U.S. GOVERNMENT ACCOUNTABILITY OFFICE

CYBERSECURITY HIGH-RISK SERIES:

Challenges in Protecting Privacy and Sensitive Data

Accessible Version

Overview

Federal agencies and our nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on technology systems to carry out fundamental operations and to process, maintain, and report vital information. The security of these systems and data is also vital to safeguarding individual privacy and protecting the nation's security, prosperity, and well-being.

However, risks to these essential technology systems are increasing—in particular, malicious actors are becoming more willing and capable of carrying out cyberattacks. Such attacks could result in serious harm to human safety, national security, the environment, and the economy. Agencies and critical infrastructure owners and operators must protect the confidentiality, integrity, and availability of their systems and effectively respond to cyberattacks.

We have designated information security as a government-wide high-risk area since 1997. We expanded this high-risk area in 2003 to include protection of critical cyber infrastructure. In 2015, we expanded it again to include protecting the privacy of personally identifiable information.

This is the last in a series of four reports that lay out the main cybersecurity areas the federal government should urgently address. It focuses on protecting privacy and sensitive data.[1] We have made 236 recommendations in public reports since 2010 in this area. About 140 of these recommendations were not implemented as of December 2022. Until these are fully implemented, federal agencies will be more limited in their ability to protect private and sensitive data entrusted to them.

For more information on this report and others in this series, visit https://www.gao.gov/cybersecurity.

What actions should the federal government take to protect privacy and sensitive data?

Federal agencies should fully address key practices for implementing privacy programs.

Federal agencies that collect personally identifiable information (PII)—such as birthplaces and Social Security numbers—are required to establish programs to protect it. In September 2022, our review of 24 agencies found that most had generally established policies and procedures for key privacy program activities. These activities included developing system-of-records notices that identify types of personal data collected, conducting privacy impact assessments, and documenting privacy program plans (see fig. 1).[2]

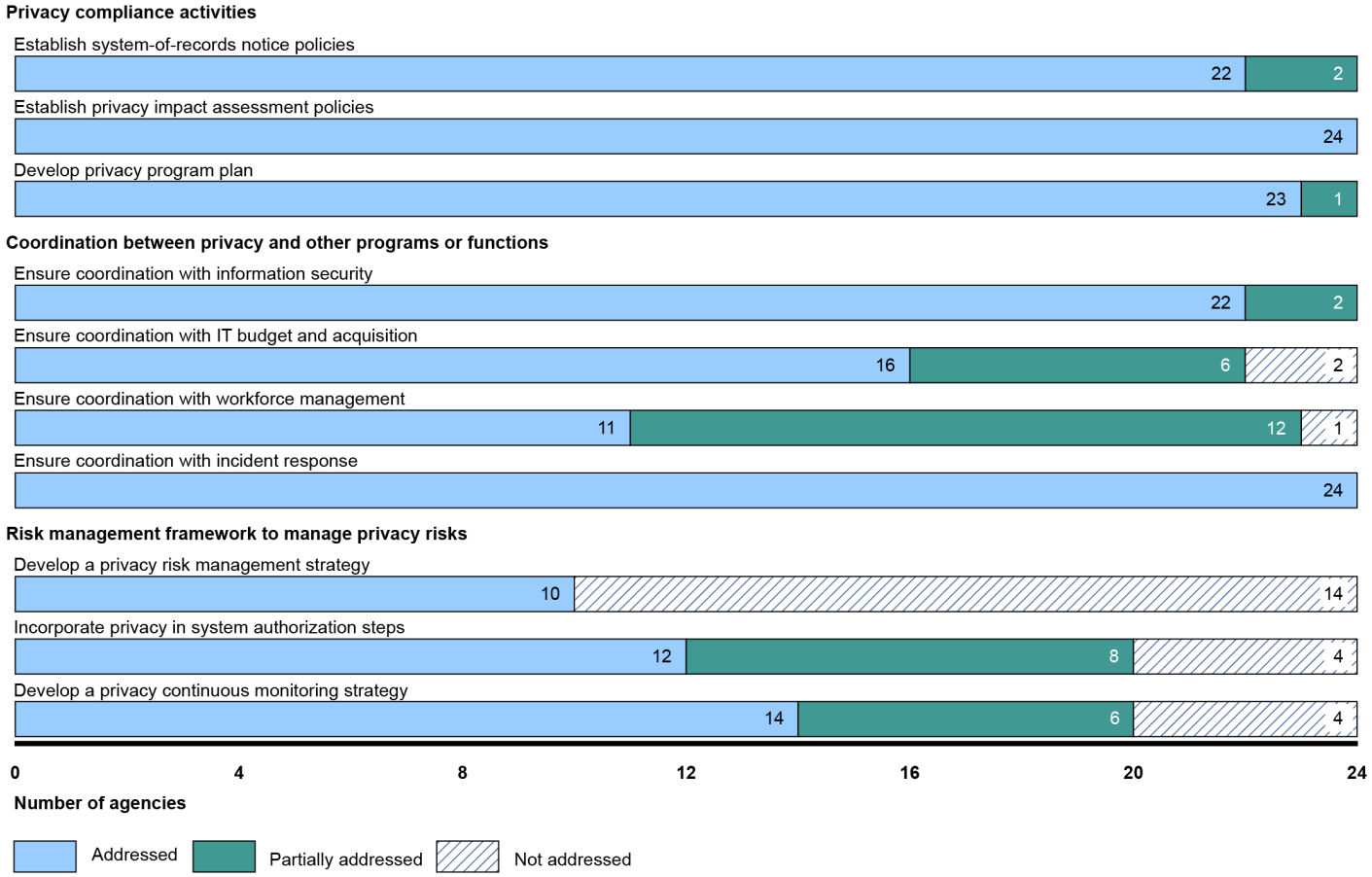
[1]In 2018, GAO reported that the federal government needed to address four major cybersecurity challenges related to (1) establishing a comprehensive cybersecurity strategy, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. For our reports on the first three challenge areas, see GAO, *Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight*, GAO-23-106415 (Washington, D.C.: Jan. 19, 2023); *Cybersecurity High-Risk Series: Challenges in Securing Federal Systems and Information,* GAO-23-106428 (Washington, D.C.: Jan. 31, 2023); and *Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure,* GAO-23-106441 (Washington, D.C.: Feb. 7, 2023).

[2]Privacy impact assessments are used to analyze how personal information is collected, stored, shared, and managed.

The 24 agencies we reviewed were 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; the General Services Administration; the National Aeronautics and Space Administration; the National Science

Agencies varied in establishing policies and procedures for coordinating privacy programs with other agency functions. Further, many agencies did not fully incorporate privacy into their risk management strategies, provide for privacy officials' input into the authorization of systems containing PII, or develop a continuous monitoring strategy for privacy. Without fully establishing these elements of their privacy programs, agencies have less assurance that they are consistently implementing privacy protections.

Figure 1: 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-23-106433

We also reported that these 24 agencies had each designated a senior agency official for privacy. However, most of these officials did not have privacy as their primary responsibility and had numerous other duties related to managing IT and information security. Legislation establishing a dedicated, senior-level privacy official could enhance the leadership commitment needed to address privacy issues across the government.

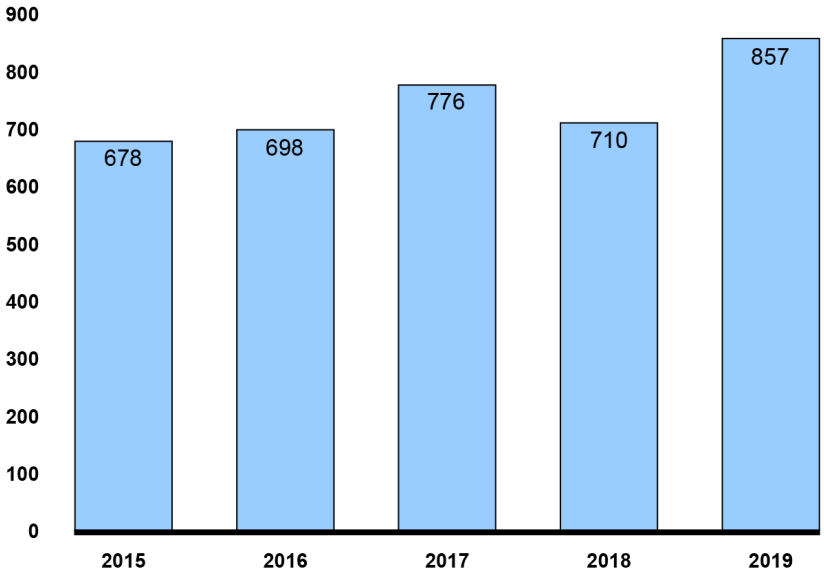
- **We recommended** that Congress consider legislation to designate a dedicated, senior-level privacy official at agencies that lacked one. We also made two recommendations to the Office of Management and Budget (OMB) to facilitate information sharing to help agencies address selected challenges and better implement privacy impact assessments. Finally, we made 62 recommendations to 23 of the 24 agencies we reviewed to fully implement all of the key practices for their privacy programs. Twenty out of 23 agencies, including OMB, agreed with the recommendations. However, the recommendation to Congress and 62 out of 64 recommendations to OMB and agencies had not yet been implemented as of February 2023.

Foundation; the Nuclear Regulatory Commission; the Office of Personnel Management; the Small Business Administration; the Social Security Administration; and the U.S. Agency for International Development.

The Department of Homeland Security (DHS) needs to improve its oversight of contractors handling personal information.

In December 2021, we reported that federal agencies, including DHS, had reported increasing numbers of privacy incidents that have placed sensitive information at risk of potentially serious impacts on federal operations, assets, and people. Figure 2 shows the number of privacy incidents DHS's Privacy Office reported to Congress annually from 2015 through 2019.

Figure 2: Privacy Incidents Reported to Congress by the Department of Homeland Security (DHS), 2015 through 2019



Source: GAO analysis of DHS provided data. | GAO-23-106443

DHS is responsible for a wide variety of functions that are critically important to maintaining the security of our nation's citizens. To carry out these functions, the department needs to collect and maintain extensive amounts of detailed and sometimes sensitive PII. In many cases, DHS leverages the capabilities and expertise of contractors to assist in its various missions and grants contractors access to PII to perform the work.

Federal law and implementing policies and guidance from OMB and the National Institute of Standards and Technology require agencies to ensure that agency information, including information collected or maintained by a contractor, is adequately protected.[3] DHS developed policies and procedures to meet these requirements related to the protection of PII that is collected, used, or stored by contractors. We found that the six selected DHS component agencies complied with most of DHS's policies and procedures, but gaps existed.[4] For example, the U.S. Coast Guard did not demonstrate that it identified and addressed gaps in privacy compliance, and DHS's Headquarters did not administer role-based privacy training.

Regarding privacy incidents, one component did not document all necessary remediation activities. Fully documenting remediation activities helps ensure that all appropriate steps have been taken to lessen potential harm that the loss, compromise, or misuse of PII could have on affected individuals.

[3]See Federal Information Modernization Act of 2014 (FISMA), Pub. L. No. 113-283 (Dec. 18, 2014) codified at 44 USC §§ 3551-3559; see also Office of Management and Budget, *Managing Information as a Strategic Resource*, OMB Circular No. A-130 (July 28, 2016); and National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 5 (Dec. 10, 2020).

[4]The six selected DHS component agencies are the U.S. Coast Guard, U.S. Customs and Border Protection, the U.S. Department of Homeland Security Headquarters, the Federal Emergency Management Agency, U.S. Immigration and Customs Enforcement, and the Transportation Security Administration.

- **We recommended** that the selected DHS components improve their oversight of contractors' privacy protections and remediation of incidents. The seven actions included providing targeted role-based privacy training to contractors who are responsible for privacy protections and ensuring that recommendations to notify affected individuals of privacy incidents are fully documented in the incident database. DHS agreed with the recommendations; however, none of these seven recommendations had been implemented as of December 2022.

What actions should the federal government take to appropriately limit the collection and use of personal information and ensure it is obtained with appropriate knowledge or consent?

Federal law enforcement agencies should better assess privacy and other risks associated with facial recognition technology.

In June 2021, we reported on the results of our survey of 42 federal agencies that employ law enforcement officers about their use of facial recognition technology.[5] Twenty reported owning systems with facial recognition technology or using systems owned by other entities, such as other federal, tribal, state, local, and territorial governments and non-government entities.[6] See figure 3 for examples of the types of photos used in federal systems with facial recognition technology.

Figure 3: Types of Photos Used by Federal Agencies That Employ Law Enforcement Officers

Types of photos used by federal agencies that employ law enforcement officers

Federal agencies reported using a number of systems with facial recognition technology. The following list includes examples of the types of photos included in these systems, as reported by system owners and users:

- Mug shot
- Publicly available on the internet
- Passport
- Visa application
- U.S. entry/exit
- Video/closed circuit television
- Terrorist screening database
- Foreign nationals and U.S. citizens who are known or suspected threats to the nation
- Employee
- State identification
- Driver's license
- Corrections identification
- Individuals under supervision

Source: GAO analysis of survey data; images: lidiia/stock.adobe.com. I GAO-23-106443

Agencies reported using the technology to support several activities (e.g., criminal investigations) and in response to COVID-19 (e.g., to verify an individual's identity remotely). Six agencies reported using the technology on images of the unrest, riots, or protests following the death of George Floyd in May 2020. Three agencies reported using it on images of the events at the U.S. Capitol on January 6, 2021. All fourteen agencies that reported using the technology to support criminal investigations also reported using systems owned by nonfederal entities. However, only one of those 14 was aware of what nonfederal systems employees used. By having a mechanism to track what nonfederal systems employees use and assessing privacy and accuracy-related risks, agencies can better mitigate risks to themselves and the public.

- **We recommended** that 13 federal agencies implement a mechanism to track what nonfederal systems with facial recognition technology employees are using, and

[5]Facial Recognition Technology is used to help identify an unknown individual in a photo or video surveillance.

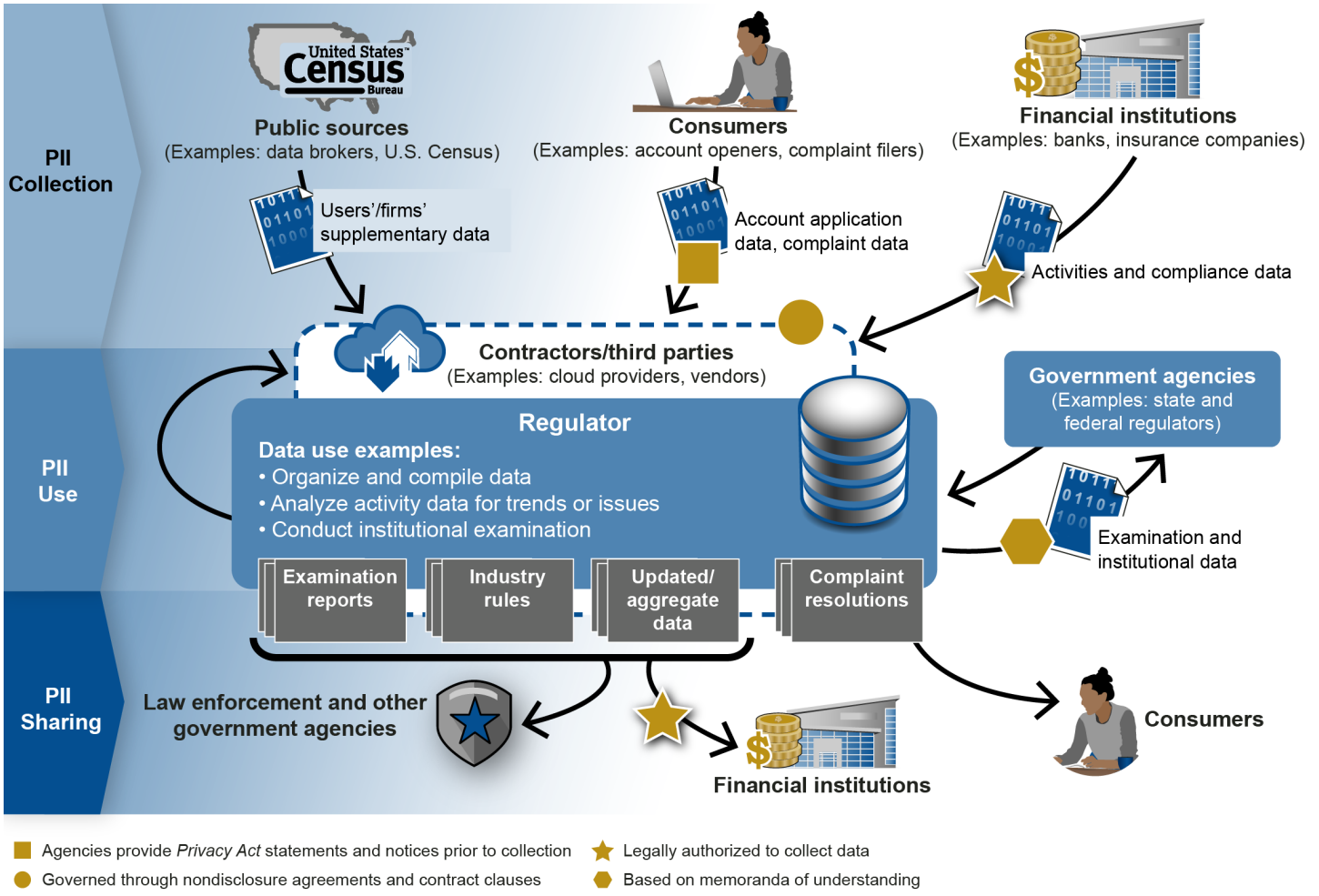
[6]The following agencies owned systems with facial recognition technology: the Department of Veterans Affairs, the Federal Bureau of Prisons, the National Aeronautics and Space Administration, and the Office of Protective Services. The following agencies used another entity's system: the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Food and Drug Administration; the Internal Revenue Service; the U.S. Park Police; the Bureau of Diplomatic Security; the U.S. Fish and Wildlife Service; the U.S. Capitol Police; the U.S. Postal Inspection Service; the Drug Enforcement Administration; U.S. Immigration and Customs Enforcement; the U.S. Marshals Service; and U.S. Probation and Pretrial Services. The following agencies owned systems and used another entity's system with facial recognition technology: U.S. Customs and Border Protection, the Pentagon Force Protection Agency, the Transportation Security Administration, the Federal Bureau of Investigation, and the U.S. Secret Service.

assess the risks of using these systems.[7] Twelve of the 13 agencies concurred with both recommendations directed towards them. However, 21 of the 26 recommendations had not yet been implemented as of December 2022.

Federal financial regulators should enhance their protection of personal information.

In January 2022, we reported that the five federal financial regulators we reviewed had built more than 100 information system applications that regularly collect and use extensive amounts of PII to fulfill their regulatory missions.[8] These regulators collect PII directly from individuals and financial institutions and share it with entities such as banks or service providers, contractors and other third parties, and other federal and state regulators. Regulators use the PII to conduct supervisory examinations of financial institutions and to receive and respond to complaints or inquiries from customers (see fig. 4).

Figure 4: Collection, Use, and Sharing of Personally Identifiable Information (PII) at Selected Federal Financial Regulators



Source: GAO. | GAO-23-106443

We reported that all five financial regulators created privacy programs that generally take steps to protect PII in accordance with key practices in federal guidance. However,

[7]The 13 federal agencies include the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Drug Enforcement Administration; the Federal Bureau of Investigation; the U.S. Marshals Service; U.S. Customs and Border Protection; the U.S. Secret Service; the U.S. Fish and Wildlife Service; the U.S. Park Police; the Bureau of Diplomatic Security; the Food and Drug Administration; the Internal Revenue Service; the U.S. Postal Inspection Service; and the U.S. Capitol Police.

[8]The five selected financial regulators include the Consumer Financial Protection Bureau and the four federal prudential regulators—the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, the National Credit Union Administration, and the Office of the Comptroller of the Currency.

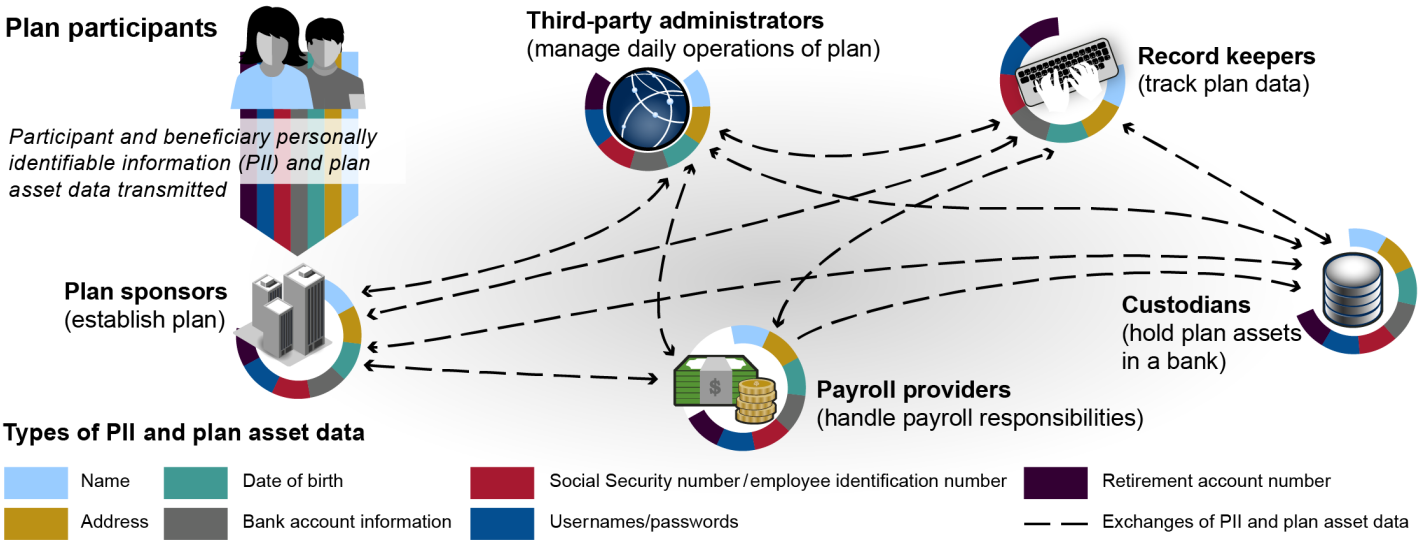
four of the regulators did not fully implement key practices in other privacy protection areas. For example, the Board of Governors of the Federal Reserve System (Federal Reserve) and National Credit Union Administration did not document steps taken to minimize the collection and use of PII. We also reported that the Federal Deposit Insurance Corporation (FDIC) and Federal Reserve did not establish agency-wide metrics to monitor privacy controls, and the Federal Reserve and the Office of the Comptroller of the Currency had not fully tracked decisions by program officials on the selection and testing of privacy controls.[9] Until these regulators take steps to mitigate these weaknesses, the PII they collect, use, and share could be at increased risk of compromise.

- **We recommended** that federal financial regulators better ensure the privacy of the PII that they collect, use, and share.[10] The regulators each described the steps they planned to take to implement the recommendations. However, six of the eight recommendations had not yet been implemented as of December 2022.

Federal guidance could help mitigate cybersecurity risks in 401(k) and other retirement plans.

Defined contribution (DC) retirement plan sponsors and their service providers—record keepers, third party administrators, custodians, and payroll providers—share a variety of PII and plan asset data among them to assist with carrying out their respective functions. The sharing and storing of this information can lead to significant cybersecurity risks for plan sponsors and their service providers as well as plan participants (see fig. 5).

Figure 5: Data Sharing among Plan Sponsors and Service Providers in Defined Contribution Plans



Source: GAO analysis of industry information. | GAO-23-106443

In February 2021, we reported that federal requirements and industry guidance could help mitigate cybersecurity risks in DC plans.[11] This includes requirements that pertain to entities directly engaged in financial activities involving DC plans. However, not all

[9]Privacy controls are the administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.

[10]We made recommendations to the FDIC, the Federal Reserve, the National Credit Union Administration, and the Office of the Comptroller of the Currency.

[11]See The White House, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636, (Washington, D.C., Feb. 12, 2013); and National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1 (Gaithersburg, MD: April 2018). Industry guidance includes the Society of Professional Asset Managers and Record Keepers (SPARK) Institute, Inc., *Industry Best Practice Data Security Reporting*, Release 1.0 (Simsbury, CT: Sept. 20, 2017), and the American Institute of Certified Public Accountants' *System and Organizational Control for Cybersecurity Framework* developed in 2017.

entities involved in DC plans were considered to have such direct engagement, and other cybersecurity mitigation guidance was voluntary. Therefore, entities could potentially be left without clear federal requirements or standards to follow to mitigate cybersecurity risks.

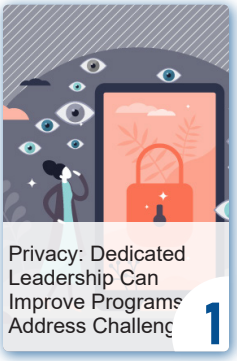
In addition, we reported that the Department of Labor (DOL) had not established minimum cybersecurity expectations for protecting PII and plan assets. Without guidance, DOL lacks assurance this sensitive information is being adequately or consistently protected. This potential lack of protection could result in substantial harm to participants and beneficiaries including loss or theft of money, identity theft, or litigation involving plan fiduciaries and their administrators.

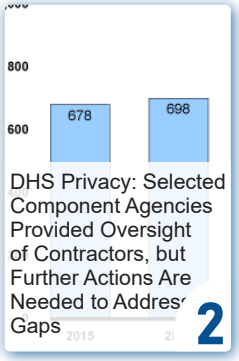
- **We recommended** that DOL establish minimum expectations for addressing cybersecurity risks in DC plans. The department agreed with the recommendation and issued new guidance for plan sponsors and service providers on best practices for maintaining cybersecurity in April 2021. However, we maintain that a minimum set of expectations for mitigating cybersecurity risks should be established, and we will follow up with DOL on their efforts to do so.

GAO's Prior Work

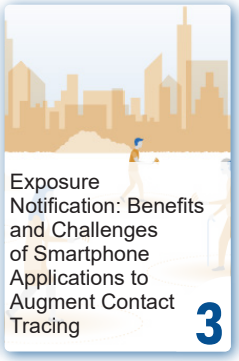
We have previously reported on the numerous challenges that the federal government faces and have made recommendations aimed at improving the protection of privacy and sensitive data. Additionally, we made recommendations related to appropriately limiting the collection and use of personal information and ensuring it is obtained with appropriate knowledge or consent. Key reports focus on the following topics:

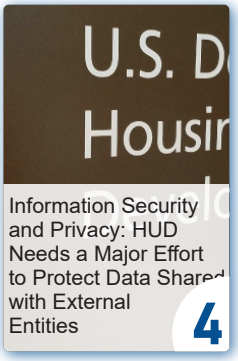
Improve federal efforts to protect privacy and sensitive data


Privacy: Dedicated Leadership Can Improve Programs Address Challeng 1

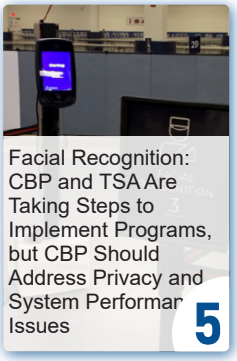


DHS Privacy: Selected Component Agencies Provided Oversight of Contractors, but Further Actions Are Needed to Addres Gaps 2

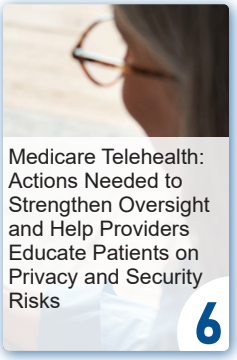

Exposure Notification: Benefits and Challenges of Smartphone Applications to Augment Contact Tracing 3



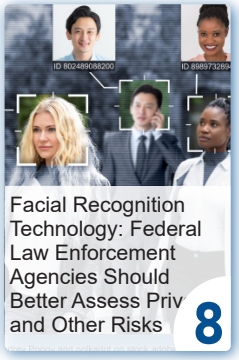
Information Security and Privacy: HUD Needs a Major Effort to Protect Data Shared with External Entities 4

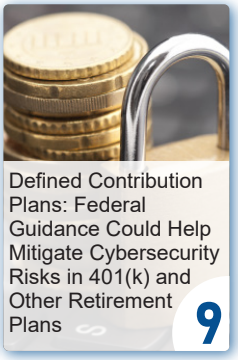

Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performar Issues 5

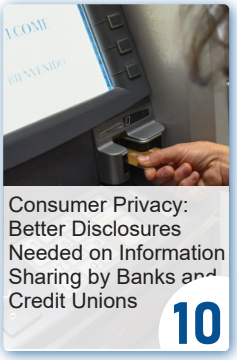
Appropriately limit the collection and use of personal information and ensure it is obtained with appropriate knowledge or consent


Medicare Telehealth: Actions Needed to Strengthen Oversight and Help Providers Educate Patients on Privacy and Security Risks 6


Privacy: Federal Financial Regulators Should Take Additional Actions to Enhance Their Protection of Personal Informati 7


Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Priv and Other Risks 8


Defined Contribution Plans: Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans 9


Consumer Privacy: Better Disclosures Needed on Information Sharing by Banks and Credit Unions 10

Source: Images: (1) VectorMine/stock.adobe.com, (2) GAO analysis of Department of Homeland Security provided data, (3) GAO, (4, 10, 9) GAO File Photo, (5) GAO, (7) GAO photo illustration; (6) insta_photos/stock.adobe.com, Andrey Popov and polkadot on stock.adobe.com, (9) Jakub Krechowicz/stock.adobe.com. | GAO-23-106443

About GAO:

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. This document is based on GAO audit products. This work of the United States may include copyrighted material, details at https://www.gao.gov/copyright.

U.S. Government Accountability Office, 441 G Street NW, Washington, DC 20548

Contact Us:

For more information about this Cybersecurity High Risk Series, contact Marisol Cruz Cain, Director, Information Technology and Cybersecurity, (202) 512-5017.

Chuck Young, Managing Director, Public Affairs, (202) 512-4800

A. Nicole Clowers, Managing Director, Congressional Relations, (202) 512-4400

Contributors: Elena Epps (Assistant Director), Keith Kim (Analyst-in-Charge), Andrea Starosciak, Ibrahim Suleman, Lauri Barnes, and Chris Businsky

Source (cover photo): GAO analysis; images: Monster Ztudio/stock.adobe.com.