GAO Highlights

Highlights of GAO-22-105065, a report to congressional requesters

September 2022

PRIVACY

Dedicated Leadership Can Improve Programs and Address Challenges

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.

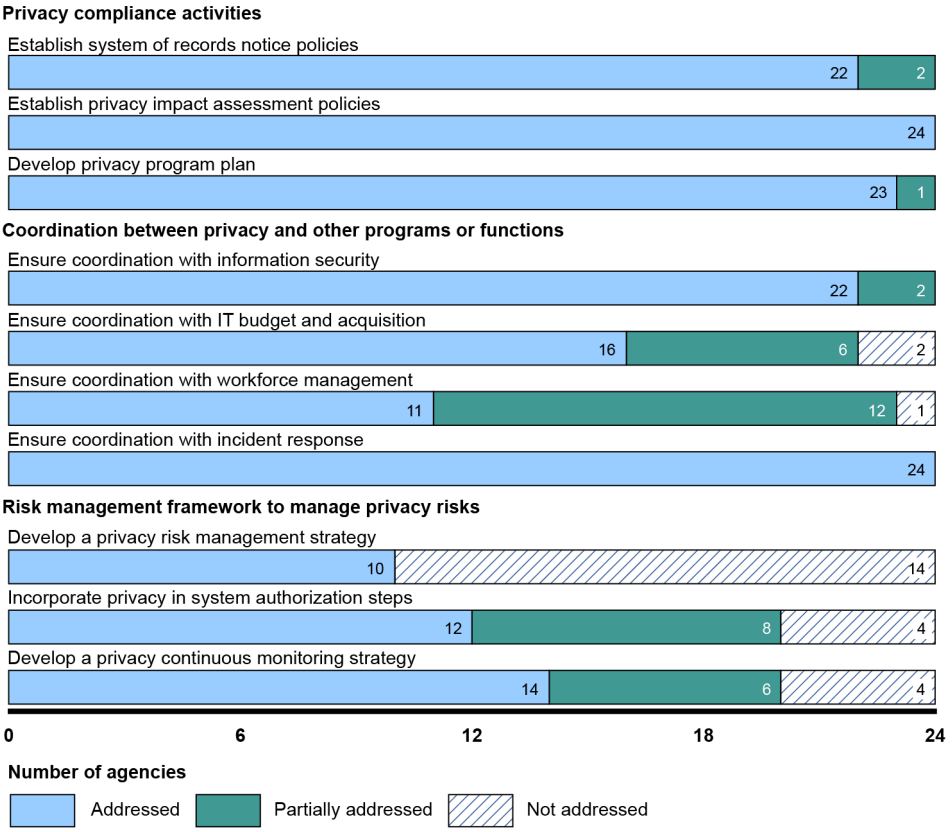
View GAO-22-105065. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov, or Marisol Cruz Cain at (202) 512-5017 or cruzcainm@gao.gov.

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



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.