

HIGH-RISK SERIES:

Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation

Report to Congressional Addressees



Why GAO Did This Study

Federal agencies and the nation's critical infrastructures depend 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 important to safeguarding individual privacy and protecting the nation's security, prosperity, and well-being.

GAO first designated information security as a government-wide High-Risk area in 1997. This was expanded to include protecting the cybersecurity of critical infrastructure in 2003 and the privacy of personally identifiable information in 2015.

In 2018, GAO reported that the federal government needed to address four major cybersecurity challenges: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting the cybersecurity of critical infrastructure, and (4) protecting privacy and sensitive data. Within these four challenges are 10 actions essential to successfully dealing with the serious cybersecurity threats facing the nation.

GAO's objective was to describe the challenges facing the federal government in ensuring the cybersecurity of the nation and the progress it has made in addressing these challenges. To do so, GAO identified its recent public reports related to each challenge and summarized relevant findings from this work. GAO also determined the implementation status of relevant recommendations made in these reports. Further, GAO identified its ongoing and upcoming work covering each of the 10 critical actions needed to address the four major cybersecurity challenges.

View [GAO-24-107231](#). For more information, contact Marisol Cain Cruz 202-512-5017, cruzcainm@gao.gov.

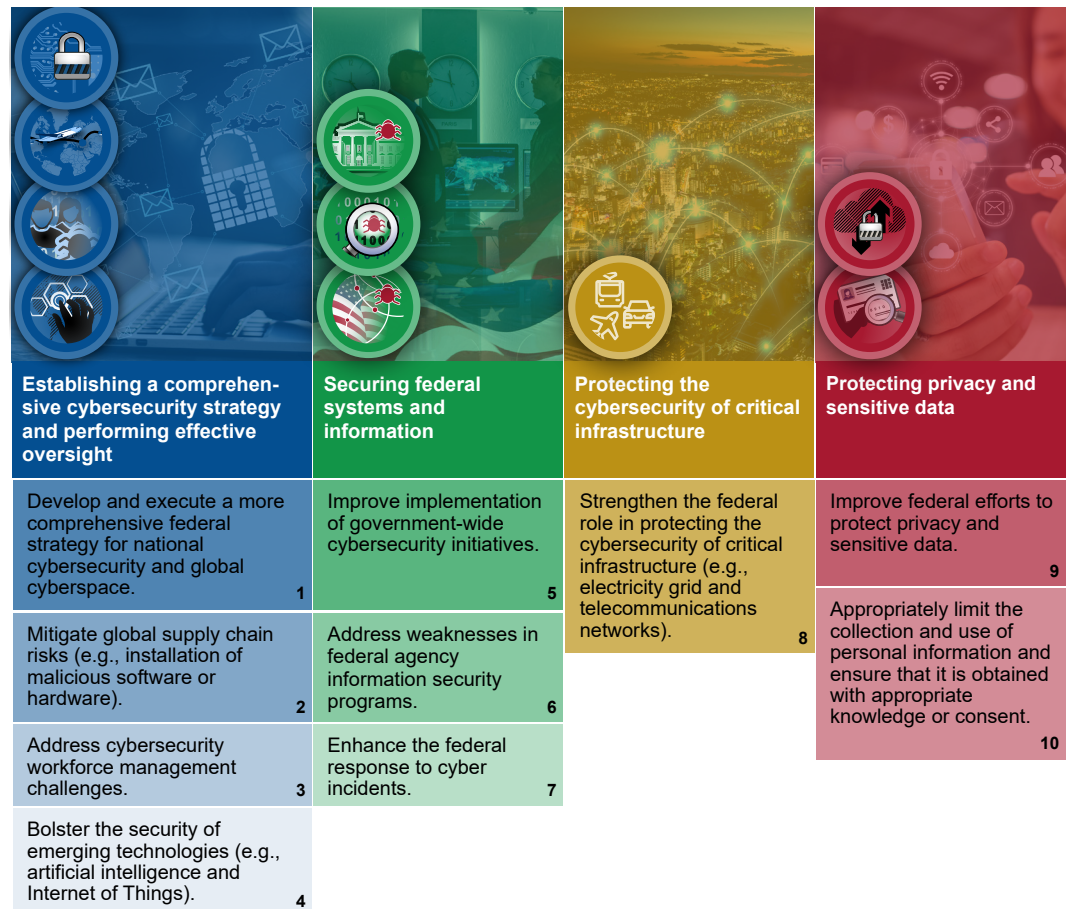
HIGH-RISK SERIES

Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation

Risks to our nation's essential technology systems are increasing. Threats to these systems can come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. Federal agencies reported 30,659 information security incidents to the Department of Homeland Security's United States Computer Emergency Readiness Team in fiscal year 2022. Such attacks could result in serious harm to human safety, national security, the environment, and the economy.

Concerted action among the federal government and its nonfederal partners is critical to mitigating the risks posted by cyber-based threats. Recognizing the growing threat, the federal government urgently needs to take action to address the four major cybersecurity challenges and 10 associated critical actions (see figure 1).

Figure 1: Four Major Cybersecurity Challenges and 10 Associated Critical Actions



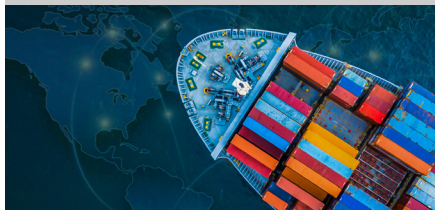
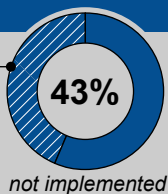
Sources: GAO (analysis and icons), Who is Danny/stock.adobe.com (blue image); Gorodenkoff/stock.adobe.com (green image); metamorworks/stock.adobe.com (yellow image); Monster Ztudio/stock.adobe.com (red image); motorama/stock.adobe.com (icons); <https://www.whitehouse.gov> (logo). | GAO-24-107231

Since 2010, GAO has made 1,610 recommendations in public reports that address the four cybersecurity challenge areas. As of May 2024, federal agencies had implemented 1,043 of these recommendations; 567 remain unimplemented. Until these recommendations are fully implemented, the federal government will be hindered in ensuring the security of federal systems and critical infrastructure and the privacy of sensitive data. This increases the risk that the nation will be unprepared to respond to the cyber threats that can cause serious damage to public safety, national security, the environment, and economic well-being.

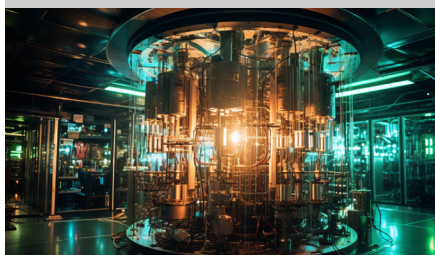
Challenge 1:

Establishing a comprehensive cybersecurity strategy and performing effective oversight

170 of 396 recommendations **have NOT** been implemented (as of May 2024)



Source: Kalyaka/stock.adobe.com. | GAO-24-107231

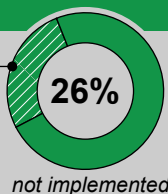


Source: Box Milk/stock.adobe.com. | GAO-24-107231

Challenge 2:

Securing federal systems and information

221 of 839 recommendations **have NOT** been implemented (as of May 2024)



Source: Justlight/stock.adobe.com. | GAO-24-107231



Source: momius/stock.adobe.com. | GAO-24-107231

View [GAO-24-107231](#). For more information, contact Marisol Cain Cruz 202-512-5017, cruzcainm@gao.gov.

The White House, through the Office of the National Cyber Director, has taken important steps in providing cybersecurity leadership, including developing and publicly releasing the *National Cybersecurity Strategy* and its accompanying implementation plan. However, in February 2024, GAO reported that the strategy and implementation plan addressed some, but not all, of the desirable characteristics of a national strategy. In particular, the strategy and implementation plan did not fully incorporate outcome-oriented performance measures and estimated resources and costs.

Additionally, the federal government needs to take actions to perform effective oversight, including monitoring the global supply chain, ensuring a highly skilled cyber workforce, and addressing risks associated with emerging technologies, such as artificial intelligence (AI). For example:

- Emerging threats in the supply chain can put federal agencies, including the Department of Defense (DOD), at risk. GAO's 2023 report showed that DOD had addressed four and partially addressed three practices for managing supply chain risk. However, DOD has not yet implemented GAO's three recommendations on the partially addressed practices.
- Regarding the cyber workforce, in July 2023 GAO reported that the National Institute of Standards and Technology (NIST) had not fully addressed nine key performance assessment practices in its efforts to strengthen cybersecurity education, training, and workforce development. GAO's recommendations to fully address these practices have not yet been implemented.
- GAO's 2023 government-wide report on AI revealed that 20 federal agencies reported a total of about 1,200 current and planned use cases—specific challenges or opportunities that AI may solve. However, many agencies had not implemented AI requirements, such as preparing an inventory on AI use. GAO made 35 recommendations to address this; however, none of these have yet been implemented.

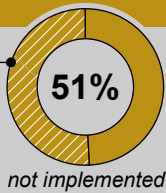
GAO has found that agencies remain limited in their ability to improve implementation of government-wide cybersecurity initiatives, address weaknesses in federal agency information security programs, and enhance the federal response to cyber incidents. For example:

- In January 2024, GAO reported that Inspectors General at 15 of the 23 civilian agencies subject to the Chief Financial Officers Act of 1990 found their agencies' information security programs to be ineffective. Out of the 23 agencies, no more than eight received an effective rating in any given year over the last 6 years of reporting (fiscal years 2017 through 2022).
- GAO's May 2023 report highlighted that four selected agencies (the Departments of Agriculture, Homeland Security, Labor, and the Treasury) varied in their efforts to implement key security practices for cloud services, which provide on-demand access to shared resources such as networks, servers, and data storage. The practices included having a plan to respond to incidents and continuous monitoring of system security and privacy. GAO made 35 recommendations to the selected agencies, most of which have not been implemented.
- In December 2023, GAO reported that 23 federal civilian agencies had made progress in cybersecurity incident response preparedness, but 20 of the 23 agencies had not fully established an event logging capability. A log is a record of the events occurring within an organization's systems and networks, and maintaining such a record is crucial for responding to incidents. GAO recommended that 19 of the 20 agencies fully implement federal event logging requirements; however, these have not yet been implemented.

Challenge 3:

Protecting the cybersecurity of critical infrastructure

64 of 126 recommendations have NOT been implemented (as of May 2024)



Source: GAO. | GAO-24-107231



Source: U.S. Air Force. | GAO-24-107231



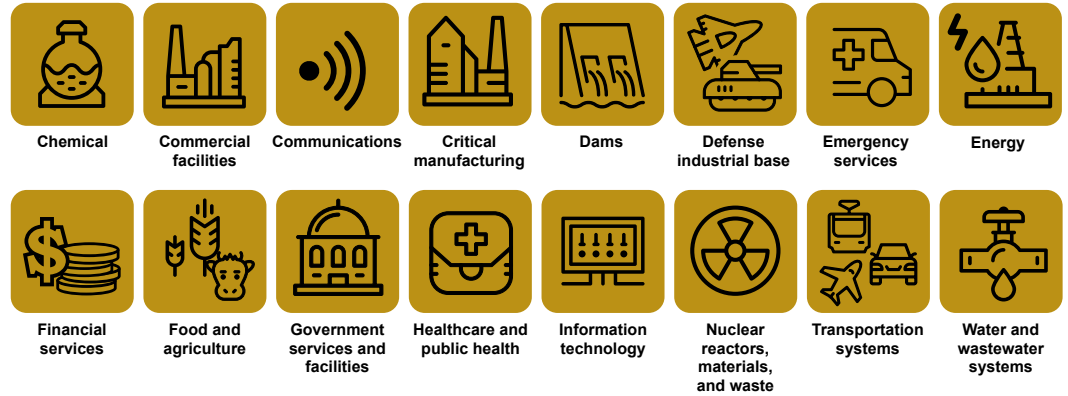
Source: National Aeronautics and Space Administration. | GAO-24-107231



Source: GAO. | GAO-24-107231

The nation's 16 critical infrastructure sectors provide the essential services that underpin American society (see figure 2).

Figure 2: The 16 Critical Infrastructure Sectors



Sources: GAO analysis of National Security Memorandum-22; motorama/stock.adobe.com (icons). | GAO-24-107231

These sectors rely on electronic systems and data to support their missions, including operational technology, which consists of systems that interact with the physical environment. Attacks on these sectors continue to grow and could result in serious harm to human safety, national security, the environment, and the economy. For example, in February 2024, a cyberattack on Change Healthcare, a health payment processor, resulting in estimated losses of \$874 million and widespread impacts on providers and patient care.

Other entities have also recognized the ongoing challenges of ensuring the cybersecurity of critical infrastructure. For example, the Cyberspace Solarium Commission has conducted studies of risks to critical infrastructure and recommended, for example, that space systems be designated as critical infrastructure.

The administration and federal agencies have taken some steps to address challenges in protecting the cybersecurity of critical infrastructure. For example, in April 2024, the White House issued the *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM-22), which describes the approach the federal government will take to protect U.S. infrastructure against threats and hazards. Among other things, the memorandum reaffirms the designation of the existing 16 critical infrastructure sectors, while calling for a periodic evaluation of changes to critical infrastructure sectors. The memorandum also requires the Secretary of Homeland Security to develop a biennial National Risk Management Plan summarizing U.S. government efforts to manage risk to the nation's critical infrastructure.

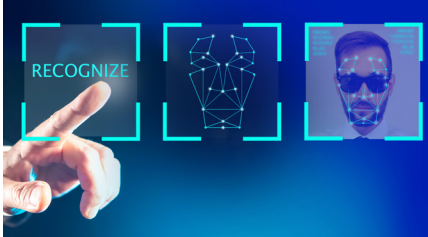
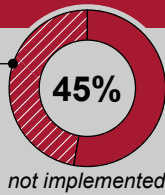
However, GAO has continued to report shortcomings in efforts to ensure the security of key critical infrastructure sectors. For example:

- In January 2024, GAO reported that the federal agencies responsible for the four critical infrastructure sectors that reported almost half of all ransomware attacks—critical manufacturing, energy, healthcare and public health, and transportation systems—had not determined the extent of their adoption of leading practices to address ransomware. GAO recommended that these agencies determine their respective sector's adoption of cybersecurity practices and assess the effectiveness of federal support. None of these recommendations have been implemented.
- GAO's March 2024 report identified challenges in collaboration between the Cybersecurity and Infrastructure Security Agency (CISA) and other federal agencies with responsibilities for mitigating cyber risks to operational technology in their sectors. The challenges were related to ineffective information sharing and a lack of sharing processes. GAO recommended that CISA take steps to address these challenges; however, the recommendations have not yet been implemented.
- In December 2023, GAO highlighted challenges identified by nonfederal entities in the healthcare sector in accessing federal support to address cybersecurity vulnerabilities in network-connected medical devices. GAO recommended that CISA and the Food and Drug Administration update existing agreements to better facilitate collaboration on these issues. However, the recommendations have not yet been implemented.

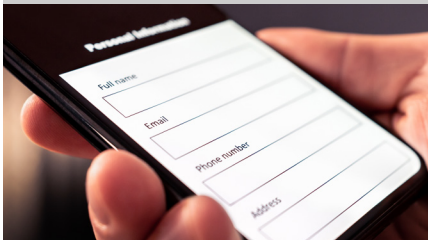
Challenge 4:

Protecting privacy and sensitive data

112 of 249 recommendations **have NOT** been implemented (as of May 2024)



Source: Grispb/stock.adobe.com. | GAO-24-107231



Source: terovesalainen/stock.adobe.com. | GAO-24-107231

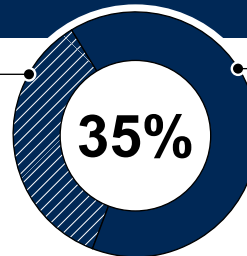
Federal government's progress in addressing GAO's recommendations for the four major cybersecurity challenges

The protection of personal privacy has become a more significant issue in recent years. It is essential that both private and public entities take effective measures to safeguard the sensitive and personal information collected from American citizens. However, incidents threatening the security of this information continue to affect private and public entities. For example, in March 2024, AT&T reported that some of its data, which included sensitive personal information such as Social Security numbers and passcodes, had been released onto the dark web. Analysis revealed that this incident had impacted 7.6 million current AT&T account holders and approximately 65.4 million former account holders.

GAO has also found that federal agencies are limited in their ability to protect private and sensitive data entrusted to them. For example:

- In August 2023, GAO reported that the Internal Revenue Service's (IRS) monitoring of efforts to prevent contractors from gaining unauthorized access to sensitive taxpayer information was limited by its incomplete inventory of systems that process or store this information. GAO recommended that IRS maintain a comprehensive inventory of its systems that process or store taxpayer information; however, the recommendation has not been implemented.
- GAO's September 2022 report highlighted the risks that the increasing collection and use of personal information pose to consumer privacy and protection. For example, companies collect personal and transactional data to create consumer scores, which businesses and other entities use to predict how consumers will behave in the future. The report further noted that there remains no comprehensive U.S. internet privacy law governing private companies' collection, use, or sale of internet users' data, leaving consumers with limited assurance that their privacy will be protected.

567 of 1,610 recommendations **have NOT** been implemented as of May 2024



GAO has made 1,610 recommendations in public reports to each of the four cybersecurity challenge areas (since 2010).

Source: GAO. | GAO-24-107231

While federal agencies have made progress in improving the security of federal and critical infrastructure IT systems, significant effort remains to address the cybersecurity challenges facing the nation. Since 2010, agencies have implemented 1,043 of the recommendations that GAO has made related to the four cybersecurity challenges. However, certain critical actions remain outstanding. For example, the federal government needs to fully establish the national cybersecurity strategy and strengthen efforts to protect the cybersecurity of critical infrastructure. Until these recommendations are fully implemented, federal agencies will be limited in their ability to:

- provide effective oversight of critical government-wide initiatives, mitigate global supply chain risks, address challenges with cybersecurity workforce management, and better ensure the security of emerging technologies;
- improve implementation of government-wide cybersecurity initiatives, address weaknesses in federal agency information security programs, and enhance the federal response to cyber incidents;
- mitigate cybersecurity risks for key critical infrastructure systems and their data; and
- protect private and sensitive data entrusted to them.

View [GAO-24-107231](#). For more information, contact Marisol Cain Cruz 202-512-5017, cruzcainm@gao.gov.

Contents

Letter		1
	Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight	6
	Challenges in Securing Federal Systems and Information	23
	Challenges in Protecting the Cybersecurity of Critical Infrastructure	39
	Challenges in Protecting Privacy and Sensitive Data	56
	Closing	74
Appendix I	Prior GAO Work	76

Tables

Table 1: Summary of Limitations Identified in Agency Artificial Intelligence (AI) Inventories	19
Table 2: Ongoing and Upcoming GAO Work Related to the Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight Challenge Area, as of May 2024	22
Table 3: Ongoing and Upcoming GAO Work Related to the Securing Federal Systems and Information Challenge Area, as of May 2024	38
Table 4: Frequency, Total Costs, and Per-Incident Costs of the Most Common Types of Cybersecurity Incidents, according to the FBI, 2016-2020 (Dollars in millions)	49
Table 5: Cybersecurity-Related Grant Award Amounts Tracked by Four Agencies, Fiscal Years 2019 through 2022	51
Table 6: Ongoing and Upcoming GAO Work Related to the Protecting the Cybersecurity of Critical Infrastructure Challenge Area, as of May 2024	55
Table 7: Extent to Which the Department of Homeland Security's Office of Intelligence and Analysis (I&A) Conducted Required Monitoring Activities to Ensure the Protection of Privacy, Civil Rights, and Civil Liberties	65
Table 8: Selected Agencies' Implementation of the Office of Management and Budget's Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act Memorandum	72
Table 9: Ongoing and Upcoming GAO Work Related to the Protecting Privacy and Sensitive Data Challenge Area, as of May 2024	73

Figures

Figure 1: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges	3
Figure 2: Extent to Which the March 2023 <i>National Cybersecurity Strategy</i> and July 2023 Implementation Plan Addressed GAO’s Desirable Characteristics of a National Strategy	9
Figure 3: The Department of State Addressed Leading Reform Practices in Establishing the Bureau of Cyberspace and Digital Policy	11
Figure 4: Assessment of the Department of Defense’s (DOD) Implementation of Selected Foundational Information and Communications Technology (ICT) Supply Chain Risk Management Practices	13
Figure 5: National Institute of Standards and Technology (NIST) Implementation of Selected Key Practices for Establishing a Program Performance Process	15
Figure 6: Scholarship Recipients Progress through Three Phases in the CyberCorps® Scholarship for Service Program	16
Figure 7: Possible Scenario of How Migration to Post-quantum Cryptography May Affect the Safety of Sensitive Information	20
Figure 8: Examples of Federal Agencies’ Views on How FISMA Metrics Should be Modified for Risk	25
Figure 9: The Cybersecurity Program Audit Guide’s Six Primary Components	26
Figure 10: Agencies’ Implementation of the Key Cloud Security Practices for Each of the Selected Systems	28
Figure 11: Examples of Selected Recommendations from Independent Assessments of the Department of Energy’s (DOE) Insider Threat Program	30
Figure 12: Examples of State’s Progress in Implementing Its Cybersecurity Risk Management Program	32
Figure 13: Department of Transportation (DOT) Mission-Oriented Operating Administrations	34
Figure 14: Examples of Tools, Services, and Resources Federal Agencies Use for Cybersecurity Incident Response	35
Figure 15: The 16 Critical Infrastructure Sectors	39
Figure 16: Treasury Reported Dollar Value of U.S. Ransomware-Related Incidents	42
Figure 17: Number of Agencies Using Each Identified Cyber Threat Information Sharing Method	44

Figure 18: Key Components of a Pipeline Operational Technology System	46
Figure 19: Example of a Compromised Medical Device That Can Lead to Disruption of Other Devices on a Hospital Network	53
Figure 20: Selected Law Enforcement Agencies' Implementation of Training Requirements to Use Facial Recognition Services, as of April 2023	59
Figure 21: Summary of Department of Homeland Security's Implementation of Selected Office of Management and Budget Privacy Requirements for the Homeland Advanced Recognition Technology (HART) Program	63
Figure 22: Utilization of Medicare Services Delivered via Telehealth or In-person, by Month, April 2019-December 2020	67
Figure 23: Key Sectors Where Consumer Scores Are Used	69

Abbreviations

AI	artificial intelligence
CASES Act	Creating Advanced Streamlined Electronic Services for Constituents Act of 2019
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CPAG	Cybersecurity Program Audit Guide
CSC	Cyberspace Solarium Commission
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
HART	Homeland Advanced Recognition Technology
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
I&A	Office of Intelligence and Analysis
ICAM	Identity, Credential, and Access Management
ICT	information and communications technology
IG	Inspector General
IRS	Internal Revenue Service
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
NSM-22	National Security Memorandum 22
OBIM	Office of Biometric Identity Management
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
OPM	Office of Personnel Management
OT	operational technology
PII	personally identifiable information
SLA	service level agreement

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.



June 13, 2024

Congressional Addressees

Federal agencies and our nation’s critical infrastructures¹—such as energy, transportation systems, communications, and financial services—depend 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 our nation’s 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. Additionally, concerted action among the federal government and its nonfederal partners is critical to mitigating the risks posed by cyber-based threats.

The *2023 Annual Threat Assessment of the U.S. Intelligence Community* and *2024 Homeland Threat Assessment* noted that multiple cyber adversaries and nation states pose a threat to our nation through targeted disruption and espionage.² Increased malicious cyber activity by these adversaries to disrupt critical infrastructure continued, with threats to many critical infrastructure sectors such as denial-of-service, website

¹The term “critical infrastructure” as defined in the Critical Infrastructures Protection Act of 2001 refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. § 5195c(e). The April 2024 White House *National Security Memorandum on Critical Infrastructure Security and Resilience* identified 16 critical infrastructures: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems. See April 2024 White House *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM-22).

²Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, D.C.: Feb. 6, 2023) and Department of Homeland Security, Office of Intelligence and Analysis, *2024 Homeland Threat Assessment*, 23-333-1A (Sept. 13, 2023).

defacement, and ransomware. With advances in artificial intelligence (AI), threat actors can carry out large-scale attacks on more victims, increasing the global cost of the average data breach 15 percent over the past 3 years to \$4.45 million.³

Recognizing the growing threat, we have designated information security as a government-wide High-Risk area since 1997.⁴ We expanded this High-Risk area in 2003 to include protecting the cybersecurity of critical infrastructure.⁵ In 2015, we expanded it again to include protecting the privacy of personally identifiable information (PII).⁶

In September 2018, we reported that the federal government needed to address four major cybersecurity challenges: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting the cybersecurity of critical infrastructure, and (4) protecting privacy and sensitive data.⁷ Within these four challenges are 10 actions critical to successfully dealing with the serious cybersecurity threats facing the nation (see figure 1).

³As we previously reported, a data breach is an unauthorized or unintentional exposure, disclosure, or loss of an organization's sensitive information. See GAO, *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). According to the Federal Bureau of Investigation, this is one of the most common and damaging types of cybersecurity incidents.

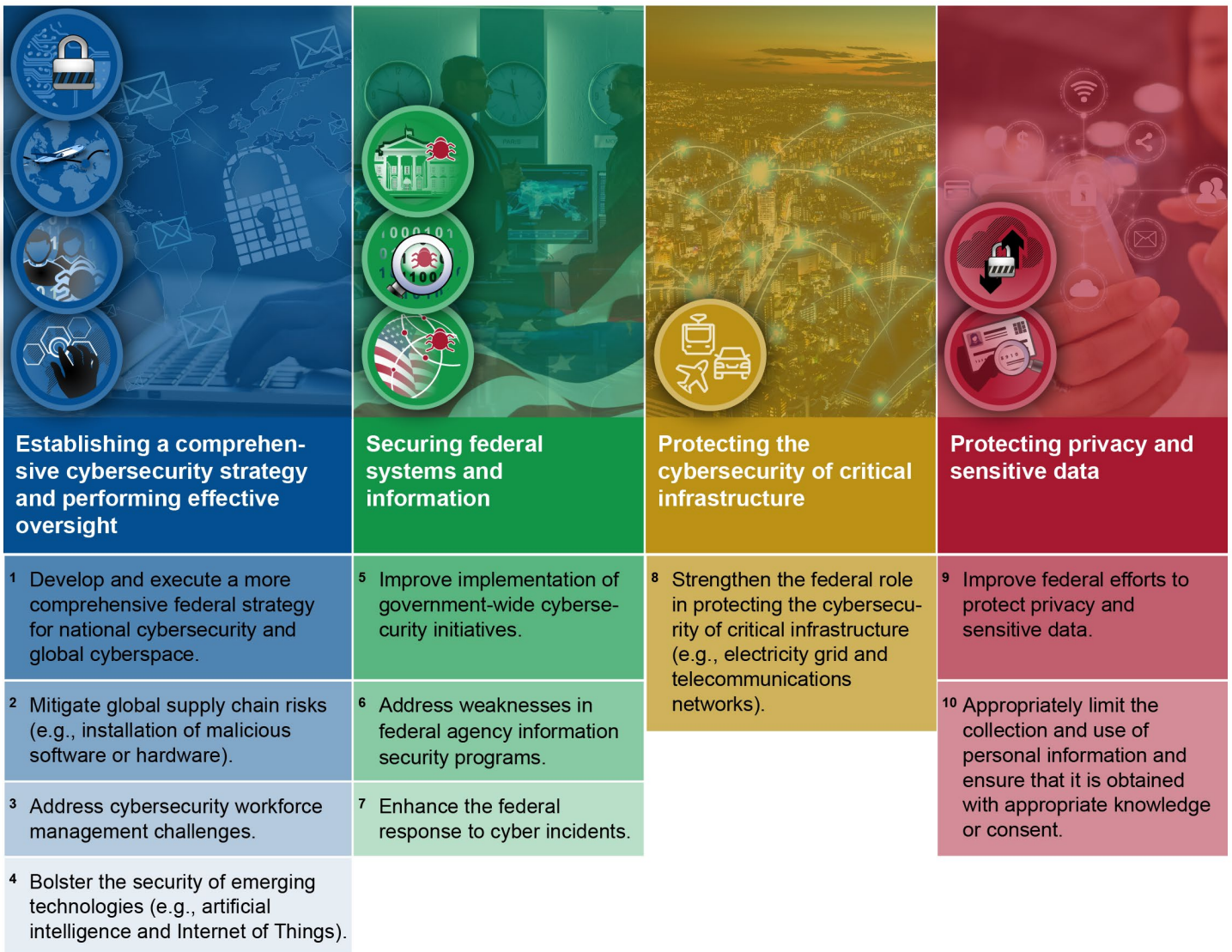
⁴For our most recent High-Risk update see GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, [GAO-23-106203](#) (Washington, D.C.: Apr. 20, 2023).

⁵See GAO, *High-Risk Series: An Update*, [GAO-03-119](#) (Washington, D.C.: Jan. 1, 2003).

⁶In 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. Also, see GAO, *High-Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: Feb. 11, 2015).

⁷GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, [GAO-18-622](#) (Washington, D.C.: Sept. 6, 2018). GAO maintains a High-Risk program to focus attention on government operations that it identifies as high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

Figure 1: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges



Sources: GAO (analysis and icons), Who is Danny/stock.adobe.com (blue image); Gorodenkoff/stock.adobe.com (green image); metamorworks/stock.adobe.com (yellow image); Monster Ztudio/stock.adobe.com (red image); motorama/stock.adobe.com (icons); <https://www.whitehouse.gov> (logo). | GAO-24-107231

Since 2010, we have made numerous recommendations to federal agencies and matters for congressional consideration related to the 10 critical actions needed to address the four major cybersecurity challenges. We have also issued products to provide an update on these

actions and challenges. For example, in a series of four short products we issued in early 2023, we provided an update on the progress the federal government had made in addressing the actions associated with the four major cybersecurity challenges.⁸ This product provides another update on the progress that the federal government has made in addressing these cybersecurity challenges and the related 10 critical actions.

We performed this work on the initiative of the Comptroller General to identify and summarize actions the government had taken to address the four major cybersecurity challenges.⁹ Specifically, our objective was to describe what challenges the federal government faces in ensuring the cybersecurity of the nation and the progress it has made in addressing these challenges.

To address our objective, we first reviewed our prior work related to each of the four challenge areas and their 10 critical actions. Using our professional judgment, we identified recent public products that aligned with each challenge area and critical action.¹⁰ We prioritized products with priority recommendations and those identified by relevant GAO staff and subject matter experts.¹¹ After selecting these products, we then summarized the findings of our prior work specific to each challenge and action. In addition, we identified our ongoing and upcoming work related to the 10 critical actions needed to address the four major cybersecurity challenges.

⁸GAO, *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); *Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure*, [GAO-23-106441](#) (Washington, D.C.: Feb. 7, 2023); and *Cybersecurity High-Risk Series: Challenges in Protecting Privacy and Sensitive Data*, [GAO-23-106443](#) (Washington, D.C.: Feb. 14, 2023).

⁹31 U.S.C. 717(b)(1).

¹⁰For this report, we excluded the products that were highlighted in the four short products we issued in early 2023.

¹¹Priority open recommendations are the GAO recommendations that warrant priority attention from heads of key departments or agencies because their implementation could save large amounts of money; improve congressional and/or executive branch decision-making on major issues; eliminate mismanagement, fraud, and abuse; or ensure that programs comply with laws and funds are legally spent, among other benefits. Since 2015 GAO has sent letters to selected agencies to highlight the importance of implementing such recommendations.

To describe overall progress, we first determined the implementation status of relevant recommendations we had made in public reports related to each challenge area since 2010. For recommendations that had not been implemented, we identified what additional actions, if any, the federal government needed to take in order to implement them.

We conducted our work from December 2023 to June 2024 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objective. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objective and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions in this product.



Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight

The federal government should:

Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace

Mitigate global supply chain risks (e.g., installation of malicious software or hardware)

Address cybersecurity workforce management challenges

Bolster the security of emerging technologies (e.g., artificial intelligence and Internet of Things)

Overview

Establishing a comprehensive cybersecurity strategy and performing effective oversight remains a critical activity to manage the challenges facing the nation. Specifically, we have previously reported that the federal government has faced challenges in establishing a comprehensive strategy to provide a framework for how the United States will engage both domestically and internationally on cybersecurity related matters.¹² We have also reported on challenges in performing oversight, including monitoring the global supply chain, ensuring a highly skilled cyber workforce, and addressing risks associated with emerging technologies.

It is essential that the federal government take action to address these challenges because cybersecurity incidents, including ones that affect the supply chain, continue to occur and pose a significant national security challenge. As an example, beginning in as early as January 2019, a threat actor breached the computing networks at SolarWinds—a Texas-based network management software company—according to the company’s Chief Executive Officer. The federal government later confirmed the threat actor to be the Russian Foreign Intelligence Service. Since the company’s software, SolarWinds Orion, was widely used in the federal government to monitor network activity and manage network devices on federal systems, this incident allowed the threat actor to breach several federal agencies’ networks that used the software. This incident resulted in one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and private sector. According to the Cybersecurity and Infrastructure Security Agency (CISA), the potential exploitation from this incident posed an unacceptable risk to federal civilian executive branch agencies because of the likelihood of vulnerabilities being exploited in the supply chain and the prevalence of affected software.¹³

Moreover, other entities have also reported on the need to address the actions associated with this challenge area. For example, in June 2022, the Cyberspace Solarium Commission (CSC) 2.0 project reported on the need to address staffing shortages in the cybersecurity workforce.¹⁴ Specifically, CSC 2.0 reported that the

¹²GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, [GAO-13-187](#) (Washington, D.C.: Feb. 14, 2013).

¹³CISA, *Mitigate SolarWinds Orion Code Compromise*, Emergency Directive 21-01 (Dec. 13, 2020).

¹⁴CSC 2.0, *Workforce Development Agenda for the National Cyber Director* (June 2, 2022). Congress created the CSC in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to “develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences.” Pub. L. No. 115-232, § 1652, 132 Stat. 1636, 2140 (2018). The commission ended when the congressional mandate ended in December 2021. However, the CSC 2.0 project was created to support continued efforts to implement outstanding CSC recommendations, provide annual assessments of the implementation of CSC recommendations, and conduct research and analysis on several outstanding cybersecurity issues identified by the CSC during its tenure.

pervasiveness of avoidable cyber problems such as misconfigured systems, slow patching, and insufficient attention to risk management can frequently be directly tied to cyber staffing shortages. Further, not only are these problems expensive to remediate after incidents occur, but they are also a threat to national security, particularly when they occur in critical infrastructure systems or in the supply chains upon which that infrastructure depends. CSC 2.0 identified recommendations to grow and strengthen the federal cyber workforce and coordinate federal support for national cyber workforce development, among other things.

In addition, the emergence of new technologies offers significant benefits but also poses challenges that must be managed by the federal government and its partners. For example, AI is a transformative technology with applications in medicine, agriculture, manufacturing, transportation, defense, and many other areas.¹⁵ It also holds substantial promise for improving government operations. However, AI systems pose unique challenges to such oversight because their inputs and operations are not always visible. Further, although concerns related to civil liberties, ethics, social disparities, and existing internal biases are not specific to AI, the use of the technology has the potential to amplify these issues.

The administration and federal agencies have taken some steps to address challenges in establishing a comprehensive cybersecurity and strategy and performing effective oversight. For example, in 2023, the White House publicly issued the *National Cybersecurity Strategy* and accompanying implementation plan that outline how the administration will manage the nation's cybersecurity.¹⁶ However, more work remains. Specifically, we have made about 396 recommendations in public reports since 2010 related to this challenge area. While federal agencies have taken steps to address 226 of these recommendations, 170 of them have not been implemented as of May 2024. Until these recommendations are fully implemented, federal agencies will be limited in their ability to provide effective oversight of critical government-wide initiatives, mitigate global supply chain risks, address challenges with cybersecurity workforce management, and better ensure the security of emerging technologies.

What actions can the federal government take to execute a more comprehensive federal cyber strategy?

The federal government needs to address missing elements in the *National Cybersecurity Strategy* and *National Cybersecurity Strategy Implementation Plan*.

Recognizing the need for national cybersecurity leadership, Congress established the Office of the National Cyber Director (ONCD) to support

¹⁵AI refers to a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action. See Exec. Order 14110, *Safe Secure, and Trustworthy Development and Use of Artificial Intelligence* (Oct. 30, 2023).

¹⁶The White House, *National Cybersecurity Strategy* (Mar. 1, 2023) and *National Cybersecurity Strategy Implementation Plan* (Washington, D.C.: July 2023).

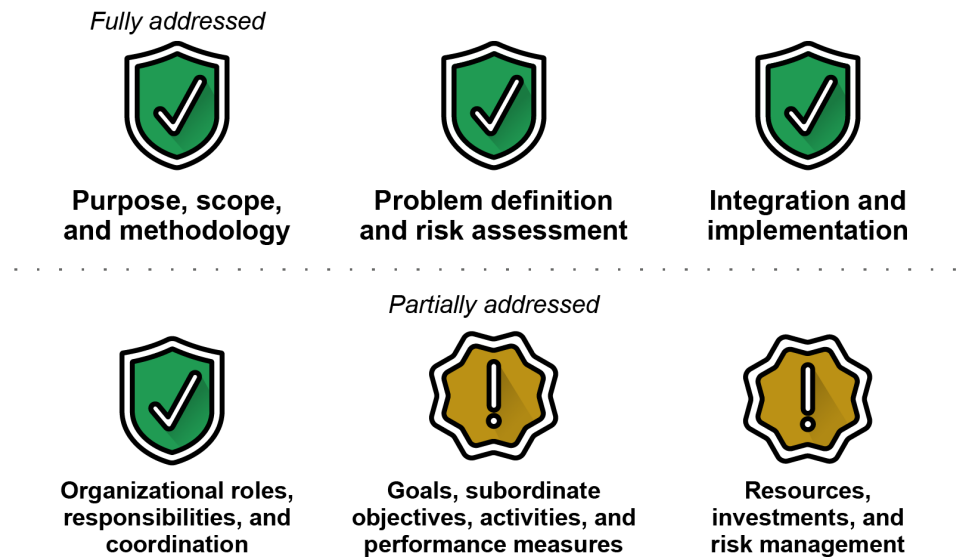
the nation's cybersecurity and lead the development of a national strategy. In March 2023, the White House publicly issued the *National Cybersecurity Strategy* that outlined how the administration will manage the nation's cybersecurity through five pillars and 27 underlying strategic objectives. In July 2023, the White House publicly issued the accompanying implementation plan that described 69 initiatives to achieve the strategy's objectives.

Fully establishing a national strategy to guide the federal government's cybersecurity activities, including its coordination with the private sector, is a critical component of the leadership commitment needed to ensure the cybersecurity of the nation. The White House, through ONCD, has taken important steps in providing this leadership, including developing and publicly releasing the *National Cybersecurity Strategy* and its accompanying implementation plan.

However, in February 2024, we reported that the strategy and implementation plan addressed some, but not all, of the desirable characteristics of a national strategy.¹⁷ Specifically, the documents jointly addressed four of six desirable characteristics, such as why the strategy was produced, the scope of its coverage, and the process by which it was developed; however, they only partially addressed the other two characteristics (see figure 2).

¹⁷GAO, *Cybersecurity: National Cyber Director Needs to Take Additional Actions to Implement an Effective Strategy*, [GAO-24-106916](#) (Washington, D.C.: Feb. 1, 2024).

Figure 2: Extent to Which the March 2023 *National Cybersecurity Strategy* and July 2023 Implementation Plan Addressed GAO’s Desirable Characteristics of a National Strategy



Sources: GAO (analysis and yellow icon); YEVHENIIA/stock.adobe.com (green icon). | GAO-24-107231

Specifically, the strategy and implementation plan did not fully incorporate outcome-oriented performance measures and estimated resources and costs. Without outcome-based performance measures, ONCD and its stakeholders will be limited in gauging the effectiveness of actions taken to implement the strategy. Further, without estimating the costs of implementing applicable initiatives, ONCD and other implementing agencies will be challenged in ensuring that adequate resources are available for those initiatives.

- **We recommended** that ONCD work with relevant federal entities to assess the initiatives to identify those that (1) lend themselves to outcome-oriented performance measures and develop such performance measures, and (2) warrant a cost estimate and develop such cost estimates. ONCD agreed with our recommendation on outcome-oriented measures but disagreed with the recommendation on estimating costs. ONCD stated that it was unable to provide details such as cost estimates for implementing any of the initiatives identified in the implementation plan. This was due to the Office of Management and Budget (OMB) guidance that restricts agencies from disclosing future year budget plans outside of the current budget

cycle, among other things. However, we identified initiatives that may require significant costs. Accordingly, we continue to believe that ONCD should assess the plan's initiatives to identify those that warrant a cost estimate and develop such cost estimates. As of May 2024, ONCD had not yet implemented either recommendation.¹⁸

The Department of State should continue to address cyberspace-related challenges.









In April 2022, State established the Bureau of Cyberspace and Digital Policy with a mission to address national security challenges, economic opportunities, and implications to U.S. values associated with cyberspace, digital technologies, and digital policy. State created this bureau to elevate cyberspace as an organizing concept for U.S. diplomacy by consolidating efforts and leadership of cyberspace-related activities into a single unit. Previously, State distributed responsibility for cyber issues between the Office of the Coordinator for Cyber Issues and other entities, according to officials.

In January 2024, we reported that, in creating the Bureau of Cyberspace and Digital Policy, the department addressed eight leading reform practices (see figure 3).¹⁹ These practices can help organizations streamline and improve the efficiency and effectiveness of their operations.

¹⁸In May 2024, the White House publicly issued the second version of the *National Cybersecurity Strategy Implementation Plan*. The updated implementation plan described 100 initiatives that are intended to achieve the objectives that are identified in the administration's *National Cybersecurity Strategy*. However, the updated implementation plan did not fully incorporate outcome-oriented performance measures and estimated resources and costs. See the White House, *National Cybersecurity Strategy Implementation Plan Version 2* (Washington, D.C.: May 2024).

¹⁹GAO, *Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities*, [GAO-24-105563](#) (Washington, D.C.: Jan. 11, 2024).

Figure 3: The Department of State Addressed Leading Reform Practices in Establishing the Bureau of Cyberspace and Digital Policy

Reform practice and questions	GAO assessment
Leadership Has the agency designated a leader or leaders to be responsible for the implementation of the proposed reforms?	 Fully addressed
Accountability How will the agency hold the leader or leaders accountable for successful implementation of the reforms?	
Implementation team Has the agency established a dedicated implementation team that has the capacity, including staffing, resources, and change management, to manage the reform process?	
Implementation plan What implementation goals and a timeline have been set to build momentum and show progress for the reforms? In other words, has the agency developed an implementation plan with key milestones and deliverables to track implementation progress?	
Employee engagement How does the agency plan to sustain and strengthen employee engagement during and after the reforms?	
Diversity How specifically is the agency planning to manage diversity and ensure an inclusive work environment in its reforms, or as it considers workforce reductions?	
Strategic workforce plan To what extent has the agency conducted strategic workforce planning to determine whether it will have the needed resources and capacity, including the skills and competencies, in place for the proposed reforms or reorganization?	
Recruitment To what extent have the reforms included important practices for effective recruitment and hiring such as customized strategies to recruit highly specialized and hard-to-fill positions?	

Sources: GAO analysis of State Department data; lovemask/stock.adobe.com (icons). | GAO-24-107231

However, the Bureau of Cyberspace and Digital Policy still faced challenges as it pursued cyber goals under the reformed structure, such as needing to clarify roles between the bureau and its partners. According to State officials, the lack of a globally agreed definition for cyber diplomacy and the diverse ways that foreign governments, multilateral actors, civil society, and the private sector organize themselves on cyber topics contributed to the challenges that they faced in identifying roles and responsibilities for some cyber issues. Bureau of Cyberspace and Digital Policy officials identified steps that they were taking to address these challenges. For example, State officials said that regular meetings and informal conversations facilitated communication between the Bureau of Cyberspace and Digital Policy and other bureaus and offices regarding these issues. Further, when multiple bureaus were involved in an issue,

officials clarified roles on an ad hoc basis. According to State officials, this approach was helping to avoid conflicts and communication breakdowns.

What actions can the federal government take to mitigate global supply chain risks?

The Department of Defense (DOD) needs to fully implement foundational practices for supply chain risk management.








Federal agencies rely extensively on information and communications technology (ICT)²⁰ products and services to carry out their operations. However, agencies face numerous ICT supply chain risks that can compromise the confidentiality, integrity, or availability of an organization's systems and the information they contain. These risks include threats posed by counterfeiters who may exploit vulnerabilities in the supply chain. Supply chain risk management is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains.

In May 2023, we reported that, while DOD had provided leadership and support for government-wide efforts to protect the ICT supply chain, the department had not fully implemented foundational practices for managing ICT supply chain risks.²¹ Specifically, DOD fully implemented four and partially implemented three of seven selected foundational practices for managing ICT supply chain risks (see figure 4).

²⁰According to the Federal Acquisition Supply Chain Security Act of 2018, ICT is information technology, information systems, and telecommunications equipment and telecommunications services. Examples of ICT products and services include printed circuit boards, cloud computing services, computing systems, software, satellite communications, and networks.

²¹GAO, *Information and Communications Technology: DOD Needs to Fully Implement Foundational Practices to Manage Supply Chain Risks*, [GAO-23-105612](#) (Washington, D.C.: May 18, 2023).

Figure 4: Assessment of the Department of Defense’s (DOD) Implementation of Selected Foundational Information and Communications Technology (ICT) Supply Chain Risk Management Practices

Practice	GAO assessment
Establish oversight of ICT risk management activities	 Fully implemented
Develop an agency-wide ICT risk management strategy	 Partially implemented
Establish an approach to identify and document agency ICT supply chain(s)	
Establish a process to conduct agency-wide assessments of ICT supply chain risks	
Establish a process to conduct a risk management review of a potential supplier	
Develop organizational ICT risk management requirements for suppliers	
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	

Sources: GAO analysis based on DOD documentation; lovemask/stock.adobe.com (icons). | GAO-24-107231

By fully implementing four of the foundational practices, DOD had taken steps to mitigate potential threats and secure its ICT supply chain. For example, the department designated responsibility for oversight and leadership of ICT supply chain risk management activities, enhancing its ability to make risk decisions across the organization. Further, DOD established an approach to identify and document its ICT supply chains, which gives critical visibility into what is happening with these supply chains.

Regarding the three partially implemented practices, the department had begun several efforts but had not committed to time frames for when the remaining practices would be implemented. For example, the department had developed a risk management strategy but had not approved guidance for implementing it. Until DOD implements these key foundational practices, it will continue to be vulnerable to malicious actors that could exploit the ICT supply chain risks to disrupt mission operations, cause harm to individuals, or steal intellectual property.

-
- **We recommended** that DOD commit to time frames for fully implementing the remaining three foundational practices in its ICT supply chain risk management efforts. DOD concurred with the three recommendations. However, as of May 2024, none of these recommendations had been implemented.

What actions can the federal government take to address cybersecurity workforce challenges?










The Department of Commerce’s National Institute of Standards and Technology (NIST) needs to better assess the performance of its National Initiative for Cybersecurity Education (NICE) program.

A well-trained cybersecurity workforce is essential for government functioning. To bolster that workforce, NIST developed the NICE program to foster more education and training through collaborative partnerships with private industry, academia, and government agencies.

In July 2023, we reported that NIST had taken several actions through the NICE program to promote and coordinate a community to strengthen cybersecurity education, training, and workforce development.²² These actions included developing an inventory of cybersecurity skills; forming public and private collaborations; and hosting webinars, forums, and conferences to share information. However, of nine selected key performance assessment practices, NIST fully implemented one, partially implemented five, and did not implement three (see figure 5).

²²GAO, *Cybersecurity Workforce: National Initiative Needs to Better Assess Its Performance*, [GAO-23-105945](#) (Washington, D.C.: July 27, 2023).

Figure 5: National Institute of Standards and Technology (NIST) Implementation of Selected Key Practices for Establishing a Program Performance Process

Practice	Implementation
Develop measurable outcome-based goals	 <i>Partially implemented</i>
Assess the program environment	
Identify strategies and resources	
Involve stakeholders	 <i>Fully implemented</i>
Develop performance measures	 <i>Not implemented</i>
Track information that is timely/accurate/useful	
Regularly communicate progress to stakeholders	
Use data to assess progress towards goals and identify any gaps	
Identify opportunities to improve program management and results	

Sources: GAO analysis of NIST information; lovemask/stock.adobe.com (icons). | GAO-24-107231

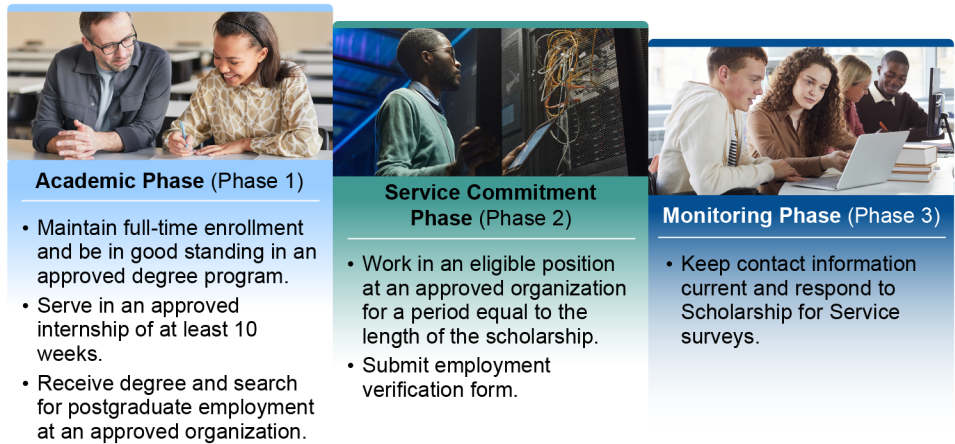
Specifically, we found that NIST lacked fully developed measurable goals and performance measures, program environment assessments and strategies, reliable information to assess and communicate progress to stakeholders, and the use of data to identify opportunities for improvement. These shortfalls hindered the ability of stakeholders, program management, agency leadership, and the public to gauge the program’s achievements.

- **We recommended** that NIST fully develop goals and performance measures, assess the program’s environment and identify strategies, track reliable information and report to stakeholders on results, and use data to assess progress and identify improvement opportunities. The Department of Commerce agreed with the recommendations. However, as of May 2024, none of these recommendations had been implemented.

The National Science Foundation (NSF) and Office of Personnel Management (OPM) need to take actions to improve the CyberCorps® Scholarship for Service Program.

We have previously reported that federal agencies faced challenges in ensuring that they have an effective cybersecurity workforce. To address this challenge, the CyberCorps® Scholarship for Service Program—which is operated by NSF in conjunction with OPM and the Department of Homeland Security (DHS)—was established in 2000 to increase the supply of new government cybersecurity employees. Specifically, the CyberCorps® Scholarship for Service Program provides participating institutions of higher education with scholarships to students in approved IT and cybersecurity fields of study. As a condition of receiving scholarships, students are required to enter agreements to work in qualifying full-time jobs upon graduation for a period equal in length to their scholarship. Figure 6 describes for how recipients progress through the program.

Figure 6: Scholarship Recipients Progress through Three Phases in the CyberCorps® Scholarship for Service Program



Sources: GAO analysis of Office of Personnel Management CyberCorps® Scholarship for Service program data; Seventy-four/stock.adobe.com (images). | GAO-24-107231

In September 2022, we reported that, of 19 selected CyberCorps® Scholarship for Service Program legal requirements, NSF and OPM fully complied with 13 requirements and partially complied with six.²³ The partially complied with requirements included the following:

- Scholarship recipients are required to provide OPM with annual verifiable documentation of post-award employment. OPM officials acknowledged that recipients provide verifiable employment documentation and up-to-date contact information only at the beginning and end of the service commitment period, rather than annually as required by law.
- NSF is required to periodically report on program performance, including how long scholarship recipients stay in the positions they enter after graduation. OPM attempted to answer this by surveying recipients. However, recipient response rates ranging from 32 to 50 percent did not yield reliable and complete results.

Until NSF and OPM ensure that they comply with all the program’s legal requirements and that the CyberCorps® Scholarship for Service Program guidance is consistently enforced, the program will be at risk of not achieving its goal of attracting and retaining high-quality graduates in the public sector cybersecurity workforce. Moreover, the program may fall short of supporting the U.S. government’s strategy to develop a superior cybersecurity workforce.

In addition, we found that NSF did not implement a risk management strategy and process to effectively identify, analyze, mitigate, and report on program risks and challenges. NSF officials stated that their approach to risk management was performed at the enterprise level. Accordingly, they did not document or track risks specific to the CyberCorps® Scholarship for Service Program. Without a risk management strategy to document risks and challenges, NSF was not in a position to mitigate the adverse effects of risk events that do occur. As a result, this could cause damage to the program.

- **We recommended** that NSF and OPM take actions to comply with the CyberCorps® Scholarship for Service Program’s legal requirements and NSF implement a risk management strategy. Both agencies agreed with our recommendations. As of May 2024, OPM

²³GAO, *Cybersecurity Workforce: Actions Needed to Improve Cybercorps Scholarship for Service Program*, [GAO-22-105187](#) (Washington, D.C.: Sept. 29, 2022).

implemented one of its two recommendations, while NSF had not yet implemented its three recommendations.

What actions can the federal government take to bolster the security of emerging technologies?

Federal agencies need to take action to improve the comprehensiveness and accuracy of their AI inventories.

AI has the potential to rapidly change the world and holds substantial promise for improving government operations. However, AI poses risks that can negatively impact individuals, groups, organizations, communities, society, and the environment. For example, according to the White House, there is extensive evidence that AI systems can produce inequitable outcomes and amplify existing inequity.²⁴ Therefore, given the rapid growth in capabilities and widespread adoption of AI, the federal government must manage its use of AI in a responsible way to minimize risk, achieve intended outcomes, and avoid unintended consequences.

In December 2023, we reported that of the 20 civilian agencies that developed AI inventories, 15 had submitted AI inventories to OMB that were not fully comprehensive and accurate.²⁵ Specifically, five of the 20 agencies provided comprehensive information for each of their reported use cases,²⁶ while the other 15 agencies' inventories had data gaps and inaccuracies. Table 1 summarizes the limitations in agencies' 2021 AI inventories that were submitted to OMB. Without accurate inventories, the government's management of its use of AI will be hindered by incomplete and inaccurate data.

²⁴The White House, *Blueprint for an AI Bill of Rights; Making Automated Systems Work for the American People* (Washington, D.C.: October 2022).

²⁵GAO, *Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements*, [GAO-24-105980](#) (Washington, D.C.: Dec. 12, 2023).

²⁶The Departments of Education and Justice, the National Science Foundation, the Office of Personnel Management, and the Social Security Administration provided comprehensive information for each of their reported use cases.

Table 1: Summary of Limitations Identified in Agency Artificial Intelligence (AI) Inventories

Agency	Had data gaps or inaccuracies	Incorrectly included research and development use cases	Included non-AI uses	Included duplicative AI uses
Department of Agriculture	X			
Department of Commerce	X	X		X
Department of Energy	X			X
Department of Health and Human Services	X	X		
Department of Homeland Security	X	X	X	
Department of the Interior	X	X		
Department of Labor	X			
Department of State	X	X	X	
Department of Transportation	X			
Department of the Treasury	X			
Department of Veterans Affairs	X			
Environmental Protection Agency	X	X		
General Services Administration	X	X		
National Aeronautics and Space Administration	X	X		X
U.S. Agency for International Development	X	X		X

Source: GAO analysis of 15 agencies' inventories where limitations were identified. | GAO-24-107231

- **We recommended** that the 15 agencies update their AI use case inventories to include required information and take steps to ensure the data aligns with federal Chief Information Officers (CIO) Council guidance, among other things. Of the 15 agencies, 10 agencies agreed with our recommendation, one agency partially agreed, and four agencies neither agreed nor disagreed. As of May 2024, none of the recommendations had been implemented.

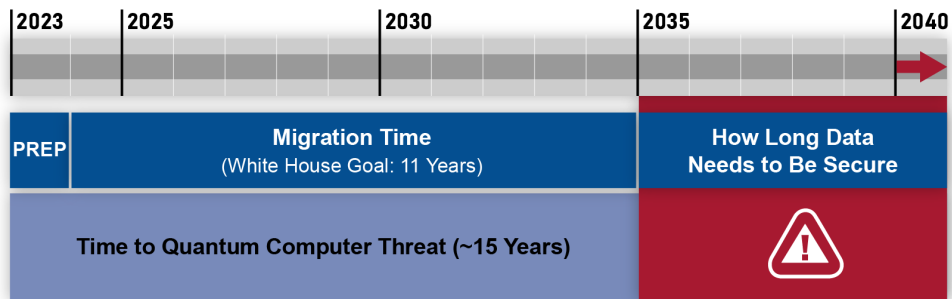
Agencies need to prepare for the risks posed by the rise of quantum computing.

We reported in March 2023 that the emergence of quantum computers offers potentially significant benefits.²⁷ These include dramatically increased processing speed compared to a classical computer, potentially solving problems that are intractable on a classical computer, with

²⁷GAO, *Science & Tech Spotlight: Securing Data for a Post-Quantum World*, GAO-23-106559 (Washington, D.C.: Mar. 8, 2023). Quantum information technologies, such as quantum computers, build on the study of quantum physics to collect, generate, and process information in ways not achievable with existing technologies.

applications in several fields. However, these computers could undermine the security of current encryption methods that protect sensitive information. In particular, the current, widely used encryption methods rely on complex mathematics that are nearly impossible for normal, or classical, computers to break in reasonable time frames. Quantum computers, in contrast, could break certain types of widely used encryption methods, such as those used for secure website connections, in exponentially shorter times because of key differences in information processing. If encryption methods able to withstand the capabilities of quantum computing are not developed and deployed soon, secure data could be decrypted as soon as the 2030s. For example, figure 7 illustrates how migration to post-quantum cryptography could affect the safety of sensitive information. The faster this migration occurs, the sooner data can be secured.

Figure 7: Possible Scenario of How Migration to Post-quantum Cryptography May Affect the Safety of Sensitive Information



⚠ Data unprotected

Source: GAO adaptation of Mosca's theorem. | GAO-24-107231

To combat this threat, researchers are developing and standardizing new encryption methods collectively referred to as postquantum cryptography. These new methods are intended to withstand attacks from both quantum and classical computers. However, even if these encryption methods are available soon, agencies face challenges in transitioning to infrastructure supportive of the new encryption methods. For example, it will likely be expensive and complex for agencies to transition to infrastructure supportive of new encryption methods. This will pose challenges to agencies in planning for costs and remaining operational during the infrastructure changeover. Nevertheless, the White House has called for federal agencies to complete the transition to postquantum cryptography

by 2035, but this may not be soon enough to keep data safe from future decryption.

What ongoing or upcoming work is GAO doing related to this challenge area?

Given the importance of addressing this challenge area, we are continuing to review and assess agencies' various cybersecurity-related initiatives in this area. It is essential that executive branch agencies continue to focus on efforts to fully establish a national cybersecurity strategy, as well as address challenges in overseeing government-wide cybersecurity initiatives, mitigating global supply chain risks, growing the cybersecurity workforce, and bolstering the security of emerging technologies. Efforts to address these challenges are critical to ensuring that the country can identify, prepare for, and respond to cyberattacks that could inflict catastrophic damage on essential systems and compromise sensitive information. Table 2 identifies our ongoing and upcoming work related to each action associated with this challenge area.

Table 2: Ongoing and Upcoming GAO Work Related to the Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight Challenge Area, as of May 2024

Critical action area	Related ongoing and upcoming GAO work
Action 1: Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.	An ongoing review of the Department of Defense’s (DOD) cyberspace operations with its allies and partners.
Action 2: Mitigate global supply chain risks.	We do not have any ongoing or upcoming work related to this action area.
Action 3: Address cybersecurity workforce management challenges.	<p>Ongoing reviews of:</p> <ul style="list-style-type: none"> • the extent to which selected agencies implemented applicable cybersecurity workforce management practices, and • identifying the size and cost of the federal cybersecurity workforce. <p>Upcoming reviews of:</p> <ul style="list-style-type: none"> • DOD’s Civilian Cybersecurity Reserve program, and • the operation and effectiveness of the Federal Rotational Cyber Workforce program.
Action 4: Bolster the security of emerging technologies.	<p>Ongoing reviews of:</p> <ul style="list-style-type: none"> • the extent to which federal agencies have analyzed and addressed the threat of quantum computing to cryptography; • technologies that enable the development of generative artificial intelligence (AI) tools and the best practices, constraints, and other factors that commercial entities consider in developing and deploying generative AI tools; • identifying the benefits and risks of the most common current and emerging uses of AI in financial services and determining how federal financial regulators use AI in their oversight activities; • the extent to which selected agencies have implemented key AI management and talent requirements; and • the extent to which selected agencies have conducted risk assessments on potential AI risks to critical infrastructure sectors in accordance with leading practices.

Source: GAO. | GAO-24-107231

Challenges in Securing Federal Systems and Information

The federal government should:

Improve implementation of government-wide cybersecurity initiatives

Address weaknesses in federal agency information security programs

Enhance the federal response to cyber incidents

Overview

Federal agencies rely extensively on computerized information systems and data and would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the safety of these systems and data is critical to public confidence and the nation's security, success, and welfare. Risks to these essential technology systems are increasing—in particular, malicious actors are becoming more willing and capable of carrying out cyberattacks. Ineffective security controls to protect these systems and data could have a significant impact on a broad array of government operations and assets.

As an example, in December 2021, a vulnerability in a piece of open-source software known as Log4j came to public attention. Log4j is used to collect and manage information about system activity and is integrated into millions of federal and private information systems. In 2013, the Log4j developers accepted a community-submitted feature called Java Naming and Directory Interface™, which was intended to make data storage and retrieval easier. In November 2021 a security engineer reported a vulnerability in the feature. The disclosure of this vulnerability prompted action to apply upgrades to the software before threat actors could exploit the systems in which Log4j was integrated, and in December 2021, CISA issued an emergency directive requiring federal agencies to mitigate the vulnerabilities. Federal agencies and other organizations spent significant resources to address the problem, which delayed other mission-critical work. Even though there have been no significant Log4j-based attacks on federal information systems, the event was assessed as an “endemic vulnerability” meaning that vulnerabilities will remain in systems for years, resulting in remaining significant risks. The Log4j event illustrated how organizations struggled to respond to the event and emphasized security risks that were specific to the volunteer-based open-source software community.

It is important for federal agencies to secure their systems because these systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising federal systems and networks. The emergence of increasingly sophisticated threats and the frequency of cyber incidents underscores the continuing and urgent need for effective information security. Threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. Federal agencies reported 30,659 information security incidents to DHS's United States Computer Emergency Readiness Team in fiscal year 2022. As an example of the impact such incidents can have, in May 2023, the Department of Transportation suffered a data breach on administrative systems potentially exposing the personal information of approximately 237,000 current and former agency employees. Such incidents highlight the need for the federal government to secure its systems and be prepared to respond to and mitigate cybersecurity incidents.

We have made about 839 recommendations in public reports since 2010 with respect to this challenge area. Federal agencies have taken steps to address 617 of these recommendations. However, as of May 2024, 221 of them have not been implemented. Until these recommendations are fully implemented, federal agencies may be limited in their ability to improve implementation of government-wide cybersecurity initiatives, address

weaknesses in federal agency information security programs, and enhance the federal response to cyber incidents.

What actions should be taken to improve the implementation of government-wide cybersecurity initiatives?

OMB should improve measures of agencies' information security programs.

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement information security programs to protect the information and systems that support the agencies' operations and assets.¹ The act also requires agency CIOs to submit FISMA reports on their information security programs to OMB, DHS, GAO, and Congress. These reports are to include the metrics to assess their progress toward outcomes intended to strengthen federal cybersecurity. In addition to the CIO FISMA reports, the act requires each agency's Inspector General (IG) or independent external auditor to perform an annual independent evaluation to determine and report on the effectiveness of its agency's information security program. OMB, in collaboration with other oversight groups, develop CIO and IG FISMA metrics that these reports are based on.

In January 2024, we reported that IGs at 15 of the 23 civilian agencies subject to the Chief Financial Officers Act of 1990 found their agencies' information security programs to be ineffective.² Out of the 23 agencies, no more than eight received an effective rating in any given year over the last 6 years of reporting (fiscal years 2017 through 2022).

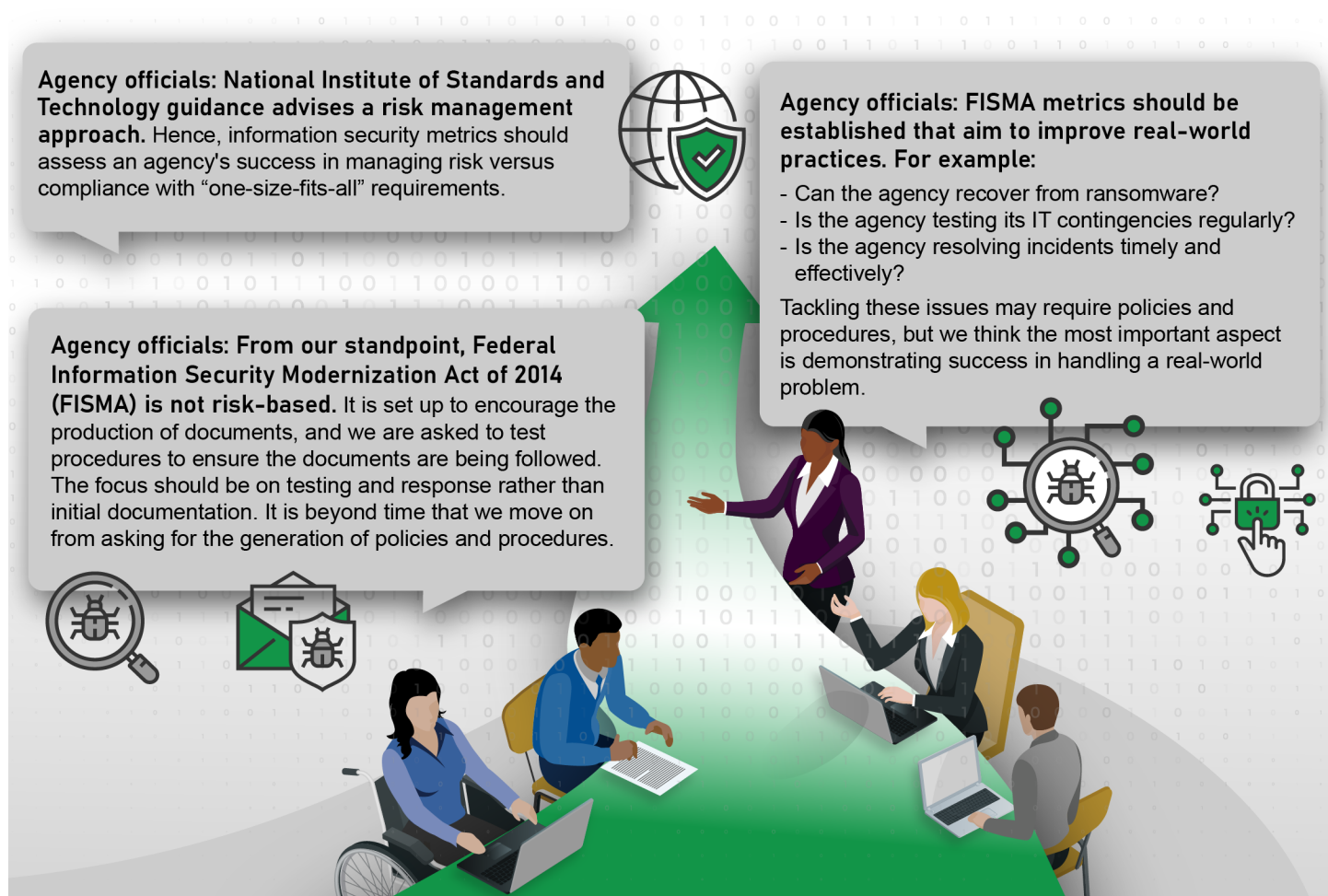
We also reported that agencies and IGs stated that some FISMA metrics were not useful because they did not always accurately evaluate information security programs. Agencies and IGs reported that metrics should be clearly tied to performance goals, account for workforce issues and agency size, and incorporate risk. Figure 8 shows examples of agencies' views on how these metrics should be modified to account for

¹The 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). FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were either incorporated or unchanged by FISMA 2014 and continue in full force and effect.

²GAO, *Cybersecurity: OMB Should Improve Information Security Performance Metrics*, [GAO-24-106291](#) (Washington, D.C.: Jan. 9, 2024).

risk. By modifying the metrics in these ways, OMB could help ensure that the measures provide an accurate picture of agencies' information security performance.

Figure 8: Examples of Federal Agencies' Views on How FISMA Metrics Should be Modified for Risk



Sources: GAO (analysis); Golden Sikorka/stock.adobe.com (people); starlineart/stock.adobe.com (background); lovemask/stock.adobe.com (icons). | GAO-24-107231

- **We recommended** that OMB collaborate with its partners to improve the FISMA metrics by clearly linking them to performance goals, address workforce challenges, consider agency size, and adequately address risk. OMB neither agreed nor disagreed with the recommendation. As of May 2024, the recommendation had not been implemented.

Agencies can use the Cybersecurity Program Audit Guide (CPAG) to help improve their cybersecurity programs and practices.

Federal cybersecurity is an urgent priority because it protects critical infrastructure, federal operations, and individuals' personal data. In September 2023, we issued the CPAG, which can help federal agencies improve the implementation of government-wide cybersecurity initiatives.³ In particular, the CPAG is to be used in conducting cybersecurity performance audits. The intent of the guide is to arm cyber analysts and auditors with a set of methodologies, techniques, and audit procedures to evaluate components of agency cybersecurity programs and systems. The CPAG has six primary components (see figure 9).

Figure 9: The Cybersecurity Program Audit Guide's Six Primary Components



Sources: GAO analysis of National Institute of Standards and Technology guidance; marinashevchenko/stock.adobe.com (icons), pixtumz88/stock.adobe.com (background). | GAO-24-107231

CPAG's six components are:

Asset and risk management: developing an understanding of the cyber risks to assets, systems, information, and operational capabilities.

Configuration management: identifying and managing security features for system hardware and software and controlling changes to the configuration.

Identity and access management: protecting computer resources from modification, loss, and disclosure by limiting authorized access.

³GAO, *Cybersecurity Program Audit Guide*, [GAO-23-104705](#) (Washington, D.C.: Sept. 28, 2023).

Continuous monitoring and logging: maintaining ongoing awareness of cybersecurity vulnerabilities and threats to an organization’s systems.

Incident response: taking action when security incidents occur.

Contingency planning and recovery: developing contingency plans and executing successful restoration of capabilities.

Each of the above components has four to seven overall key practices. For each of these practices, the CPAG provides further specificity on control objectives, applicable criteria, and available audit procedures. Although the CPAG provides suggested approaches for addressing key cybersecurity topics, it is intended to be used in a flexible manner. Depending on audit objectives and the relative importance of specific issues, organizations may adjust and fine tune audit techniques as appropriate. Use of the CPAG to guide and inform audits can help federal and nonfederal organizations improve the design and functioning of their cybersecurity programs.

What actions can be taken to address weaknesses in federal agency information security programs?

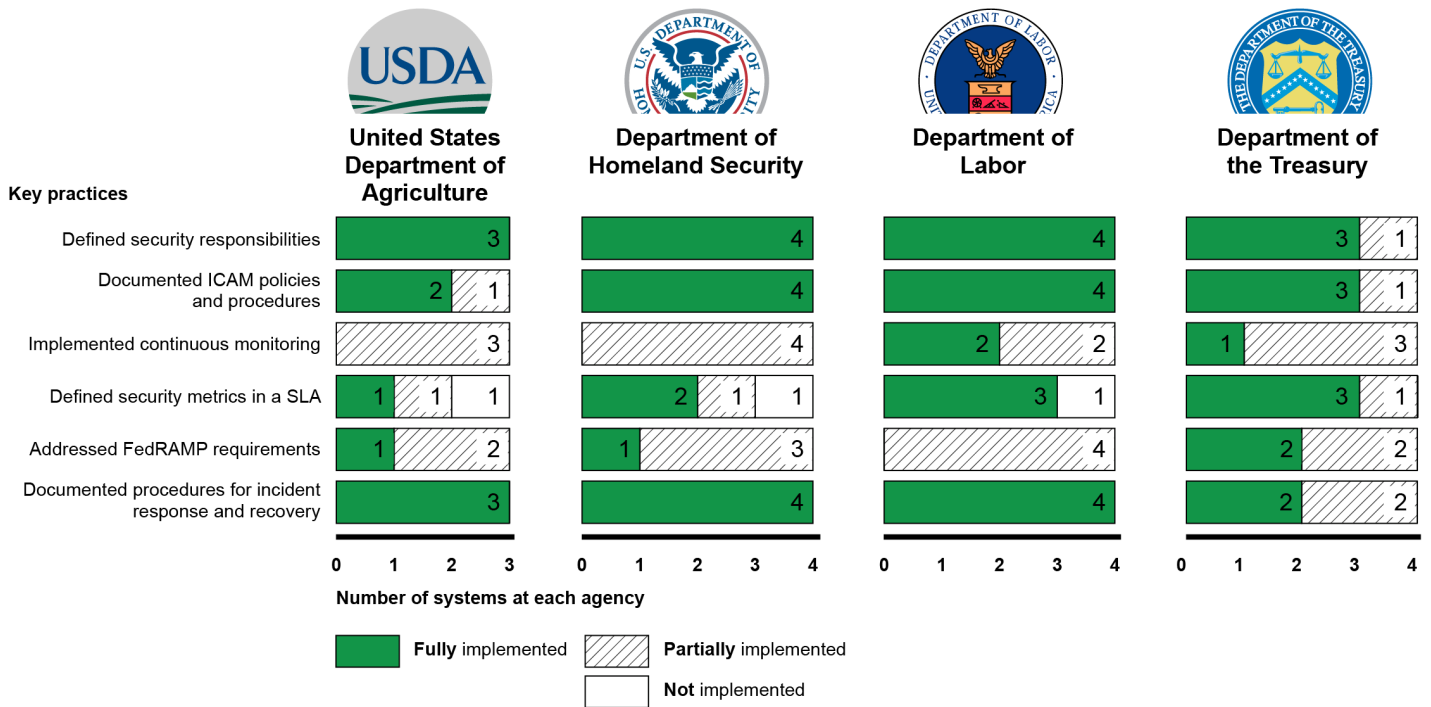
Selected agencies need to fully implement key cloud security practices.

Cloud services—on-demand access to shared resources such as networks, servers, and data storage—can help federal agencies deliver better IT services for less money. But without effective security measures, these services can make agencies vulnerable to risks such as cyberattacks.

In May 2023, we reported that four selected agencies—DHS and the Departments of Agriculture, Labor, and the Treasury—varied in their efforts to implement six key cloud security practices, such as having a plan to respond to incidents and continuous monitoring of system security and privacy posture.⁴ Specifically, three agencies fully implemented three practices for most or all of their selected systems, while another agency fully implemented four practices for most or all of its systems. However, the agencies partially implemented or did not implement the other practices for the remaining systems (see figure 10).

⁴GAO, *Cloud Security: Selected Agencies Need to Fully Implement Key Practices*, [GAO-23-105482](#) (Washington, D.C.: May 18, 2023).

Figure 10: Agencies' Implementation of the Key Cloud Security Practices for Each of the Selected Systems



ICAM = Identity, Credential, and Access Management, SLA = service level agreement, FedRAMP = Federal Risk and Authorization Management Program
 Sources: GAO analysis of agency data; agencies (logos). | GAO-24-107231

For example, the agencies fully documented security responsibilities for all but one of 15 selected systems. In addition, the agencies partially implemented the practice regarding continuous monitoring for some or all of the systems. Specifically, although the agencies developed a plan for continuous monitoring, they did not always implement their plans. In addition, agencies partially implemented or did not implement the practice regarding service level agreements for some of the systems. Specifically, agencies' service level agreements did not consistently define performance metrics, including how they would be measured and the enforcement mechanisms. Until these agencies fully implement the cloud security key practices identified in federal policies and guidance, the confidentiality, integrity, and availability of agency information contained in these cloud systems is at increased risk.

-
- **We recommended** that these four agencies fully implement key cloud security practices, which resulted in 35 recommendations. DHS concurred with the recommendations, and Agriculture, Labor, and the Treasury neither agreed nor disagreed with the recommendations. As of May 2024, two recommendations had been implemented by DHS, four by the Department of Agriculture, and five by the Department of Labor.

The Department of Energy (DOE) should take actions to fully implement its Insider Threat Program.

The theft of nuclear material and the compromise of classified information could have devastating consequences. Threats can come from external adversaries or from “insiders,” including employees or visitors with trusted access. In 2014, DOE established its Insider Threat Program to integrate its policies, procedures, and resources. The program also coordinates analysis, response, and mitigation actions among DOE organizations.

In May 2023, we reported that DOE had not implemented all required measures for its Insider Threat Program more than 8 years after it established the program in 2014, according to multiple independent assessments.⁵ Specifically, the department had not implemented seven required measures for the program, even after independent reviewers made nearly 50 findings and recommendations to help DOE fully implement its program. (See figure 11 for examples.)

⁵GAO, *Nuclear Security: DOE Should Take Actions to Fully Implement Insider Threat Program*, [GAO-23-105576](#) (Washington, D.C.: May 24, 2023).

Figure 11: Examples of Selected Recommendations from Independent Assessments of the Department of Energy’s (DOE) Insider Threat Program

Ensure insider threat awareness training completion.



Develop an implementation plan with current milestones.

Monitor all networks for suspicious user activity.



Assess program effectiveness using incident and reporting data.

Sources: GAO analysis of documents from Carnegie Mellon University, Department of Energy, the Office of the Director of National Intelligence, and National Aeronautics and Space Administration; Alwie99d/stock.adobe.com. | GAO-24-107231

We also were unable to determine the extent to which DOE had taken action on the independent reviewers’ findings and recommendations for its Insider Threat Program because the department did not formally track its actions to implement the findings and recommendations. DOE also had not submitted an annual report listing its accomplishments and goals for program improvement to the Secretary of Energy since June 2018. Without taking steps to formally track findings and recommendations from independent assessments, documenting actions it has taken to implement them, and including those actions in its annual reporting on the program, DOE cannot fully ensure that identified program deficiencies and vulnerabilities have been addressed. DOE also cannot demonstrate that it is making substantial progress toward a fully operational program capable of effectively managing insider threats.

-
- **We recommended** that DOE (1) develop a mechanism to track and report on actions it takes to address reviewers' findings and recommendations, and (2) resume annual reporting and include in those reports the actions the program has taken to address reviewers' findings and recommendations. DOE agreed with the recommendations. However, as of May 2024, neither of them had been implemented.

The Department of State needs to expeditiously implement risk management and other key practices.

The security of State's IT systems is vital to promoting an open, interoperable, and reliable information and communications infrastructure within the department. This infrastructure is also key to supporting international trade and commerce, strengthening international security, and providing consular services.

In September 2023, we reported that State had established elements of a cybersecurity risk management program, but more needed to be done to fully implement this program.⁶ Specifically, State had documented a cybersecurity risk management program that met federal requirements by identifying risk management roles and responsibilities and developing a risk management strategy. However, State had not fully implemented its program to identify and monitor risk to assets and the information maintained on its systems, as shown in figure 12.

⁶GAO, *Cybersecurity: State Needs to Expeditiously Implement Risk Management and Other Key Practices*, [GAO-23-107012](#) (Washington, D.C.: Sept. 28, 2023).

Figure 12: Examples of State’s Progress in Implementing Its Cybersecurity Risk Management Program

- ✓ Identified risk management roles and responsibilities
 - ✓ Developed a cyber risk management strategy
 - ✗ Mitigated department-wide cybersecurity risks
 - ✗ Conducted required bureau-level risk assessments
 - ✗ Completed the authorization to operate process for its 494 information systems, including high value assets (completed 44%)
 - ✗ Implemented a department-wide continuous monitoring program
- ✓ Implemented ✗ Not implemented

Sources: GAO analysis of Department of State documentation and icons. | GAO-24-107231

We noted that until the department implements required risk management activities, it lacked assurance that its security controls were operating as intended. Moreover, State was likely not fully aware of information security vulnerabilities and threats affecting mission operations.

We also found that State had taken steps to clarify and strengthen the role of the CIO in the last several years. However, the ability of State’s CIO to secure the department’s IT systems was limited due to shared management responsibilities and a lack of communication. In State’s IT structure, the CIO managed the main network and set department-wide standards, but bureaus performed many activities independently, purchasing much of their own equipment, managing many of their own IT systems, and obtaining their own funding. In addition, a lack of communication among the CIO, the Bureau of Information Resource Management,⁷ and the bureaus also hampered the CIO’s ability to secure the department’s IT systems. Until State addresses these and other deficiencies, the CIO faces challenges managing and overseeing the department’s cybersecurity program and the department’s systems remain vulnerable.

⁷The Bureau of Information Resource Management’s responsibilities include managing, overseeing, and securing the department’s IT systems and networks.

-
- **We recommended** that State develop plans to mitigate vulnerabilities that it previously identified, conduct bureau-level risk assessments for the 28 bureaus that owned information systems we reviewed, ensure that its information systems have valid authorizations to operate in accordance with department policies and federal guidance, and ensure that the CIO has access to assets at bureaus and posts to continuously monitor for threats and vulnerabilities that may affect mission operations, among other things. State agreed with our recommendations. However, as of May 2024, none of the recommendations had been implemented.

The Department of Transportation (DOT) needs to take steps to improve its oversight of components' cybersecurity activities and managers.

DOT was established in part to build, maintain, and oversee a vast national transportation system. To support its mission, the department relies on information systems to secure sensitive information.

In May 2023, we reported that DOT had established cybersecurity roles and responsibilities, but gaps existed in its oversight of components' cybersecurity.⁸ Specifically, DOT policy documented cybersecurity roles and responsibilities for senior IT officials. Further, departmental policy also described roles and responsibilities for senior managers at the nine component operating administrations (figure 13 depicts these nine operating administrations).

⁸GAO, *Cybersecurity: DOT Defined Roles and Responsibilities, but Additional Oversight Needed*, [GAO-23-106031](#) (Washington, D.C.: May 15, 2023).

Figure 13: Department of Transportation (DOT) Mission-Oriented Operating Administrations



Sources: DOT; ipopba/stock.adobe.com and EvrenKalinbacak/stock.adobe.com (images); davooda/stock.adobe.com (icons). | GAO-24-107231

With regard to providing oversight, DOT policy required annual reviews of component agency cybersecurity programs. However, the reviews had not been effective in taking needed actions to implement the 63 unresolved cybersecurity recommendations as reported by the department's IG in a September 2022 report. Using the reviews to address the recommendations could improve the department's cybersecurity program.

To assess managers' performance, DOT established performance plans for its component agency senior IT managers. However, while DOT's strategic plan identified cybersecurity as an organizational objective, 15 of 18 managers' performance plans did not include cybersecurity-related expectations. Further, the department CIO did not always participate in evaluating the performance of component agency CIOs. This was inconsistent with department regulations and resulted in less assurance that component agencies were aligned with the department in carrying out cybersecurity-related responsibilities.

- **We recommended** that DOT use annual reviews to address prior IG cybersecurity recommendations in areas such as training, ensure that senior managers' performance plans include cybersecurity-related expectations, and ensure that the DOT CIO be involved in evaluating component CIOs' performance. DOT concurred with the

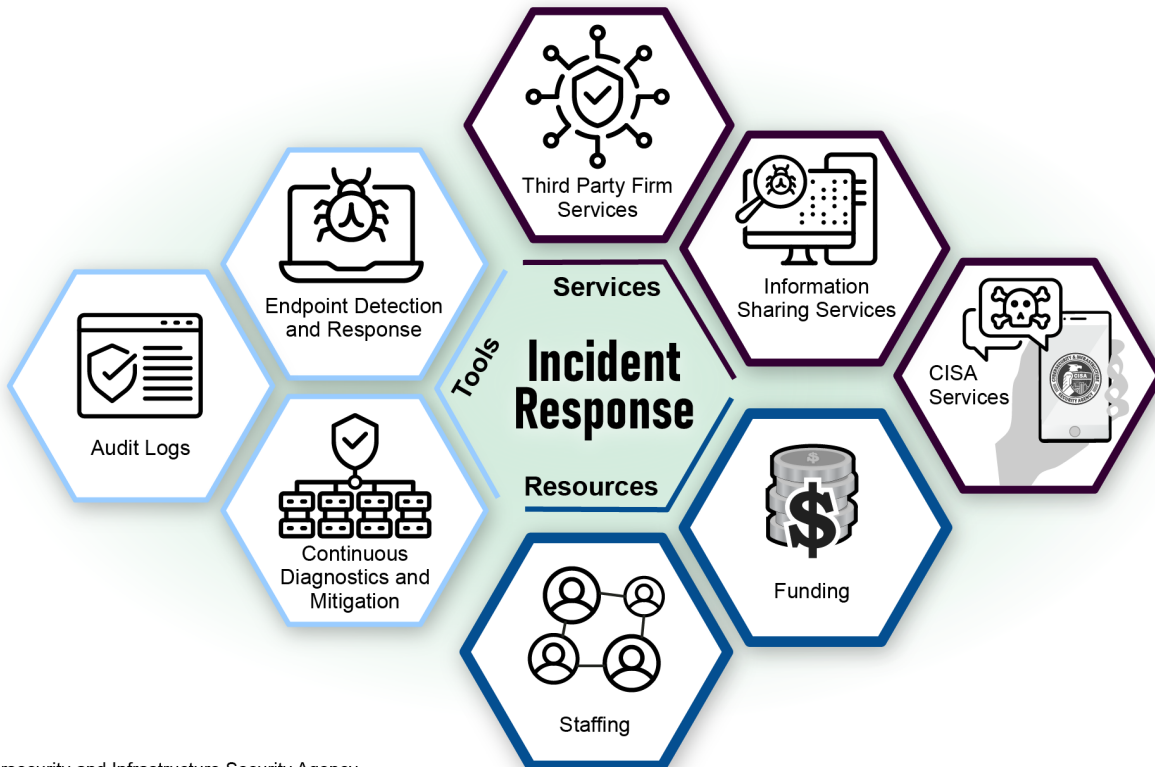
recommendations. However, as of May 2024, none of the recommendations had been implemented.

What actions can be taken to enhance the federal response to cyber incidents targeting federal systems?

Federal agencies need to fully implement incident response requirements.

Cyber-based attacks on federal systems have become more damaging and disruptive. Figure 14 depicts some of the tools, resources, and services that federal agencies rely upon for cybersecurity incident response.

Figure 14: Examples of Tools, Services, and Resources Federal Agencies Use for Cybersecurity Incident Response



CISA = Cybersecurity and Infrastructure Security Agency

Sources: GAO (hand/phone, money); Gofficon/stock.adobe.com (all other icons). | GAO-24-107231

Protecting the information systems and the information that resides on them and effectively responding to a cyber incident are important to federal agencies. This is because the unauthorized disclosure, alteration, and destruction of the information on those systems can result in great harm to those involved.

In December 2023, we reported that 23 federal civilian agencies had made progress in cybersecurity incident response preparedness by taking steps to standardize their incident response plans and demonstrating improvement in their capabilities for incident detection, analysis, and handling.⁹ However, 20 of the 23 agencies had not fully met the requirements for establishing an event logging capability.¹⁰ Until agencies implement all event logging requirements, the federal government's ability to fully detect, investigate, and remediate cyber threats will be constrained.

Agencies described three key challenges that hindered their abilities to fully prepare to respond to cybersecurity incidents: (1) lack of staff, (2) event logging technical challenges, and (3) limitations in cyber threat information sharing. Federal entities had ongoing efforts that can assist in addressing these challenges. These efforts included onsite cyber incident response assistance from CISA, event logging workshops and guidance, and enhancements to a cyber threat information sharing platform. In addition, there were long-term efforts planned, such as implementation of the National Workforce and Education Strategy and a new threat intelligence platform offering from CISA, targeted to roll out its first phase to federal departments and agencies in fiscal year 2024.¹¹

⁹GAO, *Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements*, [GAO-24-105658](#) (Washington, D.C.: Dec. 4, 2023). The 23 civilian agencies are the Departments of Agriculture, Commerce, 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 the U.S. Agency for International Development.

¹⁰A log is a record of the events occurring within an organization's systems and networks.

¹¹Office of the National Cyber Director Executive Office of the President, *National Cyber Workforce and Education Strategy: Unleashing America's Cyber Talent* (Washington, D.C.: July 31, 2023).

-
- **We recommended** that 19 of the 20 agencies who had not fully met the requirements for establishing an event logging capability should fully implement all event logging requirements as directed by OMB guidance.¹² Sixteen agencies agreed with the recommendations and three neither agreed nor disagreed. As of May 2024, none of the recommendations had been implemented.

What ongoing or upcoming work is GAO doing related to this challenge area?

Given the importance of addressing this challenge, we are continuing to review and assess agencies' various cybersecurity-related initiatives in this area. It is essential that executive branch agencies continue to focus on efforts to address challenges in improving implementation of government-wide cybersecurity initiatives, address weaknesses in federal agency information security programs, and enhance the federal response to cyber incidents targeting federal systems. Efforts to address these challenges are critical to ensuring the government is prepared to respond to and mitigate cybersecurity incidents and threats to their systems. Table 3 identifies our ongoing and upcoming work related to each action associated with this challenge area.

¹²The 19 agencies were the Departments of Commerce, 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; Nuclear Regulatory Commission; Office of Personnel Management; Social Security Administration; and the U.S. Agency for International Development. The 20th agency, the U.S. Agency for International Development, informed us that in September 2023, its Office of Inspector General had issued the same recommendation on event logging which the agency stated it planned to address. We reviewed the agency's Office of Inspector General recommendation and determined that it met the same intent as our recommendation. As such, we did not make the same recommendation.

Table 3: Ongoing and Upcoming GAO Work Related to the Securing Federal Systems and Information Challenge Area, as of May 2024

Critical action area	Related ongoing and upcoming GAO work
Action 5: Improve implementation of government-wide cybersecurity initiatives.	<p>Ongoing reviews of:</p> <ul style="list-style-type: none"> • the extent to which the administration has developed a comprehensive national strategy for addressing the threat of quantum computing and whether federal agencies have analyzed and addressed the threat of quantum computing to cryptography, • the leading practices in the private sector for adopting and implementing cloud computing services, and the successes and potential challenges in the adoption and implementation of cloud computing services, and • the extent to which the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation program (a government-wide initiative) is meeting its goals and if there are opportunities to strengthen the program.
Action 6: Address weaknesses in federal agency information security programs.	<p>Ongoing reviews of:</p> <ul style="list-style-type: none"> • the effectiveness of the Department of Veterans Affairs' information security program and information security management system; • the extent to which selected Department of Defense (DOD) IT business programs performed and to what extent has DOD implemented key software development and cybersecurity practices for selected programs; • the extent to which the Federal Aviation Administration has ongoing projects to modernize its legacy systems, including many that are over 20 years old, which can lead to cybersecurity concerns; • the extent to which DHS's Human Resources Information Technology investment incorporates key portfolio management practices; • the extent to which the National Institutes of Health has controls in place to ensure its systems used to process grant-related data can effectively protect against and detect unauthorized access and data manipulation; • the extent to which DOD's Counterintelligence and Security Agency planned for cybersecurity controls of the National Background Investigation Services system and the system's operation of the legacy background investigation systems, among other things; • the extent to which Login.gov collects, shares, and protects personally identifiable information while providing identity proofing services; • the extent to which have agencies addressed OMB's requirements for using the "Internet of Things"^a cybersecurity waivers; • the extent to which the National Aeronautics and Space Administration has protected mission systems by ensuring cybersecurity controls are effectively implemented for selected mission critical systems at its centers; and • the extent to which DOD has implemented an effective insider threat program to protect classified information.
Action 7: Enhance the federal response to cyber incidents targeting federal systems.	<p>An ongoing review of the extent to which the Department of Health and Human Services implemented effective incident response capabilities involving possible advanced persistent threats.</p>

Source: GAO. | GAO-24-107231

^aThe "Internet of Things" generally refers to the technologies and devices that allow for the network connection and interaction of a wide array of "things," throughout such places as buildings, transportation infrastructure, or homes.

Challenges in Protecting the Cybersecurity of Critical Infrastructure

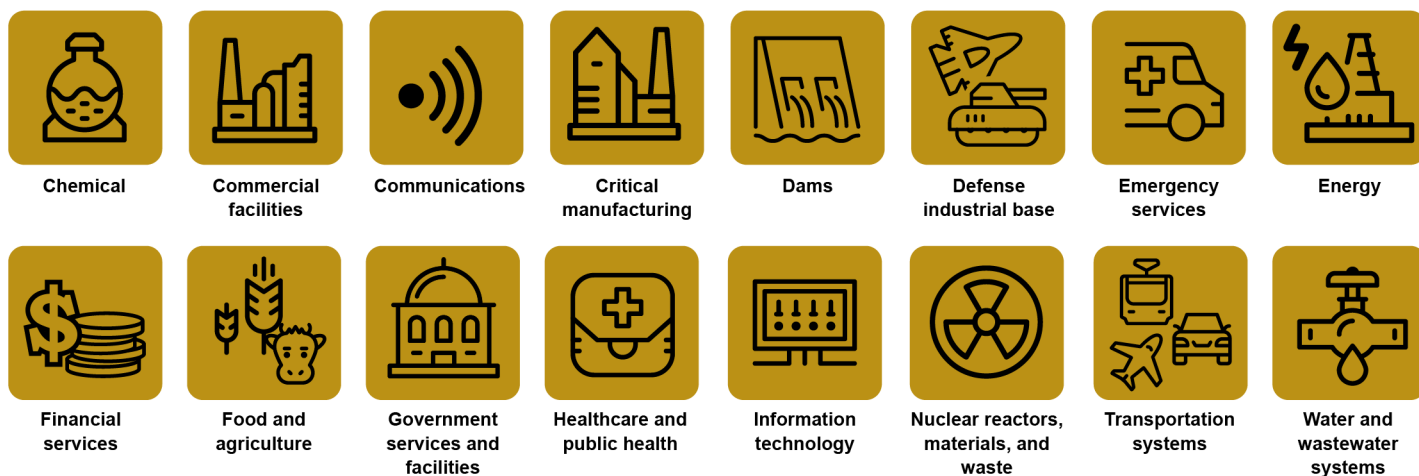
The federal government should:

Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks)

Overview

The nation's 16 critical infrastructure sectors provide the essential services that underpin American society (see figure 15). These sectors rely on electronic systems and data to support their missions. Further, much of the nation's critical infrastructure relies on operational technology (OT)—systems that interact with the physical environment—to provide essential services, like controlling distribution processes and production systems.

Figure 15: The 16 Critical Infrastructure Sectors



Sources: GAO analysis of National Security Memorandum-22; motorama/stock.adobe.com (icons). | GAO-24-107231

However, cyber threats to critical infrastructure continue to increase and represent a significant national security challenge. The nation's pipelines are one example of critical infrastructure vulnerable to cyberattacks due to increased reliance on computerized systems. In May 2021, the Colonial Pipeline Company learned that it was a victim of a cyberattack, and malicious actors reportedly deployed ransomware against the pipeline company's business systems. To prevent further compromise, the company temporarily halted all pipeline operations, leading to gasoline shortages throughout the southeast United States.

In addition to pipelines, other critical infrastructure sectors have also experienced malicious cyber incidents. In December 2023, the Federal Bureau of Investigation (FBI), CISA, and HHS released a joint cybersecurity

advisory on ransomware attacks targeting the healthcare sector.¹³ Further, starting in February 2024, Change Healthcare, a health payment processor, was the target of a cyberattack and had to shut down operations, resulting in estimated losses of \$874 million. Healthcare organizations lost revenue and were unable to submit claims or verify eligibility for benefits. Not only did the attack have devastating financial consequences, but patient care was impacted, with problems such as delayed procedures and patients being unable to access medication.

In light of the increasing and evolving threats to critical infrastructure, CISA, in consultation with sector risk management agencies and other federal interagency partners, initiated a review of the current framework for securing critical infrastructure.¹⁴ Review findings suggested that CISA should evaluate the scope of critical infrastructure sectors in collaboration with ONCD, the National Security Council, and the sector risk management agencies. The review noted they should consider new sectors in line with established criteria such as whether the addition covers a logical collection of assets, provides a common function to society, or disruptions to it would be debilitating. The review also recommended the evaluation of both a Space and Bioeconomy sector.¹⁵

In addition to the review above, the CSC 2.0 project also assessed critical infrastructure sectors and released an April 2023 report recommending Space Systems become a designated critical infrastructure sector.¹⁶ The United States relies on space systems (e.g., satellites and command and control centers) for key national security and economic operations, such as military intelligence, satellites for industrial control systems, financial services, telecommunications, and global positioning. The commission stated that the \$469 billion industry will only continue to grow and is at risk of disruption from other nation-states. The report outlined an approach consistent with the criteria and findings of the earlier CISA review, defining the sector scope, functions, and impact.

The administration and federal agencies have taken some steps to address challenges in protecting the cybersecurity of critical infrastructure. For example, in April 2024, the White House issued the *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM-22) that describes a comprehensive

¹³Cybersecurity and Infrastructure Security Agency, Department of Health and Human Services, and Federal Bureau of Investigation, Joint Cybersecurity Advisory: *#StopRansomware: ALPHV Blackcat*, AA23-353A (Dec. 19, 2023).

¹⁴Sector risk management agencies are responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. 6 U.S.C. § 651(5). See The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*, National Security Memorandum 22 (Washington, D.C.: Apr. 30, 2024).

¹⁵Cybersecurity and Infrastructure Security Agency, *FY 2021 National Defense Authorization Act – Section 9002(b) Report* (Nov. 12, 2021).

¹⁶CSC 2.0, *Time to Designate Space Systems as Critical Infrastructure* (April 14, 2023).

effort the federal government intends to take to protect U.S. infrastructure against threats and hazards.¹⁷ Further, NSM-22 requires the Secretary of Homeland Security to submit to the President a biennial National Risk Management Plan (referred to as the *National Plan*) that summarizes federal efforts to manage risk to the nation's critical infrastructure.¹⁸ The memorandum reaffirms the designation of the existing 16 critical infrastructure sectors, while calling for a periodic evaluation of changes to critical infrastructure sectors.

However, more work remains. We have made 126 recommendations in public reports since 2010 in this challenge area. While federal agencies have taken steps to implement 62 of these recommendations, 64 of them have not been implemented as of May 2024. Until these recommendations are fully implemented, key critical infrastructures will continue to have increased cybersecurity risks to their systems and data.

What actions should be taken to strengthen the federal role in protecting the cybersecurity of critical infrastructure?

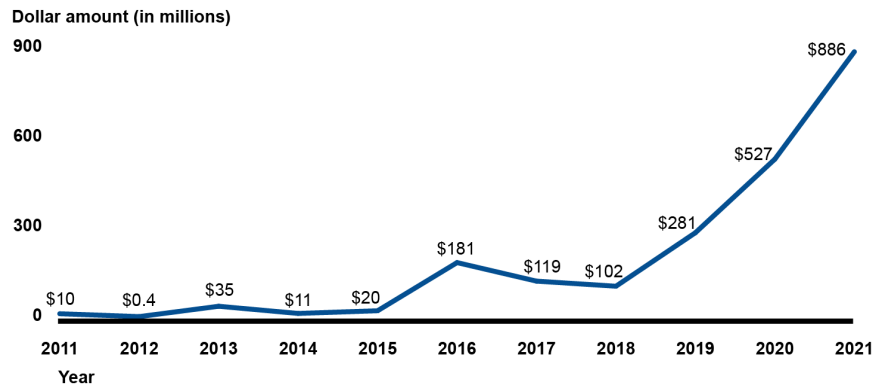
Agencies should enhance oversight of ransomware practices and assess the effectiveness of federal support designed to reduce ransomware risk.

Ransomware—a form of malicious software designed to encrypt files on a device, rendering any data and systems that rely on them unusable unless ransom payments are made—is having increasingly devastating impacts on the nation's critical infrastructure. For example, the Department of the Treasury reported that the total value of U.S. ransomware-related incidents reached \$886 million in 2021, a 68 percent increase compared to 2020 (see figure 16).

¹⁷The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*, National Security Memorandum 22 (Washington, D.C.: Apr. 30, 2024). This memorandum rescinds and replaces the White House's Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience* dated February 12, 2013.

¹⁸The Secretary of Homeland Security is required to submit the first National Plan by April 30, 2025, and on a recurring basis every 2 years thereafter by June 30 of each year.

Figure 16: Treasury Reported Dollar Value of U.S. Ransomware-Related Incidents



Source: GAO analysis of Department of the Treasury data. | GAO-24-107231

We reported in January 2024 that the four critical infrastructure sectors that reported almost half of all ransomware attacks—critical manufacturing, energy, healthcare and public health, and transportation systems—had not determined the extent of their adoption of leading practices to address ransomware.¹⁹ Specifically, none of the federal agencies designated as the lead for risk management for these sectors—DHS, Department of Health and Human Services (HHS), DOE, and DOT—had determined the extent of adoption of NIST’s recommended practices for addressing ransomware. Most of the selected agencies had assessed or planned to assess risks of cybersecurity threats like ransomware for their respective sectors, as required by law.²⁰ However, while half of the agencies had evaluated some aspects of their support of sector efforts to address ransomware, none had fully assessed the effectiveness of their support. Fully assessing effectiveness could help address sector concerns about agency communication, coordination, and timely sharing of threat and incident information.

¹⁹GAO, *Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support*, [GAO-24-106221](#) (Washington, D.C.: Jan. 30, 2024).

²⁰William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283 § 9002(c)(1), 134 Stat. 3388, 4770 (Jan. 1, 2021), codified at 6 U.S.C. § 665d.

-
- **We recommended** that the four agencies in our review determine the extent of their sector’s adoption of cybersecurity practices and assess the effectiveness of federal support in reducing risk of ransomware to their sectors. DHS and HHS agreed with their associated recommendations, while DOE and DOT agreed with some but not others. We continue to believe that all 11 recommendations are valid. As of May 2024, none of the recommendations had been implemented.

The federal government should take steps to resolve long-standing cyber threat information-sharing challenges.

As cyber threats to critical infrastructure become more complex, it is increasingly important that federal agencies and critical infrastructure owners and operators share cyber threat information. Key federal entities, such as ONCD, CISA, and sector risk management agencies, lead federal efforts to coordinate on national cyber policy and security of critical infrastructure and provide specialized expertise for their sectors, including the sharing of cyber threat information. Long-standing challenges, such as security concerns and timeliness, make sharing cyber threat information harder.

In September 2023, we reported that 14 of the federal agencies in our review—the FBI and 13 sector risk management agencies (including CISA)—relied on 11 methods to share cyber threat information with critical infrastructure owners and operators.²¹ These agencies used each of the 11 methods to varying degrees. Figure 17 shows the number of the 14 agencies that used each method.

²¹GAO, *Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods*, [GAO-23-105468](#) (Washington, D.C.: Sept. 26, 2023). For this review, we selected the FBI, seven of the nine sector risk management agencies, and six components from the remaining two sector risk management agencies. The sector risk management agencies were the Departments of Agriculture, Defense, Energy, Transportation, and the Treasury; the Environmental Protection Agency; and the General Services Administration. The six components we chose from the remaining two sector risk management agencies were the Department of Health and Human Services’ Food and Drug Administration and Administration for Strategic Preparedness and Response; and the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency, Federal Protective Service, Transportation Security Administration, and U.S. Coast Guard.

Figure 17: Number of Agencies Using Each Identified Cyber Threat Information Sharing Method



Source: GAO analysis of cyber threat sharing methods, and images/icons. | GAO-24-107231

Approaches also differed, with CISA and FBI favoring a centralized approach to sharing information with all 16 critical infrastructure sectors and the other 12 sector risk management agencies sharing only sector-specific information. We also reported that 13 of the 14 federal agencies stated that they had taken initial actions to address challenges associated

with cyber threat sharing, but 14 agencies also acknowledged that these challenges had not been fully resolved.

In March and July 2023, the White House issued its *National Cybersecurity Strategy* and accompanying implementation plan to target cybersecurity challenges, which included eight initiatives related to sharing threat information. For example, the implementation plan included an initiative that calls for CISA to assess whether new or improved sharing methods were needed. However, the strategy and implementation plan did not address outcome-orientated performance measures for these initiatives and did not call for CISA to assess whether the existing sharing methods should be retired in favor of either centralized or sector-specific approaches. Until ONCD and CISA resolve these weaknesses, the long-standing cyber threat sharing challenges will likely persist.

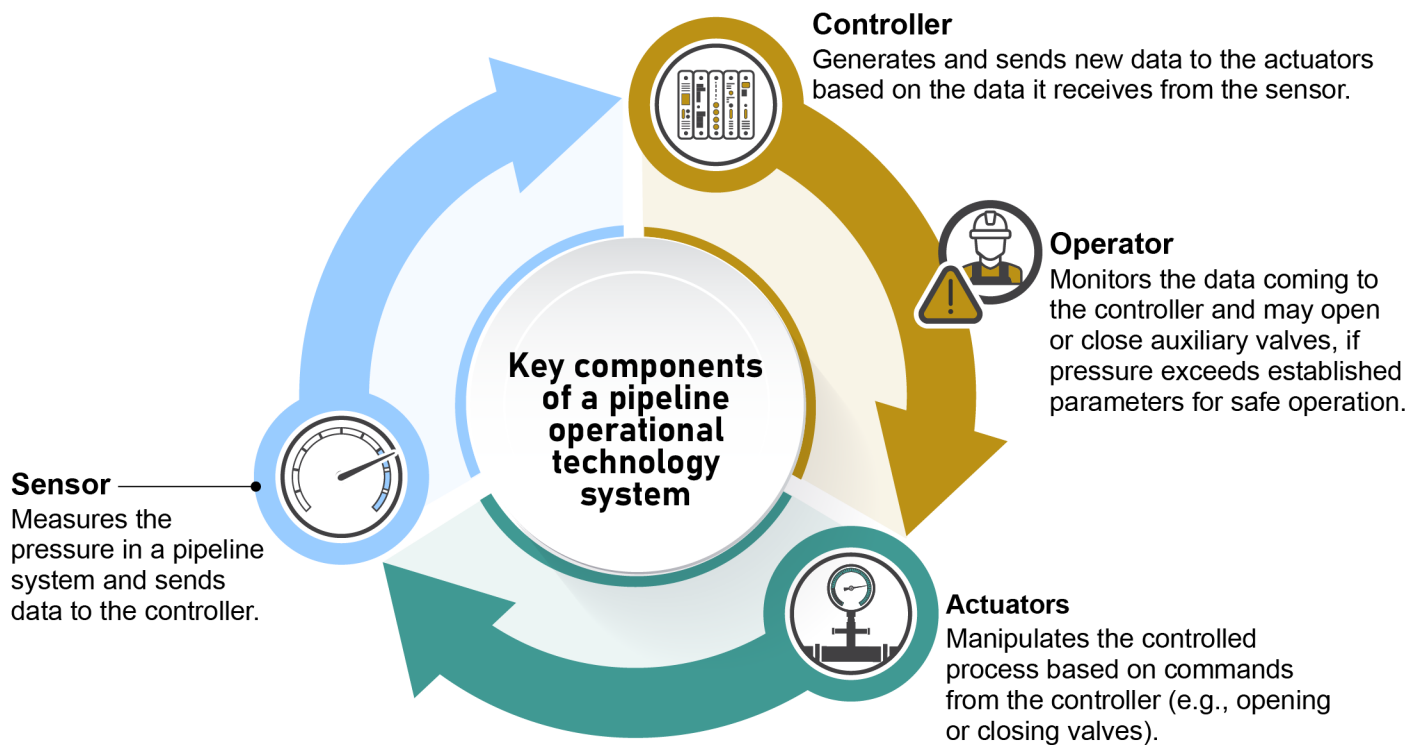
- **We recommended** that ONCD identify outcome-orientated performance measures for cyber threat sharing initiatives included in the *National Cybersecurity Strategy*, and that CISA assess whether the current mix of centralized and sector-specific sharing methods is the optimal approach. CISA agreed with its recommendation; however, ONCD did not. ONCD stated that that it was premature for the plan to include outcome-oriented measures and that without additional research, ONCD would be severely limited in its ability to identify and develop effective metrics for the plan. However, we believe that it is feasible for ONCD to develop outcome-oriented measures to help ensure that ongoing implementation of the eight information-sharing-related initiatives are achieving results in addressing and resolving the information sharing challenges. As such, we continue to believe that our recommendation for ONCD is necessary to evaluate the effectiveness of planned efforts. Neither of these recommendations had been implemented as of May 2024.

CISA needs to fully address best practices in customer service, workforce planning, and collaboration to improve the use of OT products and services for critical infrastructure.

Much of the nation's critical infrastructure relies on OT—systems that interact with the physical environment—to provide essential services, like controlling distribution processes and production systems (see figure 18). However, OT used by critical infrastructure owners and operators faces significant and increasing cybersecurity risks. Federal law designates

CISA as the lead agency in helping critical infrastructure owners and operators address these risks.²²

Figure 18: Key Components of a Pipeline Operational Technology System



Sources: GAO (analysis, controller icon); Staratel/stock.adobe.com (actuator icons); iconlauk/stock.adobe.com (operator and sensor icon). | GAO-24-107231

In March 2024, we reported that CISA provided 13 OT cybersecurity products and services between October 2018 and November 2023 at no cost to critical infrastructure owners and operators.²³ Twelve of the 13 selected nonfederal entities in our review cited examples of positive experiences with these OT products and services. For example, nonfederal entities found the industrial control system advisories and best

²²National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, § 1541, 135 Stat. 1541, 2054 (Dec. 27, 2021) amending sec. 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659).

²³GAO, *Cybersecurity: Improvements Needed in Addressing Risks to Operational Technology*, [GAO-24-106576](#) (Washington, D.C.: Mar. 7, 2024).

practice documents effective in helping them stay informed of threats and find vulnerabilities in their environments. However, CISA and seven of the nonfederal entities also identified challenges such as negative experiences using these products and services and insufficient CISA staff with requisite OT skills. Until CISA addresses best practices in customer service and effective workforce planning, the agency will not be optimally positioned to coordinate and deliver products and services needed to address OT risks.

Our review also included seven federal agencies within sector risk management agencies that were responsible for helping to protect their sectors and mitigate cyber OT risk. Six of the seven agencies in our review cited examples of collaboration with CISA that yielded positive outcomes in addressing OT risks; however, four agencies identified coordination challenges with CISA relating to ineffective information sharing and a lack of sharing processes. To address these challenges, it is important to adopt leading collaboration practices in guidance and policies. Until CISA takes action on the lack of guidance to sector risk management agencies on how to update plans for coordination and creates a policy for developing collaboration agreements with sector risk management agencies, these agencies will not be well positioned to coordinate on cyber OT risks.

- **We recommended** that CISA measure customer service for its OT products and services and perform effective workforce planning for OT staff. We also recommended that CISA issue guidance to the sector risk management agencies on how to update their sector-specific plans for better coordination on critical infrastructure issues, as well as develop an agency-wide collaboration policy on agreements with sector risk management agencies. DHS concurred with all of these recommendations; however, as of May 2024, they had not been implemented.

Federal entities should conduct an assessment to determine the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response.

Cyber threats to critical infrastructure represent a significant economic challenge (see table 4). Recent attacks illustrate that the effects of cyber incidents can spill over from the initial target to economically linked firms—thereby magnifying the damage to the economy. For example, in February 2022, Viasat, Inc. began experiencing outages with its European satellite internet service near the start of the Russian invasion

of Ukraine, according to press reporting. According to Viasat, the disruption was triggered by an attacker running destructive commands against Viasat network devices. In its forensic analysis of the incident, Sentinel Labs noted that the malware used in this attack shared some similarities with malware used in attacks attributed to the Russian government. As a result of the attack, a German wind turbine manufacturer explained that the remote operation of more than 5,000 turbines had been affected. In March 2022, CISA and the FBI warned critical infrastructure and other organizations of possible threats to U.S. and international satellite communication networks.

In addition, although the severity of cyber incidents pales in comparison to the severity of noncyber systemic events (such as the COVID-19 pandemic or the 2008 financial crisis), they could have been much more damaging than they were. For example, as discussed earlier, in May 2021, the Colonial Pipeline Company temporarily halted pipeline operations in response to a cybersecurity incident. Had the gasoline shortages caused by the Colonial Pipeline incident lasted longer, they could have had cascading effects on other sectors, with potentially devastating consequences.

Table 4: Frequency, Total Costs, and Per-Incident Costs of the Most Common Types of Cybersecurity Incidents, according to the FBI, 2016-2020 (Dollars in millions)

FBI's reported cybersecurity incidents		2016 incidents			2021 incidents		
Type	Description	Quantity	Total cost	Cost per incident	Quantity	Total cost	Cost per incident
Business email	A scam that involves compromising email accounts to conduct unauthorized transfer of funds.	12,005	\$360.514	\$0.030	19,954	\$2,395.953	\$0.120
Data breach	An unauthorized or unintentional exposure, disclosure, or loss of an organization's sensitive information.	3,403	\$95.870	\$0.028	1,287	\$151.568	\$0.118
Denial of service and distributed denial of service	An attack that prevents or impairs use of networks, systems, or apps. The distributed variant uses numerous hosts to perform the attack.	979	\$11.214	\$0.011	1,104	\$0.218	\$0.000
Ransomware	A type of malware used to deny access to IT systems or data and hold systems or data hostage until a ransom is paid.	2,673	\$2.431	\$0.001	3,729	\$49.208	\$0.013
Total		19,060	\$470.029	\$0.025	26,074	\$2,596.947	\$0.100

Source: Prior GAO reports and GAO analysis of FBI reports. | GAO-24-107231

Although cyber incident costs are paid in part by the private cyber insurance market, growing cyber threats have created uncertainty in this evolving market. Cyber insurance and the Terrorism Risk Insurance Program—the government backstop for losses from terrorism—are both limited in their ability to cover potentially catastrophic losses from systemic cyberattacks. Private insurers and the Terrorism Risk Insurance Program only cover cyberattacks that meet program criteria, even if catastrophic losses result.

In June 2022, we reported that CISA and Treasury's Federal Insurance Office had taken steps to understand the financial implications of growing cyber risks.²⁴ However, they had not assessed the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential

²⁴GAO, *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks*, [GAO-22-104256](#) (Washington, D.C.: June 21, 2022).

financial exposures warrant a federal insurance response. Due to their positions and responsibilities in critical infrastructure and insurance, they are well positioned to provide a joint assessment on whether a more extensive federal insurance response is warranted.

We have created a framework for providing federal assistance to private market participants that could inform a federal insurance response.²⁵ Consistent with the framework, any federal insurance response should include clear criteria for coverage, specific cybersecurity requirements, and a dedicated funding mechanism with concessions from all market participants.

- **We recommended** that CISA and the Federal Insurance Office produce a joint assessment on the extent to which the risks to critical infrastructure from catastrophic cyberattacks, and the potential financial exposures resulting from these risks, warrant a federal insurance response. Both agencies concurred with the recommendations; however, as of May 2024, neither of the recommendations had been fully implemented.

Grant programs provide cybersecurity support to state, local, tribal, and territorial governments, but federal agencies need to address challenges.

State, local, tribal, and territorial governments provide essential services that increasingly rely on the internet, making them vulnerable to various cybersecurity-related risks. Several types of these organizations, including schools, have also been particularly targeted by cybersecurity-related incidents such as ransomware, which can have devastating impacts on vital government operations and services. As we reported, according to the Multi-State Information Sharing and Analysis Center, state, local, tribal, and territorial organizations experienced approximately 2,800 ransomware incidents from January 2017 through March 2021.²⁶

The increasing cyber threats and attacks to state, local, tribal, and territorial entities highlight the importance and need for these entities to

²⁵GAO, *Financial Assistance: Ongoing Challenges and Guiding Principles Related to Government Assistance for Private Sector Companies*, [GAO-10-719](#) (Washington, D.C.: Aug. 3, 2010). Building on lessons learned from prior financial crises, we identified guiding principles to help serve as a framework for evaluating large-scale federal assistance efforts and provide guidelines for assisting failing companies.

²⁶GAO, *Federal Grants: Numerous Programs Provide Cybersecurity Support to State, Local, Tribal, and Territorial Governments*, [GAO-24-106223](#) (Washington, D.C.: Nov. 16, 2023).

strengthen their cybersecurity defenses. DHS and other federal agencies administer grant programs that can be used to help these governments improve their cybersecurity.

In November 2023, we reported that 27 federal grant programs that were managed by eight federal agencies could be used to fund state, local, tribal, and territorial governments' cybersecurity.²⁷ While none of these programs were intended to primarily support cybersecurity activities, four of the federal agencies tracked cybersecurity-related expenditures for 10 of the programs (see table 5).

Table 5: Cybersecurity-Related Grant Award Amounts Tracked by Four Agencies, Fiscal Years 2019 through 2022

Agency	Total cyber amount	Number of grant programs
Federal Emergency Management Agency	\$669,858,956	5
Election Assistance Commission	\$155,717,827	2
Department of the Interior	\$844,106	1
Institute of Museum and Library Services	\$708,926	2
Total	\$827,129,815.00	10

Source: GAO analysis of agency grant data. | GAO-24-107231

The eight agencies in our review had established policies and processes to monitor these grant programs and conducted periodic reviews to ensure the appropriate usage of funds. In addition, officials from national associations; state, local, tribal, and territorial government representatives; and agency officials did not identify challenges with applying for the 27 grant programs specific to cybersecurity. However, they identified challenges with the federal grant process in general. For example, officials from two national associations, one Tribal Nation, and three federal agencies said that the federal grant application process can be cumbersome for applicants, especially when the applicants are small state, local, tribal, and territorial governments with a relative lack of expertise in grant writing. Another Tribal Nation said it can be difficult to retain staff who have grant writing expertise. We had previously reported on grant programs and made many recommendations to improve the management and oversight of federal grants, but work remains to

²⁷GAO-24-106223. The eight selected agencies were the Departments of Interior, Justice, Labor, and Transportation; the Election Assistance Commission; the Environmental Protection Agency; DHS's Federal Emergency Management Agency; and the Institute of Museum and Library Services.

implement several recommendations.²⁸ Implementing the remaining recommendations will help to address grant management challenges, including the management of cybersecurity-related grant programs.

The Food and Drug Administration (FDA) and CISA should update agreements to reflect organizational and procedural changes related to the security of medical devices.

Cyber incidents that impact medical devices could delay critical patient care, reveal sensitive patient data, shut down health care provider operations, and necessitate costly recovery efforts. According to HHS and the Healthcare and Public Health Sector Coordinating Council, cyber incidents affecting network-connected medical devices are one of the types of current cyber threats in the Healthcare and Public Health Sector. As devices become more integrated with medicine and more digitally interconnected, securing medical devices against cyber threats is imperative.

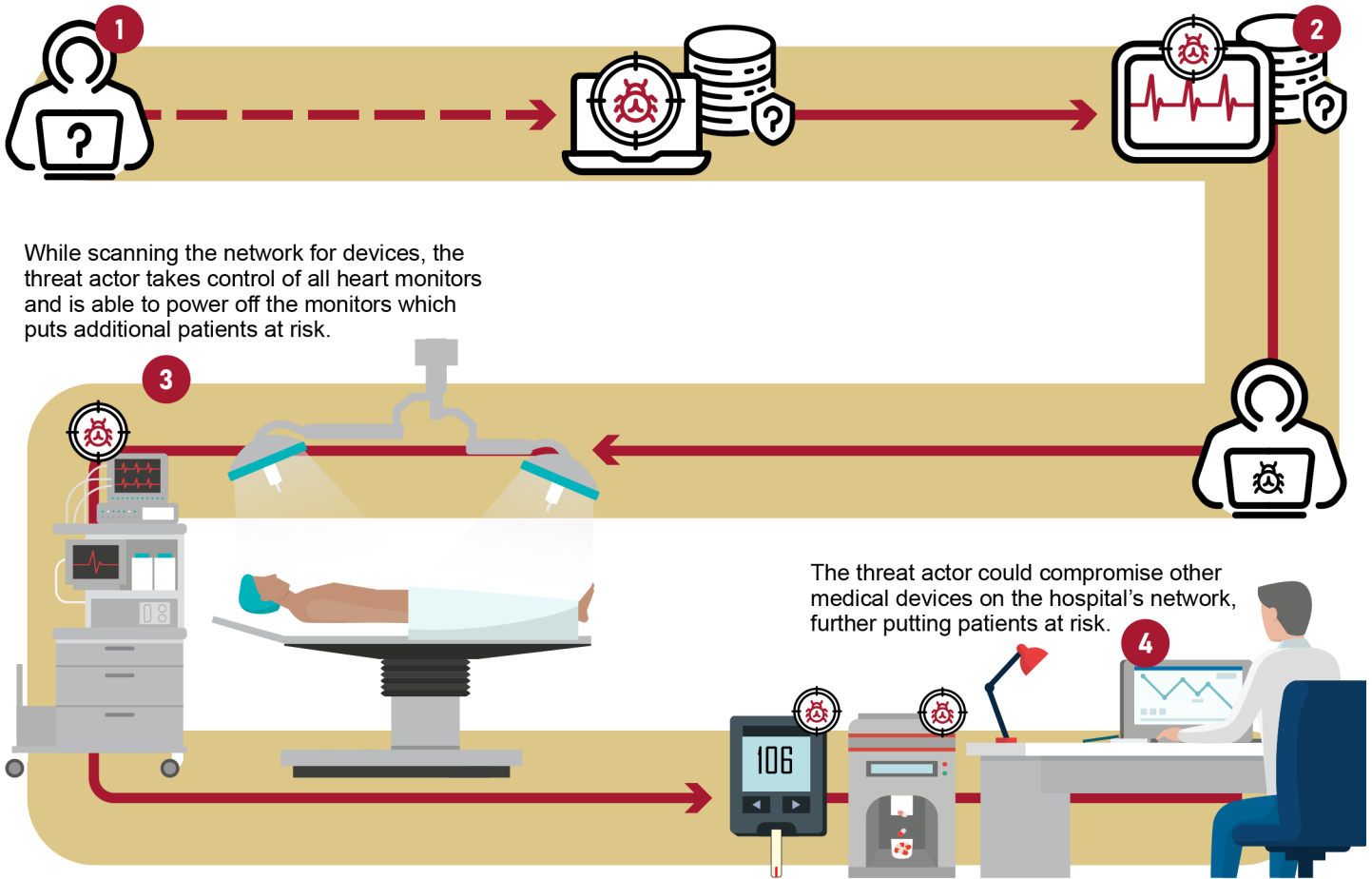
FDA is responsible for ensuring that medical devices sold in the U.S. provide reasonable assurance of safety and effectiveness. Cyber threats that target medical devices could delay critical patient care, reveal sensitive patient data, shut down health care operations, and necessitate costly recovery efforts (see figure 19).

²⁸For more information, see GAO, *Grants Management: Observations on Challenges with Access, Use, and Oversight*, [GAO-23-106797](#) (Washington, D.C.: May 2, 2023).

Figure 19: Example of a Compromised Medical Device That Can Lead to Disruption of Other Devices on a Hospital Network

Threat actor gains access to a healthcare provider's computer network by exploiting a vulnerability (e.g. a phishing attack).

Threat actor takes command of a server to which a patient heart monitor is attached.



Sources: GAO interpretation of Department of Health and Human Services example (illustrations); gofficon/stock.adobe.com (icons); elenabsl/stock.adobe.com (illustrations). | GAO-24-107231

In December 2023, we reported that nonfederal entities in the healthcare sector identified challenges in accessing federal support to address cybersecurity vulnerabilities, such as a lack of awareness of resources or difficulty understanding federal communications.²⁹ Legislation signed in

²⁹GAO, *Medical Device Cybersecurity: Agencies Need to Update Agreement to Ensure Effective Coordination*, [GAO-24-106683](#) (Washington, D.C.: Dec. 21, 2023).

2022 gave new authorities to FDA, including requiring medical device manufacturers to submit plans for monitoring, identifying, and assessing cybersecurity vulnerabilities.³⁰ Although limitations existed in authority for medical devices developed before the new legislation, FDA had taken actions to mitigate risks with CISA and other federal partners. In addition, while FDA and CISA had an agreement that generally addressed leading practices for collaboration and coordination, the agreement was over 5 years old and needed to be updated to reflect organizational and procedural changes since 2018.

- **We recommended** that CISA and FDA work together to update agency agreements to reflect organizational and procedural changes. Both agencies concurred with the recommendations. However, as of May 2024, the recommendations had not been implemented.

What ongoing or upcoming work is GAO doing related to this challenge area?

Given the importance of addressing this challenge area, we are continuing to review and assess agencies' various cybersecurity-related initiatives in this area. To combat increased cybersecurity risks, public and private sectors must continue to work together to protect critical infrastructure. Accordingly, it is important that efforts continue to strengthen the federal role to prevent attacks that could result in serious harm to human safety, national security, the environment, and the economy. Table 6 identifies our ongoing and upcoming work related to this action and challenge area.

³⁰Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, § 3305(a), 136 Stat. at 5834 (2022)(to be codified at 21 U.S.C. § 360n-2).

Table 6: Ongoing and Upcoming GAO Work Related to the Protecting the Cybersecurity of Critical Infrastructure Challenge Area, as of May 2024

Critical action area	Related ongoing and upcoming GAO work
Action 8: Strengthen the federal role in protecting the cybersecurity of critical infrastructure.	<p>Ongoing reviews of:</p> <ul style="list-style-type: none"> • the potential cybersecurity risks to water and wastewater systems and the extent to which the Environmental Protection Agency has taken action to address known cybersecurity risks to water and wastewater systems, • the extent to which the Department of Homeland Security (DHS) is implementing requirements of the Cyber Incident Reporting for Critical Infrastructure Act and mitigating associated challenges, • the extent to which selected agencies have conducted risk assessments on potential artificial intelligence risks to critical infrastructure sectors in accordance with leading practices, • cybersecurity threats and risks to the Maritime Transportation System and related Coast Guard actions to mitigate them, and • the extent to which the Federal Emergency Management Agency’s and the Cybersecurity and Infrastructure Agency’s grant processes for the State and Local Cybersecurity Grant Program meet requirements. <p>Upcoming reviews of:</p> <ul style="list-style-type: none"> • DHS’s management of the Port Security Grant program, including challenges, overall effectiveness, and reducing cybersecurity risks to U.S. ports; and • evaluating the quantity and impact of unreported cyber incidents on impacted entities, homeland security, and the national economy.

Source: GAO. | GAO-24-107231

Challenges in Protecting Privacy and Sensitive Data

The federal government should:

Improve federal efforts to protect privacy and sensitive data

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

Overview

Federal agencies must ensure that any PII they collect, store, or process is protected from unauthorized access, tampering, or loss. However, the protection of personal privacy has become a more significant issue in recent years with the advent of new technologies. The increasingly sophisticated ways in which both the federal government and nongovernment entities use personal information has 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.

It is essential that both private and public entities take effective measures to safeguard the sensitive and personal information collected from members of the public. However, incidents threatening the security of this information continue to affect private and public entities. For example, in March 2024, AT&T reported that some of its data had been released onto the dark web.³¹ Sensitive personal information, such as Social Security numbers and passcodes, were part of the data set released onto the dark web. Based on preliminary analyses at that time, the data set appeared to be from 2019 or earlier, impacting approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders. This resulted in AT&T resetting passcodes and offering complimentary identity theft and credit monitoring services to the compromised individuals.

In addition, the Department of Education reported a major incident involving the breach of PII involving a loan servicing vendor's system. Beginning in June of 2022, a nonstate criminal actor began attacking a web application, leveraging a vulnerability on a vendor-operated loan registration website. The attacker maintained a presence on the system until July 2022 when the activity was detected and the system was immediately shut down. Following the incident, the vendor took mitigating steps to better secure its systems through implementation of additional user validations and penetration testing exercises. Notification and credit monitoring services were offered to potentially affected individuals.

We have made 249 recommendations in public reports since 2010 in this challenge area. Federal agencies have taken steps to address 137 of these recommendations. However, as of May 2024, 112 of these recommendations have not been implemented. Until these recommendations are fully implemented, federal agencies will be limited in their ability to protect private and sensitive data entrusted to them.

³¹<https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html>

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

Federal law enforcement agencies should implement training and privacy requirements for the use of facial recognition services.

Law enforcement may use facial recognition services provided by commercial and nonprofit entities to help solve crimes. For example, these services allow users to quickly search through billions of photos to help identify an unknown suspect in a crime scene photo. The use of facial recognition technology for criminal investigations presents unique questions about civil rights and civil liberties. For example, civil liberties advocates have noted that the use of facial recognition at certain events—such as protests—could have a chilling effect on individuals’ exercise of their First Amendment rights.³² As a result, civil rights advocates have cautioned that an over-reliance on facial recognition technology in criminal investigations could lead to the arrest and prosecution of innocent people, and in particular innocent people of certain racial and ethnic backgrounds.³³

In September 2023, we reported that seven law enforcement agencies in DHS and the Department of Justice (DOJ) initially used facial recognition services without requiring staff to take training on topics such as how facial recognition technology works, what photos are appropriate to use, and how to interpret results.³⁴ Some agencies required general privacy training for all staff, and made optional facial recognition training available to staff, both of which may have benefited staff using facial recognition services. However, we found that, cumulatively, agencies with available data reported conducting about 60,000 facial recognition searches without requiring that staff take training on facial recognition technology to

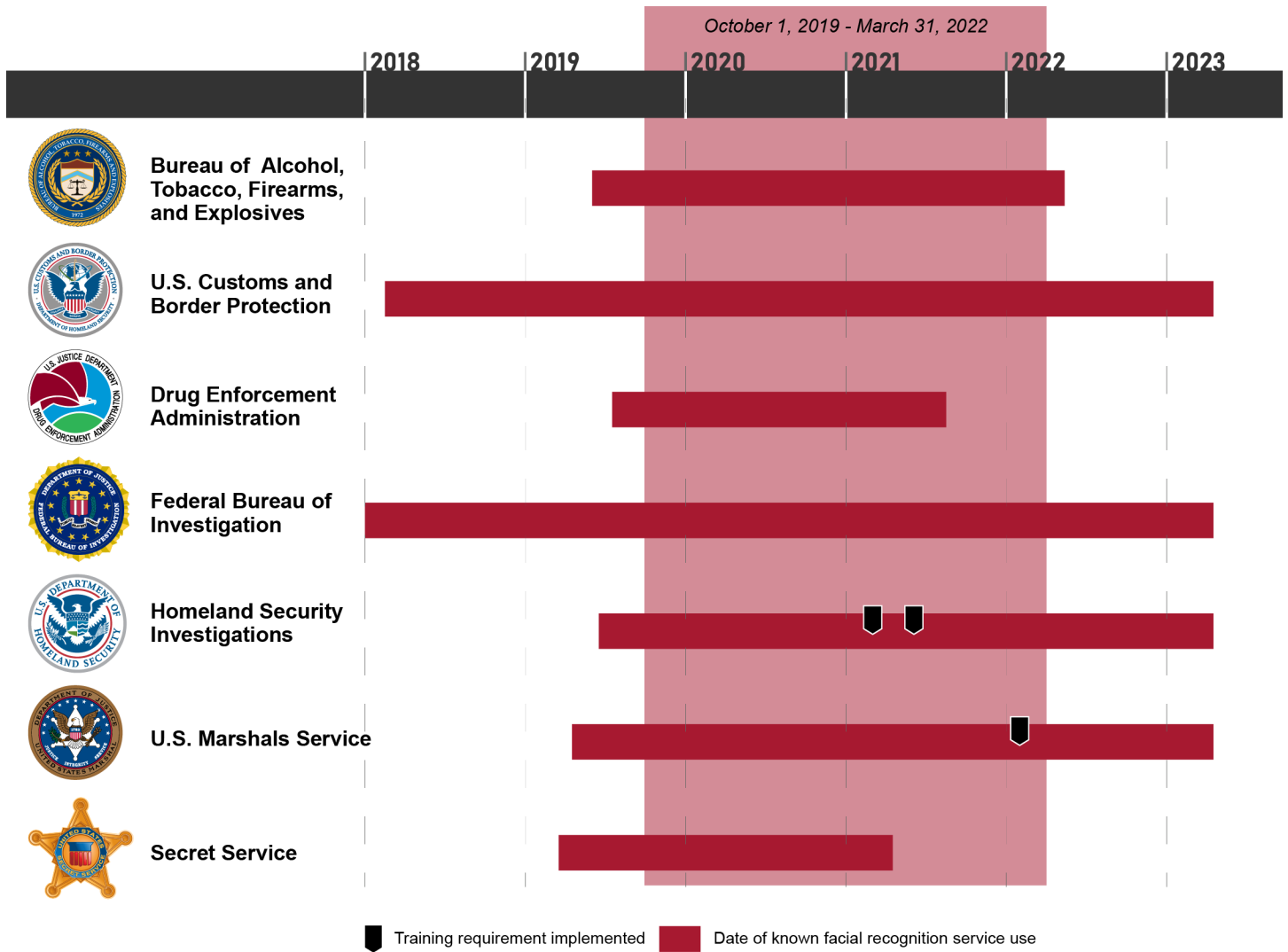
³²See, e.g., *Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties: Hearing Before the H. Comm. on Oversight and Reform*, 116th Cong. (2019) (statement of Neema Singh Guliani, Senior Legislative Counsel, American Civil Liberties Union).

³³National Association of Criminal Defense Lawyers, *Letter to the White House Office of Science and Technology Policy* (Jan. 15, 2022).

³⁴GAO, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties*, [GAO-23-105607](#) (Washington, D.C.: Sept. 5, 2023). The agencies in our review were U.S. Customs and Border Protection; U.S. Immigration Custom Enforcement’s Homeland Security Investigations; U.S. Secret Service; Bureau of Alcohol, Tobacco, Firearms, and Explosives; Drug Enforcement Administration; Federal Bureau of Investigation; and the U.S. Marshals Service. These agencies reported using four different facial recognition services in total to support criminal investigations: IntelCenter, Marinus Analytics, Thorn, and Clearview AI.

use these services. While some agencies had developed and implemented training requirements, others had not assessed whether training would be beneficial. In particular, as of April 2023, only two agencies had begun to require training (see figure 20).

Figure 20: Selected Law Enforcement Agencies' Implementation of Training Requirements to Use Facial Recognition Services, as of April 2023



Sources: GAO analysis of agency information; agencies (logos). | GAO-24-107231

Note: This timeline represents agencies' use of commercial and nonprofit facial recognition services and training requirements to use such services between October 1, 2019, through March 31, 2022 (see red shading in figure). The timeline ranges from January 2018 to April 2023 because agencies may have used these four services prior October 1, 2019, and continued to use these services after March 31, 2022. We assessed the extent to which agencies had implemented training specifically required for using facial recognition services and did not assess requirements for more general training that agency staff may receive, such as general privacy training.

Additionally, we reported that while three of the seven law enforcement agencies took steps to address some privacy requirements applicable to facial recognition services, the remaining four agencies did not fully address any privacy requirements. These requirements included (1) conducting an initial privacy review prior to acquiring the service, (2) conducting a privacy impact assessment prior to acquiring the service, (3) assessing privacy needs prior to acquisition, and (4) overseeing privacy controls for contractor access to PII. Further, we reported that most agencies had yet to make determinations about whether certain privacy requirements applied to their use of a facial recognition service. By taking actions to ensure agencies address outstanding privacy requirements for facial recognition services, DHS and DOJ can better ensure that PII is not inappropriately disclosed or compromised.

- **We recommended** that DHS and DOJ establish, implement, and clarify training requirements for their staff and stakeholders using facial recognition services. Additionally, we recommended that DHS and DOJ work to address their outstanding privacy requirements and update their privacy documentation, as appropriate, with respect to their components that continue to use facial recognition services, among other recommendations. The agencies concurred with all 10 recommendations. As of May 2024, two of the recommendations had been implemented by DOJ.

The Internal Revenue Service (IRS) needs to address critical weaknesses in safeguards for protecting taxpayer information.

In August 2023, we reported that IRS had implemented some safeguards aimed at better protecting taxpayer information and that some of the IRS's selected offices generally had followed the agency's willful unauthorized access, attempted access, or inspection of federal tax information policies.³⁵ However, IRS's oversight of contractors accessing taxpayer information had gaps. Specifically, we reported that IRS's monitoring of efforts to prevent such unauthorized access was limited by its incomplete inventory of systems that process or store taxpayer information. The lack of completeness limited IRS's visibility into all of its systems that store and process taxpayer information. The incomplete inventory also limited the Privacy, Governmental Liaison, and Disclosure Office's ability to target training and monitor willful unauthorized access, attempted access, or inspection of federal tax information case trends

³⁵GAO, *Security of Taxpayer Information: IRS Needs to Address Critical Safeguard Weaknesses*, [GAO-23-105395](#) (Washington, D.C.: Aug. 14, 2023).

because the office did not have important contextual information, such as the number of employees authorized to access taxpayer information.

Maintaining a comprehensive system inventory will help IRS ensure it has implemented safeguards to protect taxpayer information being processed or stored on all of its systems, applications, and databases. Further, having a comprehensive inventory would enable IRS to monitor all relevant IT systems—systems that process taxpayer information—to detect if its staff access taxpayer information without authorization.

Additionally, we reported that IRS did not have direct authority to inspect agencies' safeguards for taxpayer information in certain circumstances. In those specific circumstances, IRS faced challenges ensuring that taxpayer information it shared—as authorized by law—was properly protected. Federal tax law gives IRS the authority to inspect safeguards for agencies that receive taxpayer information from IRS in certain circumstances. However, in other cases where IRS shared taxpayer information pursuant to different statutory authority, it did not have direct authority to inspect agency safeguards. For these cases, Congress could provide IRS with direct authority to inspect agencies' safeguards, which would give it additional assurance that information will be sufficiently protected.

- **We recommended**, among other things, that IRS maintain a comprehensive inventory of its systems that process or store taxpayer information. Additionally, we recommended that Congress consider providing IRS with additional authority to inspect agencies' data safeguards in those instances where IRS shares taxpayer information but did not have direct authority to inspect agency safeguards. IRS agreed with the recommendation; however, as of April 2024, the recommendation had not been implemented. Further, as of May 2024, there had been no legislative action that would provide IRS with the additional authority to inspect agencies' data safeguards.

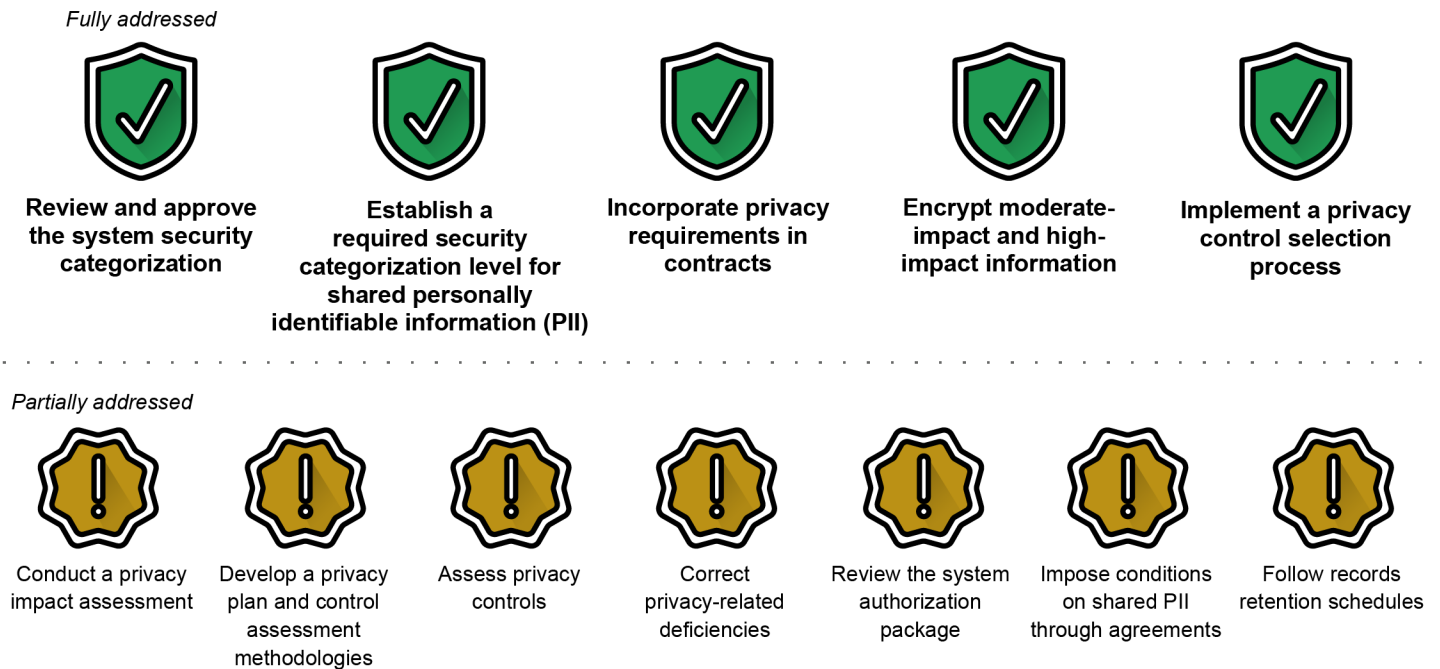
DHS needs to address significant shortcomings in privacy requirements for its modernized biometric identity management system.

The DHS Management Directorate's Office of Biometric Identity Management (OBIM) is the lead entity responsible for providing biometric identity management services that support national security and public safety decision making for DHS and its approximately 140 partners. DHS currently provides biometric identity management services through the Automated Biometric Identification System, but it initiated a multi-billion-dollar program known as the Homeland Advanced Recognition Technology (HART) program in 2016 to replace the existing program. The HART system is intended to be a centralized DHS-wide biometric database, which stores and manages over 290 million individuals' PII, including biographic and biometric information.

In September 2023, we reported that DHS did not fully implement a majority of the selected federal privacy requirements to ensure the protection of PII in the HART program.³⁶ Some of the requirements included conducting a privacy impact assessment, reviewing the system authorization package, and incorporating privacy requirements in contracts. Specifically, of the 12 selected OMB privacy requirements, the department fully implemented five and partially implemented seven (see figure 21).

³⁶GAO, *Biometric Identity System: DHS Needs to Address Significant Shortcomings in Program Management and Privacy*, [GAO-23-105959](#) (Washington, D.C.: Sept. 12, 2023).

Figure 21: Summary of Department of Homeland Security’s Implementation of Selected Office of Management and Budget Privacy Requirements for the Homeland Advanced Recognition Technology (HART) Program



Sources: GAO (analysis and yellow icon); YEVHENIIA/stock.adobe.com (green icon). | GAO-24-107231

The gaps in implementing key privacy requirements reduced HART’s ability to appropriately protect individuals’ PII. For example, without ensuring that privacy controls were assessed, and any identified deficiencies were corrected, the program had less assurance that PII collected by the system was protected from unauthorized disclosure or misuse. As a result, until OBIM addresses weaknesses in HART privacy protections, the office may develop a system that puts individuals’ PII at increased risk for compromise.

- **We recommended** that DHS work with OBIM and its Privacy Office to address the shortcomings related to the seven partially addressed privacy requirements. DHS concurred with the recommendations; however, as of May 2024, the recommendations had not been implemented.

DHS's Office of Intelligence and Analysis (I&A) should improve privacy oversight and assessment of its effectiveness by performing audits.

Within DHS, I&A has an important role to play in collecting and disseminating threat information to DHS components and other partners to mitigate threats to homeland security. Because such reporting can involve information about U.S. persons, the office issued Intelligence Oversight Guidelines that identified safeguards to protect privacy, civil rights, and civil liberties.³⁷

In August 2023, we reported that I&A had not fully implemented activities intended to monitor whether personnel were following its policies to protect the privacy, civil rights, and civil liberties of U.S. persons, including U.S. citizens and lawful permanent residents.³⁸ Specifically, I&A had not conducted two of the four monitoring activities called for in its Intelligence Oversight Guidelines—audits of information systems and audits of bulk data (see table 7). Neither the I&A Intelligence Oversight Guidelines nor the accompanying policy instruction identified who was to conduct these audits.

³⁷Department of Homeland Security, Office of Intelligence and Analysis, *Intelligence Oversight Guidelines* (Washington, D.C.: January 2017).

³⁸GAO, *Homeland Security: Office of Intelligence and Analysis Should Improve Privacy Oversight and Assessment of Its Effectiveness*, [GAO-23-105475](#) (Washington, D.C.: Aug. 28, 2023).

Table 7: Extent to Which the Department of Homeland Security’s Office of Intelligence and Analysis (I&A) Conducted Required Monitoring Activities to Ensure the Protection of Privacy, Civil Rights, and Civil Liberties

Monitoring activities	Description	GAO assessment
Audits of information systems	I&A is to audit information systems containing U.S. persons information to assess (1) whether I&A personnel had appropriate security clearances, a mission requirement, and met other requirements to access these systems; and (2) whether I&A personnel tailored their searches in these systems to minimize the amount of irrelevant U.S. persons information returned. ^a	Not conducted
Audits of bulk data	I&A is to audit bulk data that were transferred to or from I&A and that contain U.S. persons information. ^b These audits are to assess whether access to such data, and searches conducted in the data, were appropriately limited to protect individuals’ privacy, civil rights, and civil liberties.	Not conducted
Compliance reviews	The Intelligence Oversight Officer, who leads I&A’s intelligence oversight branch, is required to conduct periodic reviews to verify personnel’s compliance with the Intelligence Oversight Guidelines. These compliance reviews may involve employee or contractor interviews, reviews of audit logs, unannounced reviews (spot checks), or records reviews.	Conducted
Preliminary inquiries	The Intelligence Oversight Guidelines states that the Intelligence Oversight Officer, in consultation with the Associate General Counsel for Intelligence, is to commence a preliminary inquiry upon notification of any potential violation of federal criminal law or questionable activity.	Conducted

Source: GAO. | GAO-24-107231

^aU.S. persons information is either a single item of information or information that, when combined with other available information, is reasonably likely to identify one or more specific U.S. persons. A U.S. person is: (1) a U.S. citizen, (2) a foreign national known by the intelligence element to be a lawful permanent resident, (3) an unincorporated association substantially composed of U.S. citizens or permanent residents, or (4) a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments. Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), as amended, 3.5(k).

^bBulk data are large quantities of data acquired without the use of discriminants (e.g., specific identifiers or selection terms), a significant portion of which are not reasonably likely to have intelligence or operational value. Any bulk data containing U.S. persons information that are transferred into or out of I&A are subject to terms and conditions that the Under Secretary for Intelligence and Analysis establishes for each transfer. I&A is required to audit access to, or searches conducted in the bulk data collection only if the terms and conditions governing that collection require such audits.

With regard to not conducting two of the four monitoring activities, the Intelligence Oversight Officer said I&A may not have identified who was responsible for conducting and reporting on these audit activities when it issued the guidelines in 2017 because I&A was a relatively young agency. Further, according to the Intelligence Oversight Officer, after the Attorney General approved I&A’s guidelines in January 2017, I&A did not develop any additional implementation guidance that might have identified the responsible individuals. Without identifying who is responsible for conducting these audits and to whom the results should be reported, I&A risks being unaware of potential failures of staff to appropriately protect privacy.

-
- **We recommended** that DHS’s I&A identify who is responsible for conducting the audits of information systems and bulk data as described in I&A’s Intelligence Oversight Guidelines, and to whom the results of these audits should be reported. Further, once the responsible entities are identified, I&A should ensure that these entities are conducting the audits of information systems and bulk data. DHS agreed with our recommendations; however, as of April 2024, the recommendations had not been implemented.

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?

HHS’s Office for Civil Rights should continue to support providers in educating patients on the increased risk of privacy and security to protected health information.

By law, Medicare pays for telehealth services under limited circumstances—such as only in certain (mostly rural) geographic locations. However, in response to the COVID-19 pandemic, in March 2020, HHS issued waivers and other flexibilities that temporarily waived certain Medicare restrictions on telehealth—the delivery of some services via audio-only or video technology. However, the expanded availability of telehealth services under the waivers may also present new risks of fraud, waste, and abuse.³⁹ In addition, researchers have raised questions about the extent to which beneficiaries have equal access to telehealth services. Moreover, the use of telehealth technology may present privacy and security risks to Medicare beneficiaries, such as the inappropriate disclosure of beneficiaries’ health information.⁴⁰ Within HHS, the Office for Civil Rights is responsible for administering and enforcing the regulations

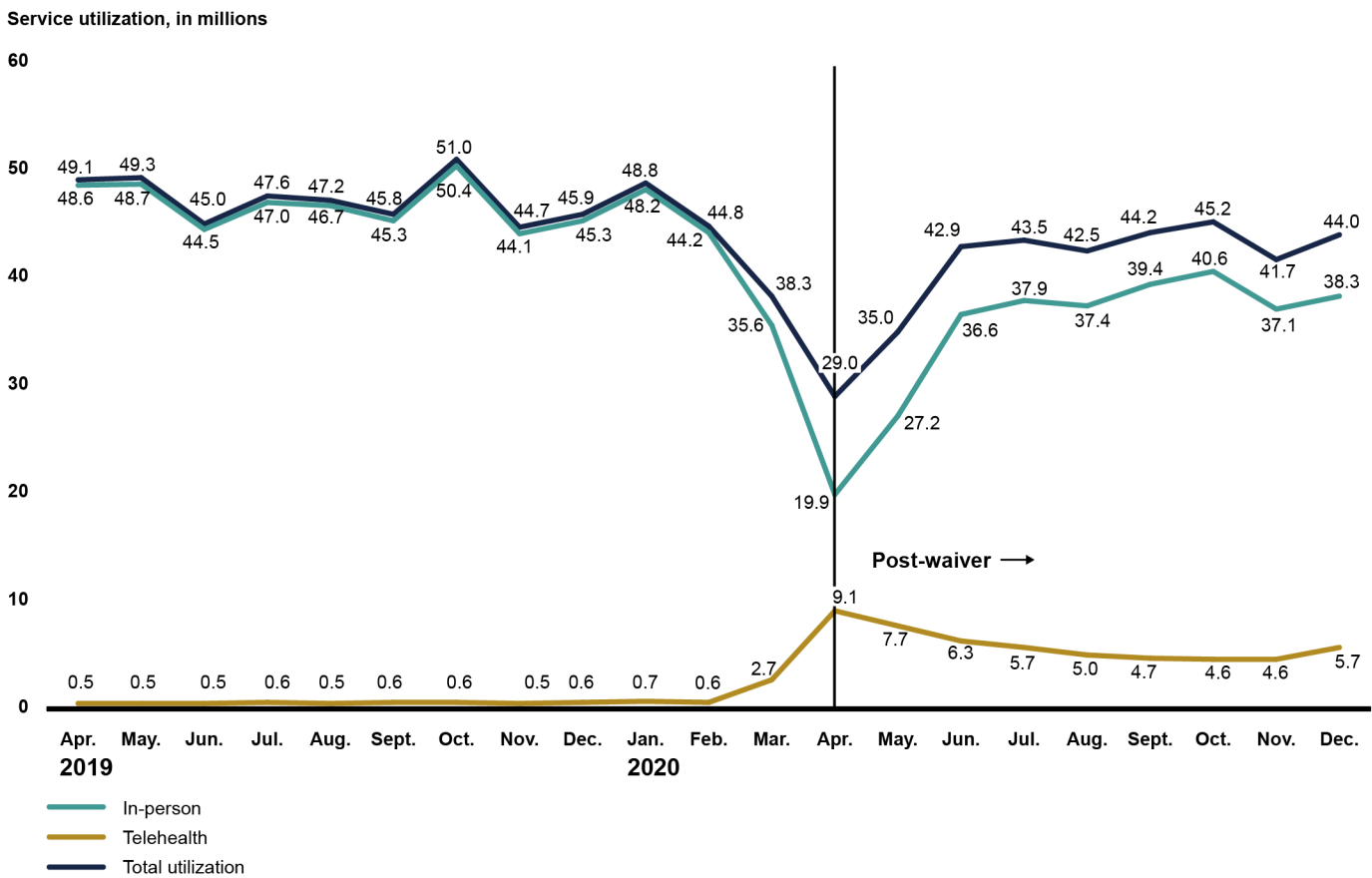
³⁹Fraud involves obtaining something of value through willful misrepresentation. Waste is the act of using or expending resources carelessly, extravagantly, or to no purpose. Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary operational practice given the facts and circumstances. This includes the misuse of authority or position for personal gain or for the benefit of another.

⁴⁰See, for example, Lori Uscher-Pines and Lucy Schulson, “Rethinking the Impact of Audio-Only Visits on Health Equity,” *Health Affairs* (Washington, D.C.: Dec. 17, 2021), accessed June 15, 2022, <https://www.healthaffairs.org/doi/10.1377/forefront.20211215.549778/full>; and Geetter, J. S., et al., “OCR Enforcement Waivers of Certain HIPAA Requirements in Furtherance of Telehealth During COVID-19 Pandemic,” *National Law Review*, vol. XII, no. 166 (2020).

which protect patients' health information, including Medicare beneficiaries.⁴¹

In September 2022, we reported that the utilization of telehealth services increased from about 5 million services from April to December 2019 to more than 53 million services over the same period in 2020—a tenfold increase (see figure 22).⁴²

Figure 22: Utilization of Medicare Services Delivered via Telehealth or In-person, by Month, April 2019-December 2020



Source: GAO analysis of Centers for Medicare & Medicaid Services data. | GAO-24-107231

⁴¹These regulations protect certain individually identifiable health information (referred to as protected health information) of individuals, including Medicare beneficiaries.

⁴²GAO, *Medicare Telehealth: Actions Needed to Strengthen Oversight and Help Providers Educate Patients on Privacy and Security Risks*, [GAO-22-104454](#) (Washington, D.C.: Sept. 26, 2022).

We also found that HHS's Office for Civil Rights used its enforcement discretion to allow providers to use a broad range of nonpublic-facing remote communication technologies to provide telehealth without the risk that the office might seek to impose a penalty for noncompliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules during the public health emergency. Providers' subsequent use of such technologies potentially introduced additional privacy and security risks—such as patients' protected health information being overheard or disclosed without their permission or knowledge. Providing additional education, outreach, or other assistance to providers may help ensure that patients understand potential privacy and security risks of video telehealth platforms. This also may help patients make better informed decisions in accessing telehealth services.

- **We recommended** that HHS's Office for Civil Rights provide additional education, outreach, or other assistance to providers to help them explain the privacy and security risks to patients in plain language when using video telehealth platforms to provide telehealth services. HHS concurred with this recommendation and the Office for Civil Rights subsequently took steps in November 2023 to fully implement the recommendation.

Congress needs to increase oversight and protection to mitigate the increasing risks to consumer data privacy.

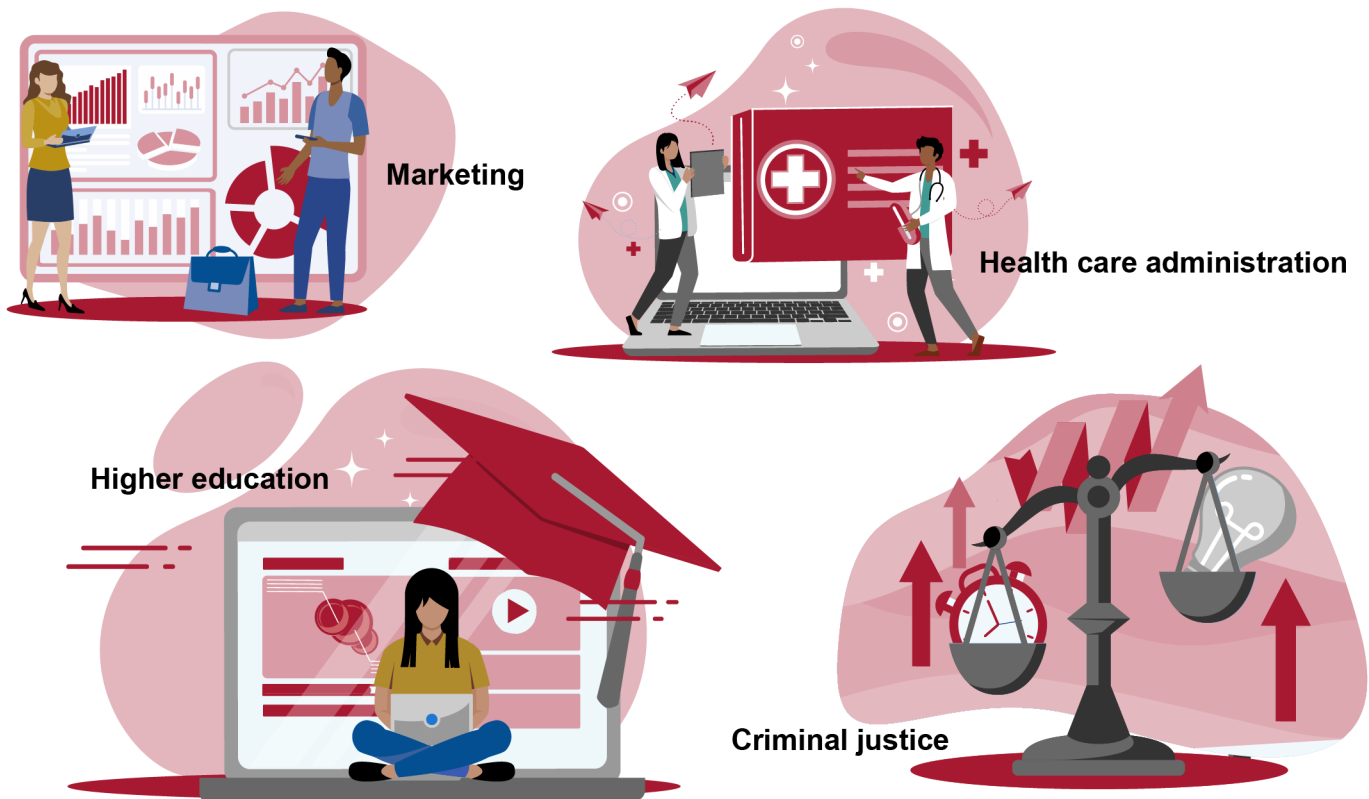
As technologies change, consumers may not always know what data businesses are collecting about them, or how those data are used and shared. Advanced, internet-connected technologies help businesses gather increasing amounts of personal data, track online behavior, and monitor consumers' locations and activities, intensifying concerns about the privacy and accuracy of consumer data. For example, in April 2018, Facebook disclosed that a Cambridge University researcher may have improperly shared the data of up to 87 million of its users with a political consulting firm. This disclosure followed other recent incidents involving the misuse of consumers' personal data from the internet, which is used by about three-quarters of Americans.

In September 2022, we highlighted our previous work on the risks that the increasing collection and use of personal information pose to consumer privacy and protection.⁴³ For example, companies collect personal and transactional data to create consumer scores, which businesses and

⁴³GAO, *Consumer Data: Increasing Use Poses Risks to Privacy*, [GAO-22-106096](#) (Washington, D.C.: Sept. 13, 2022).

other entities use to predict how consumers will behave in the future. Figure 23 identifies key sectors where the collection of consumer data is used to create these scores.

Figure 23: Key Sectors Where Consumer Scores Are Used



Sources: GAO; Alwie99d/stock.adobe.com (illustrations). | GAO-24-107231

These consumer scores are separate and distinct from credit scores, which serve a different purpose, and introduce a variety of potential risks, such as biased outcomes, inaccurate scores, and differential treatment. No federal law expressly governs the creation, sale, and use of consumer scores, and existing federal consumer protection laws may not apply to some newer uses of consumer data. This could result in gaps in federal consumer protections.

Businesses can also use facial recognition technology to verify or identify people and provide them with access to buildings or online accounts.

They can also use the technology to authorize payments, identify shoplifters, and even monitor the spread of COVID-19. However, consumers may be unaware of potential privacy and data security risks associated with this technology, such as loss of anonymity, lack of consent, and performance differences between demographic groups, which could lead to misidentification or profiling. Further, in most contexts federal law does not address how personal data derived from facial recognition technology may be used or shared.

As we have previously reported, while the Federal Trade Commission has the lead in overseeing internet privacy across all industries, with some exceptions, there is no comprehensive U.S. internet privacy law governing private companies' collection, use, or sale of internet users' data, leaving consumers with limited assurance that their privacy will be protected.

- **We recommended** in our previous work on consumer privacy that Congress consider ways to determine and implement appropriate consumer protections for consumer scores beyond existing federal laws, such as allowing consumers to view and correct data and to be informed of score uses and their potential effects. Additionally, we recommended that Congress strengthen the federal consumer privacy framework to reflect changes in technology and the marketplace. Further, we recommended that Congress consider comprehensive legislation on internet privacy that would enhance consumer protections and include the oversight authorities agencies should have. As of May 2024, there had been no new legislative action related to implementing consumer protections for consumer scores, strengthening the consumer privacy framework, or new internet privacy legislation to enhance agencies' oversight authority.

Agencies need to fully implement OMB guidance and requirements related to the disclosure of personal information.

With certain enumerated exceptions, the Privacy Act of 1974 prohibits disclosure of records to any person or agency, unless disclosure is pursuant to the prior written request by, or with the prior written consent of, the individual to whom the record pertains.⁴⁴ Accordingly, agencies have developed various procedures and forms by which individuals may

⁴⁴With certain enumerated exceptions, “[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant written request by, or with the prior written consent of, the individual to whom the record pertains...” 5 U.S.C. §552a(b).

establish their identity and request access to or provide written consent for the disclosure of their records.

To simplify and modernize this process, the Creating Advanced Streamlined Electronic Services for Constituents Act of 2019 (CASES Act) required OMB to issue applicable guidance. This guidance was to: (1) require agencies to accept electronic identity proofing and authentication, (2) create a template for electronic consent and access forms and requires each agency to post the template on the agency website, and (3) require each agency to accept electronic consent and access forms from individuals that have been properly identity proofed and authenticated.⁴⁵ As required by the CASES Act, in November 2020, OMB issued guidance to agencies that included all the required elements referenced by the CASES Act requirements.⁴⁶ Agencies were instructed to implement the requirements in OMB's guidance by November 2021.

In December 2022, we reported on the extent to which 17 selected agencies addressed the requirements in the CASES Act.⁴⁷ We found that only one of the 17 selected agencies had reported full implementation of the requirements set forth by OMB, while five agencies had committed to time frames for implementing the requirements (see table 8).

⁴⁵Creating Advanced Streamlined Electronic Services for Constituents Act of 2019, Pub. L. No. 116-50, 133 Stat. 1073-74 (Aug. 22, 2019).

⁴⁶Office of Management and Budget, *Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act*, OMB Memorandum M-21-04 (Washington, D.C.: Nov. 12, 2020).

⁴⁷GAO, *Information Management: Agencies Need to Streamline Electronic Services*, [GAO-23-105562](#) (Washington, D.C.: Dec. 20, 2022).

Table 8: Selected Agencies' Implementation of the Office of Management and Budget's Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act Memorandum

Agency	Accept remote identity proofing and authentication	Digitally accept the access and consent forms	Post the forms on privacy program website
Department of Agriculture	◐	◐	○
Department of Defense	○	○	○
Department of Health and Human Services	◐	◐	○
Department of Homeland Security	◐	○	○
Department of the Interior	○	◐	○
Department of Justice	○	○	○
Department of Labor	○	○	○
Department of State	◐	◐	○
Department of Transportation	○	○	○
Department of the Treasury	◐	◐	○
Department of Veterans Affairs	○	○	○
Environmental Protection Agency	◐	◐	○
Equal Employment Opportunity Commission	○	◐	○
National Archives and Records Administration	○	○	○
Office of Personnel Management	○	◐	○
Securities and Exchange Commission	●	●	●
Social Security Administration	◐	◐	○

● = Fully implemented ◐ = Partially implemented ○ = Not implemented

Source: GAO. | GAO-24-107321

The remaining 11 agencies had not addressed the requirements or committed to time frames for implementing them. Until the other agencies implement the requirements or commit to doing so within a reasonable time frame, these agencies could not ensure that they are using modern processes for individuals to establish their identity and request access to or provide consent for disclosure of their records.

- **We recommended** that each of the 11 remaining agencies establish reasonable time frames for fully implementing OMB guidance. Specifically, the abilities to accept remote identity proofing with authentication, to digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, as well as to post access and consent forms on the agency's privacy program website. Seven agencies concurred with our recommendations. The remaining four agencies either generally agreed or did not state whether they agreed or disagreed with the

recommendations. As of May 2024, none of the recommendations had been implemented.

What ongoing or upcoming work is GAO doing related to this challenge area?

Given the importance of addressing this challenge area, we are continuing to review and assess agencies' various cybersecurity-related initiatives in this area. It is essential that executive branch agencies continue to focus on efforts to fully protect privacy and sensitive data. Efforts to address these challenges are critical to ensuring that the country can identify, prepare for, and respond to unauthorized attempts to compromise sensitive and personal information. Table 9 identifies our ongoing and upcoming work related to each action associated with this challenge area.

Table 9: Ongoing and Upcoming GAO Work Related to the Protecting Privacy and Sensitive Data Challenge Area, as of May 2024

Critical action area	Related ongoing and upcoming GAO work
Action 9: Improve federal efforts to protect privacy and sensitive data.	<p>Ongoing reviews of:</p> <ul style="list-style-type: none"> • the Internal Revenue Service's protection of taxpayer information, and • Login.gov's cost and protection capabilities in comparison to other vendor solutions. <p>Upcoming reviews of:</p> <ul style="list-style-type: none"> • the security implications due to the Department of Defense's personnels' digital footprints, and • the Department of Homeland Security's Homeland Advanced Recognition Technology System and its compliance with privacy standards.
Action 10: Appropriately limit collection and use of personal information and ensure it is obtained with appropriate knowledge or consent.	<p>Ongoing reviews of:</p> <ul style="list-style-type: none"> • Federal Civil Rights and Civil Liberties Programs' collection, use, and sharing of personal information; • the extent of the Department of Health and Human Services' efforts to safeguard the collection of public health data; • the Department of Veterans Affairs' collection, use, and sharing of veterans' data; and • the extent to which Department of Justice law enforcement agencies have policies and procedures in place that limit the collection and use of information from detection, observation, and monitoring technologies.

Source: GAO. | GAO-24-107231

Closing

Cybersecurity remains a critical high-risk issue facing our nation. We have highlighted this issue for over 25 years, and it has only grown more significant as cyberattacks have become more sophisticated and potentially damaging to the essential operations of the federal government and the critical infrastructure supporting American life. Further, the capability to carry out potentially devastating cyberattacks is increasingly spread among adversarial nation-states, cyber criminals, and other malicious actors.

Although the emergence of new technologies such as AI and quantum computing holds promise for dramatic advances in a variety of fields, they also have the potential to introduce significant new risks to systems, information, and personal privacy. The federal government must therefore take a proactive approach to assessing these technologies and mitigating the risks they may introduce.

New technologies and their corresponding risks underscore the urgency of tackling the four major cybersecurity challenges and 10 associated actions. Key to addressing these critical actions is implementing our recommendations. Until these recommendations are fully implemented, the federal government will be hindered in ensuring the security of federal systems and critical infrastructure and the privacy of sensitive data. This increases the risk that the nation will be unprepared to respond to the cyber threats that can cause serious damage to public safety, national security, the environment, and economic well-being.

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

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

Marisol Cruz Cain
Director, Information Technology and Cybersecurity

List of Addressees

The Honorable Gary C. Peters
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Mitt Romney
Ranking Member
Subcommittee on Emerging Threats and Spending Oversight
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Jamie Raskin
Ranking Member
Committee on Oversight and Accountability
House of Representatives

The Honorable Marsha Blackburn
Senator
United States Senate
The Honorable Gerald E. Connolly
Representative
House of Representatives



Appendix I: Prior GAO Work

We have previously reported on the numerous challenges that the federal government faces in ensuring the cybersecurity of the nation and have made recommendations aimed at addressing these challenges. This appendix identifies prior GAO products that address each of the four challenge areas and associated critical actions.

Challenge 1:

Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight

Key reports related to this challenge area and associated critical actions include:

Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace

 1	 2	 3	 4	 5	 6
-------	-------	-------	-------	-------	-------

Mitigate global supply chain risks

 7	 8	 9	 10	 11
-------	-------	-------	--------	--------

Address cybersecurity workforce management challenges

 12	 13	 14	 15
--------	--------	--------	--------

Bolster the security of emerging technologies

 16	 17
--------	--------

 18	 19	 20	 21	 22
--------	--------	--------	--------	--------

Challenge 2:

Securing Federal Systems and Information

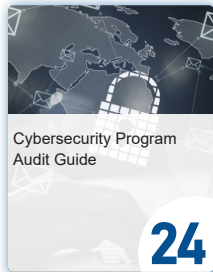
Key reports related to this challenge area and associated critical actions include:

Improve the implementation of government-wide cybersecurity initiatives



Cybersecurity: OMB Should Improve Information Security Performance Metrics

23



Cybersecurity Program Audit Guide

24



Cloud Computing: Federal Agencies Face Four Challenges

25



Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes...

26



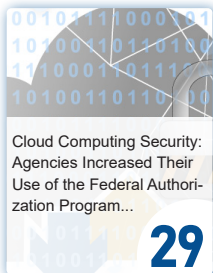
Cybersecurity: OMB Should Update Inspector General Reporting Guidance to Increase Rating Consistency...

27



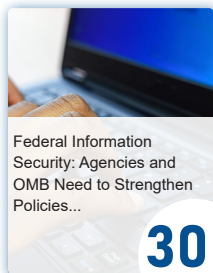
Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network...

28



Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program...

29



Federal Information Security: Agencies and OMB Need to Strengthen Policies...

30

Address weaknesses in federal agency information security programs



Cloud Security: Selected Agencies Need to Fully Implement Key Practices

31



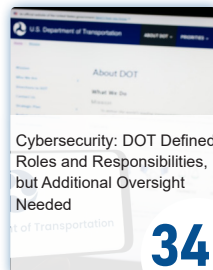
Nuclear Security: DOE Should Take Actions to Fully Implement Insider Threat Program

32



Cybersecurity: State Needs to Expeditiously Implement Risk Management and Other Key Practices

33



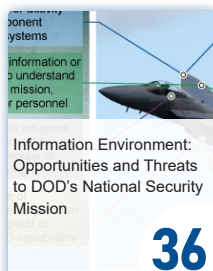
Cybersecurity: DOT Defined Roles and Responsibilities, but Additional Oversight Needed

34



Cybersecurity: Secret Service Has Made Progress Toward Zero Trust Architecture, but Work Remains

35



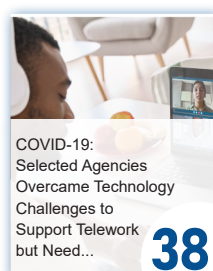
Information Environment: Opportunities and Threats to DOD's National Security Mission

36



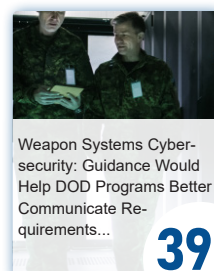
Cybersecurity: NIH Needs to Take Further Actions to Resolve Control Deficiencies and Improve Its Program

37



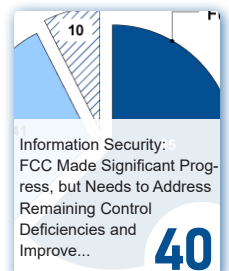
COVID-19: Selected Agencies Overcame Technology Challenges to Support Telework but Need...

38



Weapon Systems Cybersecurity: Guidance Would Help DOD Programs Better Communicate Requirements...

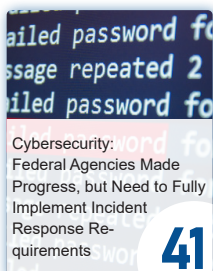
39



Information Security: FCC Made Significant Progress, but Needs to Address Remaining Control Deficiencies and Improve...

40

Enhance the federal response to cyber incidents



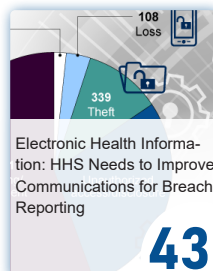
Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements

41



DOD Cybersecurity: Enhanced Attention Needed to Ensure Cyber Incidents Are Appropriately Reported and Shared

42



Electronic Health Information: HHS Needs to Improve Communications for Breach Reporting

43



Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents

44

Challenge 3:

Protecting the Cybersecurity of Critical Infrastructure

Key reports related to this challenge area and associated critical action include:

Strengthen the federal role in protecting the cybersecurity of critical infrastructure

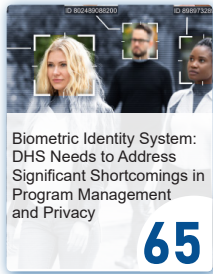
<p>Cybersecurity: Improvements Needed in Addressing Risks to Operational Technology</p> 45	<p>Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support</p> 46	<p>Medical Device Cybersecurity: Agencies Need to Update Agreement to Ensure Effective Coordination</p> 47	<p>Federal Grants: Numerous Programs Provide Cybersecurity Support to State, Local, Tribal, and Territorial Governments</p> 48	<p>Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods</p> 49	<p>Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement...</p> 50
<p>Critical Infrastructure: Actions Needed to Better Secure Internet-Connected Devices</p> 51	<p>Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure</p> 52	<p>Critical Infrastructure Protection: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity</p> 53	<p>Ransomware: Federal Agencies Provide Useful Assistance but Can Improve Collaboration</p> 54	<p>Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks</p> 55	<p>Cybersecurity: Internet Architecture is Considered Resilient, but Federal Agencies Continue to Address Risks</p> 56
<p>Critical Infrastructure Protection: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing</p> 57	<p>Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance</p> 58	<p>Defense Contractor Cybersecurity: Stakeholder Communication and Performance Goals Could Improve Certification Framework</p> 59	<p>Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector</p> 60	<p>Critical Infrastructure Protection: Education Should Take Additional Steps to Help Protect K-12 Schools from Cyber Threats</p> 61	<p>Critical Infrastructure Protection: TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses</p> 62
<p>Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks</p> 63	<p>Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts</p> 64				

Challenge 4:

Protecting Privacy and Sensitive Data

Key reports related to this challenge area and associated critical actions include:

Improve federal efforts to protect privacy and sensitive data



Biometric Identity System: DHS Needs to Address Significant Shortcomings in Program Management and Privacy

65



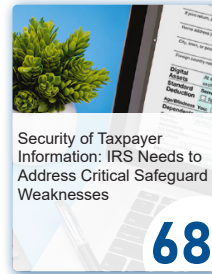
Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties

66



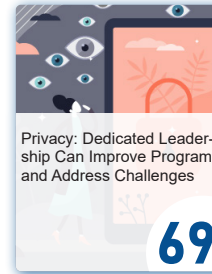
Homeland Security: Office of Intelligence and Analysis Should Improve Privacy Oversight and Assessment of Its Effectiveness

67



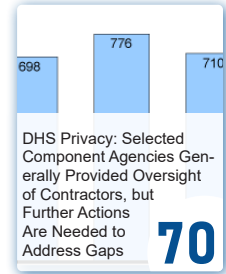
Security of Taxpayer Information: IRS Needs to Address Critical Safeguard Weaknesses

68



Privacy: Dedicated Leadership Can Improve Programs and Address Challenges

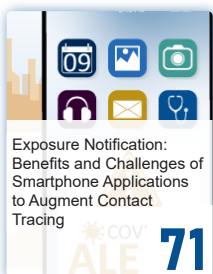
69



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

70

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



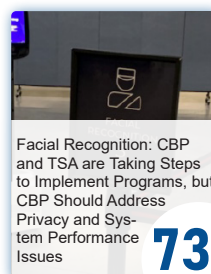
Exposure Notification: Benefits and Challenges of Smartphone Applications to Augment Contact Tracing

71



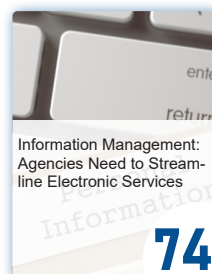
Information Security and Privacy: HUD Needs a Major Effort to Protect Data Shared with External Entities

72



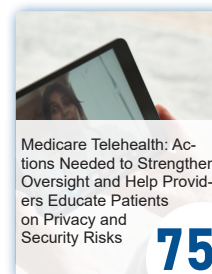
Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues

73



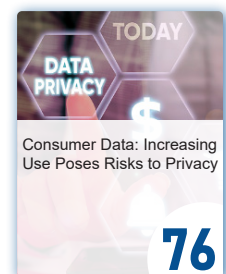
Information Management: Agencies Need to Streamline Electronic Services

74



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

75



Consumer Data: Increasing Use Poses Risks to Privacy

76



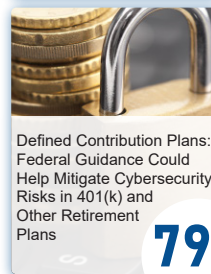
Privacy: Federal Financial Regulators Should Take Additional Actions to Enhance Their Protection of Personal Information

77



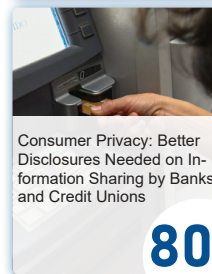
Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks

78



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

79



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

80

Sources: Images: (1, 3, 5, 13, 56) VideoFlow/stock.adobe.com, (2, 6, 8, 10, 28, 30, 37, 61, 64, 67, 72, 77, 80) GAO file photo, (4) denisismagilov/stock.adobe.com, (7, 26, 42, 62) Maksim Kabakou/stock.adobe.com, (9) Kannapat/stock.adobe.com, (11) weerapat1003/stock.adobe.com, (12) snowing12/stock.adobe.com, (14) Andrey Popov/stock.adobe.com, (15) Executive Office of the President, (16) putilov_denis/stock.adobe.com, (17) Larry/stock.adobe.com, DanRentea/stock.adobe.com, (18) Mysterylab/stock.adobe.com, (19, 51) metamorworks/stock.adobe.com, (20, 36) GAO analysis of Department of Defense (DOD) information; Thaut Images/stock.adobe.com and U.S. Airforce/Staff Sgt. E. Nuñez (photos), (21) GAO analysis of Ericsson data, (22) GAO analysis of Congressional Research Service data, (23, 27, 44, 48) Alex/stock.adobe.com, (24) Who is Danny/stock.adobe.com; marinashvchenko/stock.adobe.com, (25, 39, 59) Gorodenkoff/stock.adobe.com, (29) GAO (illustration), (31) FAMILY STOCK/stock.adobe.com, (32) Parradee/stock.adobe.com, (33) kras99/stock.adobe.com (background); Nicole/stock.adobe.com (sign); Department of State (logo), (34) Timon/stock.adobe.com, (35) ArtemisDiana/stock.adobe.com, (38, 75) insta_photos/stock.adobe.com, (40) GAO analysis of Federal Communications Commission data, (41) 123tin/stock.adobe.com, (43) GAO analysis of Department of Health and Human Services' January 2022 data; bearsky23/stock.adobe.com; Chor muang/stock.adobe.com, (45) Quality Stock Arts/stock.adobe.com, (46, 54) alexlrx/stock.adobe.com, (47) nimon_t/stock.adobe.com, (49) Song_about_summer/stock.adobe.com, (50) Vadim/stock.adobe.com, (52) United States Coast Guard, (53) GAO analysis of federal and nonfederal documents; marinashvchenko/stock.adobe.com (images), (55, 58) Murrstock/stock.adobe.com, (57) Department of Homeland Security, (60) TebNad/stock.adobe.com, (63) GAO analysis of Federal Aviation Administration and industry documentation, (65) Pond5, (66) Ilya/stock.adobe.com, (68) Constantine/stock.adobe and Internal Revenue Service, as modified by GAO, (69) VectorMine/stock.adobe.com, (70) GAO analysis of Department of Homeland Security provided data, (71, 73) GAO, (74) tashatvango/stock.adobe.com, (76) Artur/stock.adobe.com, (78) GAO photo illustration; Andrey Popov and polkadot on stock.adobe.com, (79) Jakub Krechowicz/stock.adobe.com.

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.

[Sarah Kaczmarek](#), Acting Managing Director, Public Affairs, (202) 512-4800

[A. Nicole Clowers](#), Managing Director, Congressional Relations, (202) 512-7114

Contributors: Lee McCracken (Assistant Director), Javier Irizarry (Analyst-In-Charge), Chris Businsky, Jillian Clouse, Rebecca Eyster, Corwin Hayward, Ceara Lance, Ashley Mattson, Andrew Stavisky, Adam Vodraska, and Marshall Williams, Jr. made key contributions to this report.

Sources (cover photo and section headers): Dorido/stock.adobe.com (background); Who is Danny/stock.adobe.com (laptop); Gorodenkoff/stock.adobe.com (people); metamorworks/stock.adobe.com (city); Monster Zstudio/stock.adobe.com (phone).