PCM strategy in June 2022 to include the catalog of available privacy controls and the VA-defined assessment frequency for each control (Attachment B). VA posted the PCM strategy and privacy controls catalog on the VA Information Security Knowledge Service SharePoint.

VA requests closure of the recommendation.

Appendix XIV: Comments from the Environmental Protection Agency



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

July 25, 2022

OFFICE OF MISSION SUPPORT

Mr. Alfredo Gomez
Director
Natural Resources and Environment
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Gomez:

Thank you for the opportunity to review and comment on GAO's draft report, "PRIVACY - Dedicated Leadership Can Improve Programs and Address Challenges, GAO-22-105065."

The purpose of this letter is to provide the Environmental Protection Agency's (EPA) response to the draft report's findings, conclusions, and recommendation(s). The EPA agrees with the GAO's findings, conclusions, and recommendations with respect to EPA's Privacy Program.

In general, GAO found that the 24 CFO Act Agencies varied in the extent to which they addressed key practices for implementing Privacy Programs. While all Agencies have each designated a Senior Agency Official for Privacy (SAOP); many of the SAOPs do not have privacy as their primary responsibility. Additionally, all Agencies generally established policies and procedures for key privacy activities but varied in coordinating those policies and procedures with other programs and activities such as information security, budget and acquisition, workforce planning and incident response. GAO also found that many agencies did not fully incorporate privacy into their risk management strategies, nor had they developed a privacy continuous monitoring strategy. GAO concludes by stating that addressing key privacy program practices, program challenges, and privacy impact assessment effectiveness requires significant leadership commitment at Agencies.

GAO Recommendation:

Recommendation 46: The Administrator of EPA should fully develop and document a privacy continuous monitoring strategy.

Internet Address (URL) • <http://www.epa.gov>

**Appendix XIV: Comments from the
Environmental Protection Agency**


EPA Response:

The EPA agrees with this recommendation. The Office of Mission Support, Office of Information Security and Privacy has established an Information Security Continuous Monitoring (ISCM) plan. This ISCM will be updated by February 17, 2023, to specifically include the privacy controls continuous monitoring requirements as outlined in the National Institute of Standards and Technology, 800-53, Security and Privacy Controls for Information Systems and Organizations and the NIST Privacy Framework.

In closing, the EPA agrees with the findings and recommendation from the GAO report. Again, thank you for the opportunity to review the draft report. If there are any questions, please contact Lee Kelly at kelly.lee@epa.gov, 202.566.1197 (Desk), or 202.430.2451 (Mobile)

Sincerely,

VAUGHN
NOGA

 Digitally signed by
VAUGHN NOGA
Date: 2022.07.26
12:02:20 -04'00'

Vaughn Noga
Chief Information Officer

cc: Jennifer Franks; FranksJ@gao.gov
Marisol Cruz Cain; CruzCainM@gao.gov
Lee McCracken; McCrackenL@gao.gov
Shaunyce J Wallace; WallaceSJ@gao.gov
Kiana Beshir; BeshirK@gao.gov
EPA GAO Liaison Team
Erin Collard
Tonya Manning
Mark Bacharach
Lee Kelly
Dan Coogan
Jan Jablonski
Marilyn Armstrong
Afreeka Wilson
Daniela Wojtalewicz
Darryl Perez
Robert Stachowiack
Marissa Pizarick
Amir Ingram

Appendix XV: Comments from the General Services Administration

DocuSign Envelope ID: E0DAE7AE-8770-4BF4-B290-EBC7D1869A08



The Administrator

August 2, 2022

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
Washington, DC 20548

Dear Comptroller General Dodaro:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the U.S. Government Accountability Office's (GAO) draft report, *PRIVACY: Dedicated Leadership Can Improve Programs and Address Challenges* (GAO-22-105065).

GAO made the following recommendations to GSA:

- (1) GAO recommends that the GSA Administrator should fully define and document a process for ensuring that the senior agency official for privacy, or other designated privacy official, reviews IT capital investment plans and budgetary requests.
- (2) GAO recommends that the GSA Administrator should establish a time frame for fully defining a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy, and document that process.
- (3) GAO recommends that the GSA Administrator should fully define and document the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages.

GSA agrees with the recommendations and is developing a plan to address them.

If you have any questions or concerns, please contact me or Gianelle Rivera, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink that reads "Robin Carnahan".

Robin Carnahan
Administrator

U.S. General Services Administration
1800 F Street NW
Washington DC 20405-0002
www.gsa.gov

**Appendix XV: Comments from the General
Services Administration**

DocuSign Envelope ID: E0DAE7AE-8770-4BF4-B290-EBC7D1869A08

2

cc: Mr. David C. Trimble, Managing Director, Physical Infrastructure, GAO

Appendix XVI: Comments from the National Aeronautics and Space Administration

National Aeronautics and Space Administration

Mary W. Jackson NASA Headquarters
Washington, DC 20546-0001



Reply to Attn of: Office of the Chief Information Officer

Ms. Jennifer R. Franks
Director
Information Technology and Cybersecurity
United States Government Accountability Office
Washington, DC 20548

Dear Ms. Franks:

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, "Privacy: Dedicated Leadership Can Improve Programs and Address Challenges" (GAO-22-105065), dated June 30, 2022.

GAO found that the 24 Chief Financial Officers Act agencies have established privacy programs with overall responsibility for privacy policy, compliance, and risk management. However, the agencies have not fully established policies and procedures for implementing certain key practices. These include cross-agency activities such as reviewing IT budget proposals, workforce planning, and managing risks to IT systems that contain personal identifiable information (PII). Without fully establishing these elements of the privacy programs, agencies will have less assurance that they are consistently and effectively implementing privacy protections.

In the draft memorandum, GAO makes two recommendations addressed to the NASA Administrator.

Specifically, GAO recommends the NASA Administrator should:

Recommendation 1: The Administrator of NASA should incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance.

Management's Response: NASA concurs with this recommendation. NASA specifically addresses this in the strategy section of our update to NASA Procedural Requirements (NPR) 1382.1B, NASA Privacy Procedural Requirements. Specifically, NPR 1382.1B includes a section, Risk Management Strategy, which outlines the incorporation of privacy into the organization-wide risk management approach to include risk tolerance.

Estimated Completion Date: December 15, 2022.

**Appendix XVI: Comments from the National
Aeronautics and Space Administration**

2

Recommendation 2: The Administrator of NASA should fully define and document the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages.

Management's Response: NASA concurs with this recommendation. The role of Privacy officials (Senior Agency Official for Privacy, Chief Privacy Officer, and Privacy Managers) is defined in NASA Policy Directive 1382.17, NASA Privacy Policy. Additionally, IT Security Handbook 1382.03_01 outlines the responsibilities for reviewing and approving privacy threshold assessments (PTAs) and privacy impact assessments (PIAs), which determine/document any PII maintained in information systems. This review and approval process for PTAs and PIAs directly impacts the system categorizations (any system containing PII must at a minimum be categorized as moderate) and must be completed prior to authorization to operate. NASA further outlines roles and responsibilities for the privacy official in assessment and authorization process handbooks and role view documents.

Estimated Completion Date: December 15, 2022.

We have reviewed the draft report for information that should not be publicly released. As a result of this review, we have not identified any information that should not be publicly released.

Once again, thank you for the opportunity to review and comment on the subject draft report. If you have any questions or require additional information regarding this response, please contact Lara Petze at (202) 358-5489.

Sincerely,

JEFFREY SEATON Digitally signed by JEFFREY SEATON
Date: 2022.08.08 08:20:26 -04'00'

Jeff Seaton
Chief Information Officer

Appendix XVII: Comments from the Nuclear Regulatory Commission



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

July 20, 2022

Jennifer Franks, Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Ms. Franks:

Thank you for providing the U.S. Nuclear Regulatory Commission (NRC) with the opportunity to review and comment on the U.S. Government Accountability Office (GAO) Draft Report on Privacy: Dedicated Leadership Can Improve Program and Address Challenges GAO-22-105065. The NRC staff has reviewed the draft report and is in general agreement with its findings and recommendations. The NRC's comments on the two recommendations are listed below:

- **GAO Recommendation:** The Chairman of NRC should fully define and document a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy (Recommendation 52).

NRC Response: The NRC agrees with this recommendation and will revise the NRC's Privacy Program Plan, Section 2.2 (NRC Privacy Office Organization), and Section 3 (Privacy Workforce Management) to fully define and document that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy.

- **GAO Recommendation:** The Chairman of NRC should fully define and document the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages (Recommendation 53).

NRC Response: The NRC agrees with this recommendation and will revise its Risk Management Framework Process (CSO-PROS-2030) to fully define and document the role of the senior agency official for privacy and other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages.

**Appendix XVII: Comments from the Nuclear
Regulatory Commission**

J. Franks

2

If you have any questions regarding the NRC's response, please contact Scott Flanders by phone at (301) 415-6717, or by e-mail at Scott.Flanders@nrc.gov or John Jolicoeur by phone at (301) 415-1642, or by e-mail at John.Jolicoeur@nrc.gov.

Sincerely,



Haney, Cathy signing on behalf
of Dorman, Dan
on 07/20/22

Daniel H. Dorman
Executive Director
for Operations

Appendix XVIII: Comments from the Small Business Administration



U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, DC 20416

DATE: July 27, 2022

TO: Lee McCracken
Senior Analyst, IT and Cybersecurity
U.S. Government Accountability Office

FROM: Stephen Kucharski
Acting Chief Information Officer

SUBJECT: SBA Management Response: GAO Draft Report 22-105065,
Privacy - Dedicated Leadership Can Improve Programs and
Address Challenges

We appreciate the opportunity to review the Government Accountability Office (GAO) draft report entitled *Privacy: – Dedicated Leadership Can Improve Programs and Address Changes (GAO-22-105065)*. Select Federal agencies participated in a GAO engagement which included the Small Business Administration (SBA) around last fall of fiscal year 2022, relating to our Privacy Program.

This review was based on a request from the Senate Committee on Homeland Security and Governmental Affairs with the overall objectives of insight to the selected agency's privacy programs. The intent and purpose were to have an idea of the various agencies privacy programs, identify challenges that the agencies maybe experiencing, and how agencies perceive the practicality of the privacy impact assessments (PIA) based upon their survey response.

The Office of the Chief Information Officer finds this GAO draft report to be consistent with our submissions and initial comments of the Statement of Facts we submitted April 2022.

In reference to the near final draft report, SBA did not have any sensitive comments. We identified three editorial comments within the document needing attention:

- Page 7: Spell out first instance of acronym OIRA. It is spelled out in the next paragraph, perhaps the paragraphs were switched during edits.
- Page 22: Responsible office: Please change "Cybersecurity and Privacy Program, OCIO" to "Information Security Division, OCIO". Note: (Currently we are the "Information Security Division, OCIO" soon TBD "Cybersecurity and Privacy Division, OCIO" ((or something similar)).
- Page 72: Please remove the word "take" in the first sentence for clarity or revise the paragraph. The sentence currently reads: "The Administrator of SBA should take fully define and document a..."

**Appendix XVIII: Comments from the Small
Business Administration**

SBA concurs with GAO's only recommendation for SBA:
"The Administrator of SBA should fully define and document a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. (Recommendation 60)".

SBA appreciates the opportunity to participate, and found the information to be most valuable, especially how we fare with our fellow federal agencies and the best practices of privacy advocacy organizations, privacy experts, and academia.

Sincerely,

Stephen Kucharski
Stephen Kucharski
Acting Chief Information Officer
Office of Chief Information Officer (OCIO)

Appendix XIX: Comments from the Social Security Administration



SOCIAL SECURITY
Office of the Commissioner

July 29, 2022

Ms. Jennifer R. Franks, Director
Center for Enhanced Cybersecurity
Ms. Marisol Cruz Cain, Director
Information Technology and Cybersecurity
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Director Franks and Director Cruz Cain,

Thank you for the opportunity to review the draft report "PRIVACY: Dedicated Leadership Can Improve Programs and Address Challenges" (GAO-22-105065). We agree with the recommendations.

Please contact me at (410) 965-2611 if I can be of further assistance. Your staff may contact Trae Sommer, Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

A handwritten signature in blue ink that reads "Scott Frey".

Scott Frey
Chief of Staff

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Appendix XX: Comments from the U.S. Agency for International Development



July 27, 2022

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity

Marisol Cruz Cain
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20226

Re: Federal Agency Privacy Programs (GAO-22-105065)

Dear Ms. Franks and Ms. Cain:

I am pleased to provide the formal response of the U.S. Agency for International Development (USAID) to the draft report produced by the U.S. Government Accountability Office (GAO) titled, *Federal Agency Privacy Programs* (GAO-22-105065). USAID appreciates the continued work of GAO in reporting on Federal Agency Privacy Programs and would like to thank the office for the opportunity to review and provide comments.

USAID appreciates the opportunity to participate in the Audit of Federal Privacy Programs and looks forward to working with you again in the future to continuously make improvements to the privacy program.

I am transmitting this letter and the enclosed comments regarding the recommendations from USAID for inclusion in the GAO's final report. Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement. We appreciate the opportunity to participate in the complete and thorough evaluation of our Privacy Program.

Sincerely,

Colleen R. Allen
Colleen Allen
Assistant Administrator
Bureau for Management

Enclosure: a/s

**COMMENTS BY THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT ON
THE DRAFT REPORT PRODUCED BY THE U.S. GOVERNMENT
ACCOUNTABILITY OFFICE (GAO) TITLED, *Federal Agency Privacy Programs*
(GAO-22-105065).**

The U.S. Agency for International Development (USAID) would like to thank the U.S. Government Accountability Office (GAO) for the opportunity to respond to this draft report. We appreciate the extensive work of the GAO engagement team, and the specific findings that will help USAID achieve greater effectiveness in our Privacy Program.

The draft report contains two recommendations for USAID.

1. The Administrator of USAID should fully define and document a process for ensuring that the senior agency official for privacy, or other designated privacy official, reviews IT capital investment plans and budgetary requests. (Recommendation 66)

- **Comment:** The Director of the Office of Acquisition and Assistance (M/OAA) in the Bureau for Management is a permanent member of the Information Technology Steering Subcommittee (ITSS) that provides oversight of capital investment plans and requests. The incumbent of the position is also currently Acting as the Deputy Assistant Administrator for the Management Bureau (DAA/M). The DAA/M is designated at USAID as the Senior Agency Official for Privacy (SAOP). Therefore, because of the Acting position of the DAA/M, the Agency SAOP reviewed the most recent capital investment plans and budget requests. USAID agrees that clearly defining the role of the SAOP in the budget and acquisition process would help ensure consistent oversight and involvement in a critical privacy activity. Welcoming the opportunity to strengthen the effectiveness of the Privacy Program, USAID is looking into how to include the Agency's SAOP input as a voting member of the subcommittee.

- **Status:** The request was adopted by the Agency's Chief Privacy Officer and accepted by the ITSS Secretariat. The Agency's Management Operations Council (MOC) will vote on the request in August.

- **Target Completion Date:** 10/31/2022

2. The Administrator of USAID should incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance. (Recommendation 67)

**Appendix XX: Comments from the U.S. Agency
for International Development**

- **Comment:** USAID agrees that an effective privacy risk management strategy supports consistent decision-making for identifying, assessing and responding to privacy risks. Prior to the GAO Engagement, USAID published a [Risk Appetite Statement](#) (2018), which integrates considerations for protecting personally identifiable information (PII) into the broader Enterprise-wide Risk Management Framework. Doing so allows the Agency an opportunity to make decisions about privacy risks in the context of other risks. For instance, the Agency adopted a LOW risk threshold for security, which incorporates violations of information security that lead to the unauthorized disclosure of PII. Similarly, the risk threshold for Information Technology is Medium, but is LOW for weaknesses that threaten the security of PII. Understanding, however, that while managing cybersecurity risk contributes to managing privacy, it is not sufficient, as those risks can arise in activities unrelated to cybersecurity incidents.

In response to this finding, the Privacy Program seeks to update USAID's Risk Appetite Statement to acknowledge the overlap between privacy and cybersecurity risks without overlooking other privacy-related risks to better inform decision-making.

- **Status:** Awaiting Final Approval of updated Risk Appetite Statement.
- **Target Completion Date:** 10/31/2022

Appendix XXI: Comments from the Office of Personnel Management



Office of Privacy and Information
Management

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Mr. Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Dodaro:

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, Federal Agency Privacy Programs, GAO-22-105065.

Responses to your recommendations are provided below.

Recommendation # 54: The Director of OPM should establish a time frame for updating the agency's policy for creating, reviewing, and publishing system of records notices, and make these updates.

We partially concur: OPM concurs with the concept that fully documented processes for creating, reviewing, and publishing systems of records notices (SORNs) are beneficial, but does not concur with the implication in the Report that OPM has no process in place and as such is impeding publication of SORNs. OPM adheres to the requirements of the Privacy Act, OMB Circular A-108, and other relevant OMB guidance on the content and preparation of SORNs. The Office of Privacy and Information Management (OPIM) communicates these requirements to program offices within the agency and is in regular contact with offices throughout OPM when the need to establish or modify a system of records is identified. OPIM works closely with the relevant offices to draft new or modified SORNs and, once drafted, the Senior Agency Official for Privacy reviews and approves the draft SORN to be routed through the established formal inter-agency clearance process, to include review and approval by the relevant program office, the Office of the General Counsel, the

Office for Congressional, Legislative, and Intergovernmental Affairs, the Office of Communications, and the Office of the Director. Once cleared via that process, OPIM submits the draft SORN to OMB and Congress for statutorily required review and publishes it in the Federal Register. OPM's Administrative Delegations of Authority also denote relevant offices' authority with respect to the drafting and approval of SORNs. Within OPM, this process is clear and does not impede timely establishment, review, or modification of SORNs. OPM recognizes that more fully documenting guidance and process regarding SORNs will benefit OPM in the long-term and is committed to reviewing and updating any outdated SORN guidance by the close of FY 2023.

Recommendation #55 The Director of OPM should define and document procedures for coordination between privacy and information security functions.

We partially concur: We agree that the coordination of privacy and security are necessary and valuable, but we do not concur with the implication that such coordination does not occur at our agency. The Office of Privacy and Information Management regularly coordinates with the Office of the Chief Information Officer (OCIO), including with those in OCIO responsible for information security, both formally and informally. The Senior Agency Official for Privacy (SAOP) is both a voting member of the Investment Review Board, co-chaired by the CIO, the Capital Investment Council, where both the SAOP and the CIO are voting members, and the Risk Management Council, where both are also voting members. Each of these bodies provide formal, consistent opportunity for coordination between the privacy and security functions. In addition, the privacy and security teams coordinate to review, revise, and draft as needed annual security and privacy awareness training. Moreover, the privacy team has regular and recurring meetings with our information security colleagues to discuss upcoming security assessments, FIPS 199 determinations, and to coordinate the completion of privacy and security assessments and documentation in the process of obtaining or renewing Authorizations to Operate (ATOs). Final ATO and ATU packages and FIPS 199 determinations are required to be circulated to the SAOP, who signs off on the routing slip to confirm receipt. This coordination across these two functional areas is ongoing and evolving. For example, starting with the second quarter FY 22, the two programs commenced regularly

scheduled meetings biweekly to discuss the implementation of NIST 800-53, rev. 5 regarding security and privacy controls revisions. During FY 23, we will evaluate the need for increased documentation of the coordination between the privacy and security functions.

Recommendation #56 The Director of OPM should fully define and document a policy and process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy.

We do not concur: OPM's Senior Agency Official for Privacy (SAOP) is a member of the Senior Executive Service and the office head for the Office of Privacy and Information Management, the central OPM office that houses OPM's centralized privacy program. In that role, the SAOP is responsible for evaluating the hiring, training, and professional development needs of the office generally and the privacy program specifically. OPM provided GAO with evidence to support the fact that the SAOP is responsible for meeting the hiring needs of the agency regarding privacy. We have developed career ladder positions for the privacy program in an effort to better recruit and retain privacy professionals within the office and have reformulated the structure of the office over time to dedicate FTEs to the privacy program. Beyond the needs of the centralized privacy program, we regularly interact with our colleagues in OCIO and provide opportunities for informal and formal cross-training, such as the SAOP providing the opportunity to send information system security officials to attend the Federal Privacy Council's Privacy Boot Camp; engaging in the development of privacy and security awareness training annually, and where possible bringing in detailees from other offices at OPM.

Recommendation #57 The Director of OPM should incorporate privacy into an organization-wide risk management strategy that includes a determination of risk tolerance.

We do not concur. As evidenced in documentation provided to GAO, the Senior Agency Official for Privacy has been a member of the OPM Risk Management Council (RMC), the OPM body that identifies, evaluates, and works to mitigate enterprise-wide risk since approximately 2017. The RMC's risk registers consistently address privacy risks at the enterprise level. In

addition to that enterprise-wide approach, the privacy team address risk at a program level through engagement with the program offices to conduct Privacy Threshold Analyses and Privacy Impact Assessments. We are continually working to better evaluate and address privacy risk across OPM, but privacy is incorporated into the enterprise-wide risk management through the RMC.

Recommendation #58 The Director of OPM should establish a time frame for fully defining the role of the senior agency official for privacy or other designated privacy official in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages, and document these roles.

We partially concur. OPM disagrees with the portion of the recommendation that indicates that the role of the Senior Agency Official for Privacy (SAOP) is not defined in reviewing and approving systems categorizations, overseeing privacy control assessments and reviewing authorization packages. We are conducting these activities. As noted above, the SAOP along with the privacy team, is involved in FIPS 199 system categorizations and in authorization packages. The privacy team conducts privacy control assessments as part of our continuous monitoring review. The privacy and security teams are currently engaged in a review and evaluation of NIST 800-53 rev. 5, examining roles and responsibilities with respect to the controls and their selection and evaluation. We partially concur with the recommendation in that we are currently evaluating with OCIO colleagues whether and how to better document this and the appropriate time frame for doing so.

Recommendation #59 The Director of OPM should fully develop and document a privacy continuous monitoring strategy.

We partially concur. OPM disagrees with the portion of the recommendation that indicates that we do not have a continuous monitoring strategy. OPM has a current continuous monitoring strategy in place which provides a comprehensive view of each system, including the NIST 800-53 rev. 4 privacy controls, at a defined frequency. We partially concur in that as OPM moves to implement NIST 800-53 rev. 5, which more directly incorporates the privacy controls with the security controls process, we will further evaluate our approach to privacy continuous monitoring and review the need for more comprehensive documentation by the end of FY 23.

**Appendix XXI: Comments from the Office of
Personnel Management**

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Marc Flaster, Senior Advisor to the Chief Privacy Officer, 202-577-9016 at Marc.Flaster@opm.gov.

Sincerely,

KELLIE RILEY Digitally signed by KELLIE RILEY
Date: 2022.08.02 22:59:23 -0400

Kellie Cosgrove Riley
Senior Agency Official for Privacy
Office of Personnel Management

www.opm.gov

Empowering Excellence in Government through Great People

www.usajobs.gov

Appendix XXII: GAO Contacts and Staff Acknowledgments

GAO Contacts

Jennifer R. Franks, franksj@gao.gov, (404) 679-1831

Marisol Cruz Cain, cruzcainm@gao.gov, (202) 512-5017

Staff Acknowledgments

In addition to the contacts listed above, the following staff made key contributions to this report: Lee McCracken (analyst in charge), Christy Abuyan, Gerard Aflague, Alexander Anderegg, Logan Arkema, Kiana Beshir, Alina Budhathoki, Christopher Businsky, Joseph P. Cruz, Wayne Emilien, Donna Epler, Franklin Jackson, Melissa Melvin, Ahsan Nasar, Brian Palmer, Monica Perez-Nelson, Scott Pettis, Kelly Rubin, Andrew Stavisky, Adam Vodraska, Jonathan Wall, and Shaunyce Wallace.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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

