

HIGH-RISK SERIES

Critical Actions Needed to Urgently Address IT Acquisition and Management Challenges

Report to Congressional Committees

January 2025

GAO-25-107852

United States Government Accountability Office

Accessible Version



GAO Highlights For more information, contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov.

Highlights of [GAO-25-107852](#), a report to congressional committees

January 2025

HIGH-RISK SERIES

Critical Actions Needed to Urgently Address IT Acquisition and Management Challenges

Why GAO Did This Study

Federal agencies rely extensively on IT to carry out operations and fulfill their missions. Each year, the federal government invests more than \$100 billion on IT. However, for several decades, GAO has reported that federal IT investments too frequently fail or incur cost overruns and schedule slippages while contributing little to mission-related outcomes. Because of these challenges, GAO added the federal government's management of IT acquisitions and operations to its high-risk list as a government-wide challenge in 2015 and continues to designate it as a high-risk area.

Over time, this high-risk area has become increasingly more complex as technologies have matured and evolved. In addition, as technologies have changed, the skills needed to manage them have also changed.

This report provides an update to the IT acquisitions and operations high-risk area. To do so, GAO identified three key IT acquisition and management areas in which federal agencies face continued challenges and nine critical actions that the agencies need to take to address those challenges. GAO reviewed its prior reports and prioritized reports that were government-wide and had open recommendations, among other things. Based on the results of its work, GAO is renaming this high-risk area to *Improving IT Acquisitions and Management*.




What GAO Recommends

GAO has made over 1,800 recommendations to agencies aimed at improving their management of IT since 2010. As of January 2025, 463 had not been implemented.

What GAO Found

GAO has identified three major IT acquisition and management challenges: (1) strengthening oversight and management of IT portfolios, (2) implementing mature IT acquisition and development practices, and (3) building federal IT capacity and capabilities. To address these challenges, it has identified nine critical actions that the federal government urgently needs to take.

Nine Critical Actions Needed to Address Three Major IT Acquisition and Management Challenges

		
<p>Strengthening oversight and management of IT portfolios</p>	<p>Implementing mature IT acquisition and development practices</p>	<p>Building federal IT capacity and capabilities</p>
<p>1 Improve the effectiveness of key IT leadership positions, including the Federal Chief Information Officer (CIO), agency CIOs, and agency chief artificial intelligence officers.</p>	<p>5 Improve implementation of leading IT acquisition and development practices to effectively plan and manage IT project costs, schedules, risks, requirements, and testing.</p>	<p>7 Address workforce management challenges for the technically-capable workforce.</p>
<p>2 Enhance agency efforts to strategically plan for and manage portfolios of IT systems, applications, and software licenses, and to manage existing IT system operations.</p>	<p>6 Strengthen the planning and management of cloud services, supply chains, and telecommunications services.</p>	<p>8 Improve federal customer experience for digital services.</p>
<p>3 Improve the monitoring of, and transparency into, the performance of IT investments.</p>		<p>9 Ensure effective management of emerging technologies.</p>
<p>4 Strengthen planning and budgeting for the acquisition of IT systems and services.</p>		

Sources: GAO; ximich_natali/stock.adobe.com (top left); BestCam/peopleimages.com/stock.adobe.com (center); suththirat/stock.adobe.com (top right); 32 pixels/stock.adobe.com (all icons). | GAO-25-107852

GAO has made over 1,800 recommendations to the Office of Management and Budget (OMB) and federal agencies aimed at improving their management of IT. However, many of these recommendations have not been implemented and many agencies continue to be challenged in effectively acquiring IT and managing IT projects. Of the 1,881 recommendations made since 2010 related to this high-risk area, 463 had not been implemented as of January 2025. GAO has also designated 69 as priority recommendations and, as of January 2025, 32 had not been implemented. Urgent actions are needed to address the ongoing challenges that the government faces in effective and efficient IT acquisition and management. Until OMB and federal agencies take the critical actions identified, they will continue to struggle with IT acquisitions that fail to consistently deliver capabilities in a timely manner, incur cost overruns and/or schedule slippages, and contribute little to mission-related outcomes.

Contents

GAO Highlights For more information, contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov.

Why GAO Did This Study i

What GAO Recommends i

What GAO Found i

Letter	1
Background	3
Nine Critical Actions Needed to Address Major IT Acquisition and Management Challenges	7
Strengthening Oversight and Management of IT Portfolios	9
Implementing Mature IT Acquisition and Development Practices	34
Building Federal IT Capacity and Capabilities	54
Continued Implementation of Our Recommendations Is Needed to Address IT Acquisition and Management Weaknesses	65

Appendix I: Prior GAO Work on IT Acquisitions and Management	67
Challenge 1: Strengthening Oversight and Management of IT Portfolios	67
Challenge 2: Implementing Mature IT Acquisition and Development Practices	68
Challenge 3: Building Federal IT Capacity and Capabilities	69

Appendix II: Accessible Data	71
------------------------------	----

Tables

Table 1: GAO's Ongoing Work Related to the Strengthening Oversight and Management of IT Portfolios Challenge Area (as of December 2024)	33
Table 2: GAO's Ongoing Work Related to the Implementing Mature IT Acquisition and Development Practices Challenge Area (as of December 2024)	52
Table 3: GAO's Ongoing Work Related to the Building Federal IT Capacity and Capabilities Challenge Area (as of December 2024)	65

Figures

Nine Critical Actions Needed to Address Three Major IT Acquisition and Management Challenges	ii
Figure 1: Ratings for Improving the Management of IT Acquisitions and Operations, as of April 2023	6
Figure 2: Nine Critical Actions Needed to Address Three Major IT Acquisition and Management Challenges	8
Figure 3: Extent to Which 24 Agencies' Policies Addressed the Role of Their Chief Information Officers (CIO), Presented from Most Addressed to Least Addressed Area (as of August 2018)	12

Figure 4: Extent of Sharing of IT Management Area Responsibilities Reported by 71 Private Sector Chief Information Officer (CIO) Respondents (as of September 2022) 13

Figure 5: Extent to Which the Office of Management and Budget (OMB) Followed Statutory Requirements (as of November 2024) 15

Figure 6: Assessment of Whether Agencies Fully Met Practices for Establishing Complete Software Application Inventories (as of September 2016) 17

Figure 7: CIO Council’s Six-step Application Rationalization Process Outlined in *The Application Rationalization Playbook: An Agency Guide to Portfolio Management* 18

Figure 8: Number of Department of Health and Human Services Systems Supporting Pandemic Public Health Preparedness and Response, per component (as of September 2024) 19

Figure 9: Software Vendors with the Highest Amounts Paid Reported by Agencies for Fiscal Year 2021 21

Figure 10: Extent to Which the Office of Management and Budget’s (OMB) Plans Addressed Elements of the Technology Business Management Taxonomy Version 3.0 (as of September 2022) 23

Figure 11: Department of Defense Air Force Strategic Automated Command and Control System 24

Figure 12: GAO Assessment of the Internal Revenue Service’s (IRS) Modernization Plans (as of August 2022) 25

Figure 13: Results of GAO Survey on Satisfaction with Digital Services Projects (as of August 2016) 26

Figure 14: Inflation Reduction Act Strategic Operating Plan Transformation Objectives (as of April 2023) 27

Figure 15: Unemployment Insurance System Modernization Timeline for Selected States (as of February 2023) 28

Figure 16: Evaluation of Selected Departments’ Policies and Procedures for Key IT Budgeting Requirements (as of November 2018) 30

Figure 17: The Department of Veterans Affairs’ Documented Chief Information Officer Approvals for Selected Fiscal Year 2021 IT Contract Actions (as of March 2023) 32

Figure 18: Extent to Which the Small Business Administration (SBA) Met Selected IT Management Areas for the Unified Certification Platform Modernization (as of November 2024) 36

Figure 19: Examples of Technical Issues Affecting the Rollout of the Free Application for Federal Student Aid (FAFSA) (as of December 2024) 37

Figure 20: Decline in Free Application for Federal Student Aid (FAFSA) Submissions, Current Application Cycle Compared to Prior Year 37

Figure 21: Total Number of Calls to Education’s Call Center, from January 1, 2024, to May 31, 2024 38

Figure 22: Expected Modernization Completion Dates for 10 of the Most Critical and At-Risk Federal Aviation Administration (FAA) Air Traffic Control Systems (as of September 2024) 40

Figure 23: Extent to Which the Federal Aviation Administration (FAA) Followed Leading Program Management Practices in Managing the Next Generation Air Transportation System (NextGen) Program (as of November 2023) 41

Figure 24: Examples of the Issues Encountered by Thrift Savings Plan (TSP) Participants After System Deployment in 2022 42

Figure 25: Timeline of Homeland Advanced Recognition Technology (HART) Acquisition Program Baselines and Breaches (as of November 2024) 44

Figure 26: Status of Required Governance Reviews and Key Documentation for the Farm Production and Conservation's Farmers.gov program (as of April 2021) 45

Figure 27: Comparison of Agile and Waterfall Methods for Developing Software 46

Figure 28: Extent to Which Federal Agencies' Guidance Addressed the Five Procurement-Related Cloud Computing Requirements (as of July 2024) 48

Figure 29: Extent to Which the 23 Civilian Chief Financial Officers Act Agencies Implemented Information and Communications Technology (ICT) Supply Chain Risk Management Practices (as of December 2020) 49

Figure 30: Extent to Which 10 Selected Agencies Fully Implemented 16 Telecommunications Transition Planning Practice Activities 51

Figure 31: Agencies' Overall Implementation of the Key IT Workforce Planning Activities (as of May 2019) 56

Figure 32: National Institutes of Health's (NIH) Implementation of Key Activities for Data Science Workforce Planning (as of June 2023) 57

Figure 33: Extent to Which 24 Agencies' Submitted Reports in 2022 and 2023 Addressed the Eight Modernization Requirements from the 21st Century Integrated Digital Experience Act 59

Figure 34: Demographics of Direct File Taxpayers During the 2024 Filing Season 61

Figure 35: Artificial Intelligence (AI) Use Case Application Areas (as of December 2023) 62

Figure 36: Assessment of the Extent to Which the Federal Government's Quantum Cybersecurity Strategy Documents Addressed GAO's Desirable Characteristics of a National Strategy (as of November 2024) 64

Abbreviations

21st Century IDEA	21st Century Integrated Digital Experience Act
AI	artificial intelligence
ATC	air traffic control
CFO	chief financial officer
CIO	chief information officer
DHS	Department of Homeland Security
DOD	Department of Defense
DOT	Department of Transportation
EIS	Enterprise Infrastructure Solutions
FAA	Federal Aviation Administration
FAFSA	Free Application for Federal Student Aid
FITARA	Federal IT Acquisition Reform Act
FPAC	Farm Production and Conservation
FRTIB	Federal Retirement Thrift Investment Board
GSA	General Services Administration
HART	Homeland Advanced Recognition Technology
HHS	Department of Health and Human Services
ICT	information and communications technology
IRS	Internal Revenue Service
NextGen	Next Generation Air Transportation System
NIH	National Institutes of Health
OMB	Office of Management and Budget
SBA	Small Business Administration
TSP	Thrift Savings Plan
UI	unemployment insurance
USDA	U.S. Department of Agriculture
USDS	U.S. Digital Service
VA	Department of Veterans Affairs

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



January 23, 2025

The Honorable Rand Paul, M.D.
Chairman
The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable James Comer
Chairman
The Honorable Gerald E. Connolly
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

Federal agencies rely extensively on IT to carry out operations and meet their missions. As part of this, federal IT systems provide essential services that are critical to the health, economy, and defense of the nation. Each year, the federal government invests more than \$100 billion on IT investments.

However, for several decades, we have reported that federal IT investments too frequently fail or incur cost overruns and schedule slippages while contributing little to mission-related outcomes. To improve the management of IT, Congress enacted the Federal IT Acquisition Reform Act (FITARA) in December 2014.¹ This act enables Congress to monitor covered agencies' efforts to manage their IT acquisitions and hold them accountable for reducing duplication and achieving cost savings.²

In the decade since FITARA was passed, sustained congressional focus on the implementation of the act led to improvement in agencies' efforts to acquire and manage IT. However, additional work is needed to institutionalize agency processes established in response to FITARA, as well as tackle remaining challenges that hamper efficient and effective acquisition and management of the government's IT assets. Such challenges include a lack of disciplined and effective management in areas such as project planning, requirements definition, and program oversight.

Because of these longstanding challenges, we added the federal government's management of IT acquisitions and operations to our high-risk list as a government-wide challenge in 2015.³ Underscoring the significance of

¹Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438-3450 (Dec. 19, 2014).

²The provisions apply to the agencies covered by the Chief Financial Officers Act of 1990, 31 U.S.C. § 901(b). These agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Justice, Labor, State, the Interior, the Treasury, Transportation, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development. FITARA has limited applicability to the Department of Defense.

³GAO, *High-Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: Feb. 11, 2015).

the issues agencies face in effectively acquiring and managing IT, we have continued to designate IT acquisitions and operations as a high-risk area in each of our high-risk series updates since then.⁴

Over time, this high-risk area has become increasingly more complex as technologies have matured and evolved. In addition, as technologies have changed, the skills needed to manage them have also changed. Further, critical government systems have continued to age and either become obsolete or extremely costly to maintain.

This report provides an update to the IT acquisitions and operations high-risk area by identifying actions that the federal government and other entities need to take to address IT acquisition and management challenges. To do so, this report reflects work we conducted since the prior high-risk update was issued in April 2023, among other things. We also plan to issue an updated assessment of this high-risk area in February 2025. Based on the results of our work and the three key challenges that we identified (discussed in more detail later), we are changing the name of this area from *Improving the Management of IT Acquisitions and Operations* to *Improving IT Acquisitions and Management*.

We performed this work on the initiative of the Comptroller General to identify and describe the key challenges that the federal government faces in effectively managing its IT acquisitions and the critical actions it needs to take to address those challenges.

To do so, we first analyzed the topics and open recommendations discussed in previous updates to the IT acquisitions and operations area in our high-risk reports. From these topics, we developed an initial list of critical actions that federal agencies need to take to improve their IT acquisitions and management. We then analyzed these critical actions and grouped them into key challenge areas.

To validate the accuracy and completeness of the identified challenge areas and critical actions, we solicited input from internal experts and stakeholders responsible for and involved in our previous and ongoing work assessing the Office of Management and Budget's (OMB) and federal agencies' IT acquisition and management efforts. Based on these actions, we identified three key IT acquisition and management areas in which federal agencies face continued challenges and nine critical actions that the agencies need to take to address those challenges.

To identify related GAO reports for potential inclusion in this report, we identified all reports related to this high-risk area that have been issued since fiscal year 2010. In selecting reports for inclusion, we prioritized reports that met one or more of the following criteria: (1) were government-wide, (2) pertained to multiple agencies, (3) had open priority recommendation(s), or (4) had significant attention from Congress or the Comptroller

⁴GAO, *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). 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. We address the cybersecurity-related challenges that agencies face in a separate high-risk area called *Ensuring the Cybersecurity of the Nation*.

General.⁵ We also identified and selected ongoing engagements related to this high-risk area that planned to publicly release a product by December 2024 and met one or more of the previous criteria.

We validated the list of selected reports with internal experts and stakeholders. For the selected reports, we summarized the key findings and open recommendations.⁶ We also identified our ongoing work related to each challenge area.

We conducted this work from September 2024 to January 2025 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.

Background

The federal government invests more than \$100 billion on IT investments each year. A large majority of these investments are to support the operation and maintenance of existing IT systems—such as those that support tax filings, Census survey information, and veterans' health records. These investments also support system development and activities, including software upgrades, replacement of legacy IT, and the adoption of new technologies.

Notwithstanding the billions of dollars spent annually, federal IT investments too frequently fail to deliver capabilities in a timely manner, incur cost overruns, and/or experience schedule slippages while contributing little to mission-related outcomes. These investments often lack disciplined and effective management in areas such as project planning, requirements definition, and program oversight and governance. In many instances, agencies have not consistently applied best practices that are critical to successfully acquiring IT investments. Federal IT projects have also failed due to a lack of oversight and governance. Executive-level governance and oversight across the government has often been ineffective, specifically from chief information officers (CIO).

Over the past two decades, the executive branch has undertaken multiple initiatives in an attempt to address the persistent issues with IT acquisitions and management. For example,

⁵Priority recommendations are 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.

⁶For more information about how we conducted those reviews, refer to the objective, scope, and methodology sections within the related reports.

- In June 2009, OMB launched the IT Dashboard.⁷ It is intended to provide transparency for IT investments to facilitate public monitoring of government operations and accountability for investment performance by the Federal CIO who oversees them.⁸ Among other things, agencies are to submit CIO ratings for major investments. According to OMB's instructions, these ratings should reflect the level of risk facing an investment relative to that investment's ability to accomplish its goals.⁹
- In January 2010, OMB began conducting TechStat sessions. OMB envisioned these sessions as face-to-face, evidence-based reviews of an at-risk IT investment. The sessions were an effort to turnaround, halt, or terminate IT projects that were failing or not producing results. At the time, OMB used CIO ratings from the IT Dashboard, among other sources, to select at-risk investments for the TechStats. OMB conducted TechStats from 2010 through 2011 and subsequently required federal agencies to hold them, too.¹⁰
- In December 2010, the White House issued a 25-point plan intended to reform federal IT management.¹¹ Among other things, the document directed agencies to reform and strengthen their investment review boards and begin holding TechStats at the department and bureau levels.
- In March 2012, recognizing the proliferation of duplicative and low-priority IT investments within the federal government and the need to drive efficiency, OMB launched the PortfolioStat initiative.¹² This required agency CIOs to conduct annual agency-wide reviews of their IT portfolios to, among other things, assess the current maturity of their IT portfolio management processes, reduce duplication, demonstrate how investments align with the agencies' missions, and achieve savings by identifying opportunities to consolidate investments or move to shared services.
- In 2014, the General Services Administration (GSA) established 18F, a team that provides IT services (e.g., develop websites and provide software development training) to federal agencies on a reimbursable basis. Also in 2014, the President established the U.S. Digital Service within OMB. Similar to 18F, the U.S. Digital Service aims to improve the most important public-facing federal digital services.¹³

Despite these initiatives aimed at improving federal IT, implementation has been inconsistent and significant issues persisted. Recognizing the severity of these issues, in December 2014, Congress enacted federal IT acquisition reform legislation, commonly referred to as FITARA.¹⁴ This act enables Congress to monitor

⁷See IT Dashboard, <https://itdashboard.gov/> (accessed December 19, 2024).

⁸In March 2009, the President designated the Administrator of the Office of Electronic Government within OMB as the Federal CIO. Among other things, the President assigned the Federal CIO responsibility for directing the policy and strategic planning of federal IT investments and overseeing federal technology spending. OMB now refers to the Office of Electronic Government as the Office of the Federal CIO.

⁹According to the IT Dashboard, each agency CIO is to rate investments based on their best judgment, using a set of pre-established criteria, including risk management, requirements management, contractor oversight, historical performance, human capital, and any other factors the CIO deems important to forecasting future success.

¹⁰The White House, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, D.C.: Dec. 9, 2010) and *Chief Information Officer Authorities M-11-29* (Washington, D.C.: Aug. 8, 2011). OMB's M-11-29 was rescinded by M-17-26 on June 15, 2017.

¹¹The White House, *25 Point Implementation Plan* (Washington, D.C.: Dec. 9, 2010).

¹²OMB, *Implementing PortfolioStat*, M-12-10 (Washington, D.C.: Mar. 30, 2012).

¹³OMB defines digital services as the delivery of digital information (data or content) and transactional services (e.g., online forms and benefits applications) across a variety of platforms, devices, and delivery mechanisms (e.g., websites, mobile applications, and social media).

¹⁴Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438-3450 (Dec. 19, 2014).

covered agencies' efforts and hold them accountable for reducing duplication and achieving cost savings. Among other things, the act strengthens the authority of CIOs to provide needed direction and oversight of covered agencies' IT acquisitions.¹⁵ In June 2015, OMB released guidance describing how agencies are to implement the act.¹⁶ The guidance emphasized the need for CIOs to have full accountability for IT acquisition and management decisions.

In December 2017, Congress also enacted legislation that established a new funding mechanism to improve, retire, or replace existing IT systems. The provisions of the National Defense Authorization Act for Fiscal Year 2018, commonly referred to as the Modernizing Government Technology Act,¹⁷ established the Technology Modernization Fund within the Department of the Treasury.¹⁸ By using this fund to improve, retire, or replace aging legacy systems, agencies could improve the effectiveness of federal IT systems. The act also established a Technology Modernization Board, which is chaired by the Federal CIO. The board evaluates the proposals submitted by agencies seeking funding to replace legacy systems or acquire new systems, recommends the funding of modernization projects to the Administrator of General Services, and monitors the progress and performance of approved projects.

Managing IT Acquisitions and Operations Included on GAO's High-Risk List Since 2015

Because of the longstanding challenges in the federal government's management of IT, we added the management of IT acquisitions and operations as a government-wide challenge on our high-risk list in 2015.¹⁹ We have also continued to designate it as a high-risk area in each of our high-risk series updates since then.²⁰

Our experience has shown that the key elements needed to make progress toward being removed from the high-risk list are top-level attention by the administration and agency leaders grounded in the five criteria for removal, as well as any needed congressional action.

The five criteria for removal that we identified in November 2000 are as follows:²¹

- **Leadership Commitment.** Demonstrated strong commitment and top leadership support.
- **Capacity.** The agency has the capacity (i.e., people and resources) to resolve the risk(s).

¹⁵These provisions, codified at 40 U.S.C. § 11319(b), apply to agencies covered by the Chief Financial Officers Act of 1990, 31 U.S.C. § 901(b)), with the exception of the Department of Defense.

¹⁶OMB, *Management and Oversight of Federal Information Technology*, M-15-14 (Washington, D.C.: June 10, 2015).

¹⁷Modernizing Government Technology Act provisions of the National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, div. A, title X, subtitle G, 131 Stat. 1283, 1586-1594 (2017).

¹⁸The act established a fund in the Department of the Treasury to provide transfers of amounts to agencies to help them improve, retire, or replace existing federal IT systems.

¹⁹GAO, *High-Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: Feb. 11, 2015).

²⁰GAO, *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).

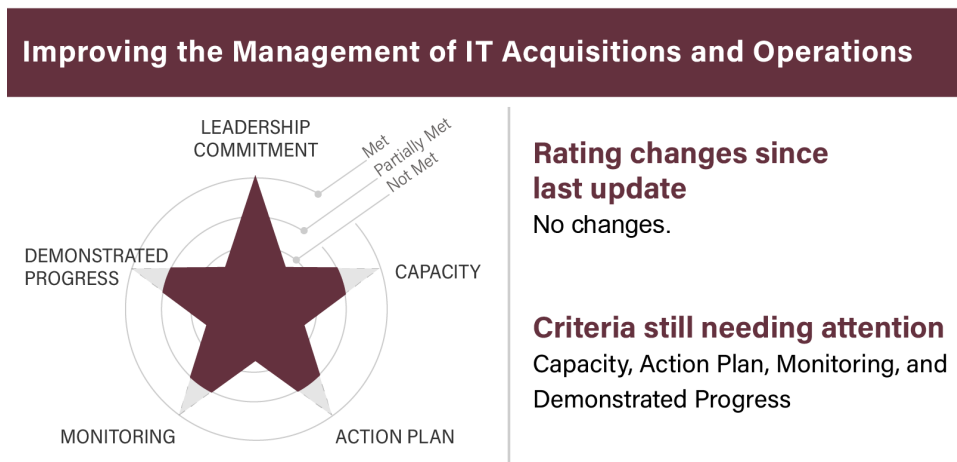
²¹GAO, *Determining Performance and Accountability Challenges and High Risks*, [GAO-01-159SP](#) (Washington, D.C.: November 2000).

- **Action Plan.** A corrective action plan exists that defines the root cause, solutions, and provides for substantially completing corrective measures, including steps necessary to implement solutions we recommended.
- **Monitoring.** A program has been instituted to monitor and independently validate the effectiveness and sustainability of corrective measures.
- **Demonstrated Progress.** Ability to demonstrate progress in implementing corrective measures and in resolving the high-risk area.

These five criteria form a road map for efforts to improve and ultimately address high-risk issues. Addressing some of the criteria leads to progress, while satisfying all of the criteria is central to removal from the list.

In our April 2023 high-risk report, the federal government's efforts to improve its management of IT acquisitions and operations had fully met one of the five criteria for removal from the high-risk list—leadership commitment—and partially met the other four, as shown in figure 1.²² However, since that report, OMB has not maintained its level of leadership commitment to ensure that agencies improve IT acquisitions and management. In addition, agencies have not maintained efforts to develop and implement action plans to address IT management issues. We plan to update our assessment of this high-risk area against the five criteria in February 2025.

Figure 1: Ratings for Improving the Management of IT Acquisitions and Operations, as of April 2023



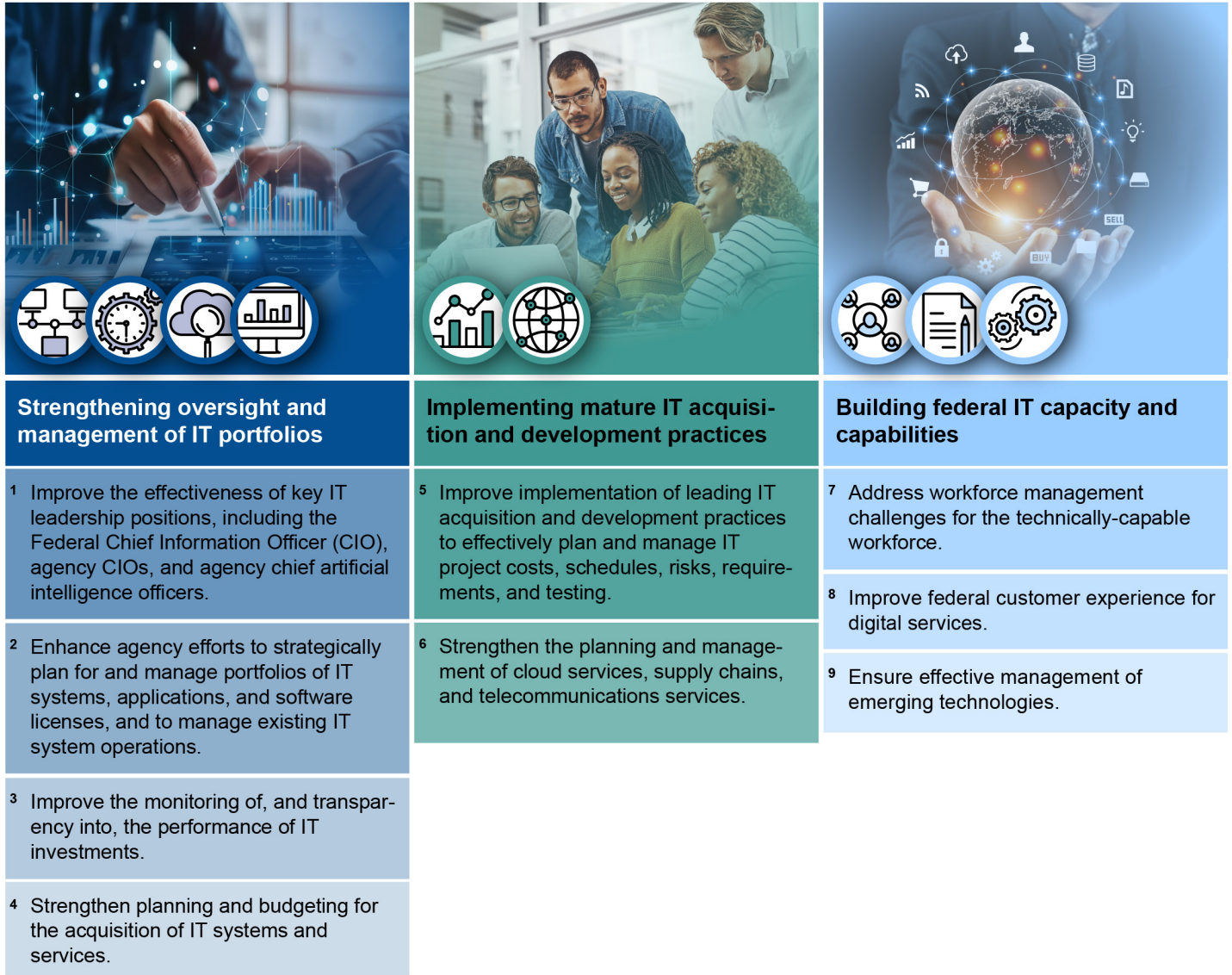
Source: GAO. | GAO-25-107852

²²GAO-23-106203.

Nine Critical Actions Needed to Address Major IT Acquisition and Management Challenges

Based on our prior work, we have identified three major IT acquisition and management challenges: (1) strengthening oversight and management of IT portfolios, (2) implementing mature IT acquisition and development practices, and (3) building federal IT capacity and capabilities. To address these challenges, we have identified nine critical actions that the federal government needs to take (see figure 2). These three challenges and nine critical actions are discussed in more detail following the figure.

Figure 2: Nine Critical Actions Needed to Address Three Major IT Acquisition and Management Challenges



Sources: GAO; ximich_natali/stock.adobe.com (top left); BestCam/peopleimages.com/stock.adobe.com (center); suththirat/stock.adobe.com (top right); 32 pixels/stock.adobe.com (all icons). | GAO-25-107852



Strengthening Oversight and Management of IT Portfolios

The federal government should:

- Improve the effectiveness of key IT leadership positions, including the Federal Chief Information Officer (CIO), agency CIOs, and agency chief artificial intelligence officers.
- Enhance agency efforts to strategically plan for and manage portfolios of IT systems, applications, and software licenses, and to manage existing IT system operations.
- Improve the monitoring of, and transparency into, the performance of IT investments.
- Strengthen planning and budgeting for the acquisition of IT systems and services.

Strengthening Oversight and Management of IT Portfolios

Overview

Over the years, Congress has enacted various laws to improve the government's oversight and management of IT. For example, the Clinger-Cohen Act of 1996 required agency heads to designate CIOs to lead reforms that would help better manage technology spending, among other things.²³ In addition, FITARA, enacted in December 2014, strengthened the role of covered agency CIOs in managing IT and includes various requirements for OMB and agencies to perform annual IT portfolio reviews.²⁴ However, agencies have continued to be challenged in providing effective oversight and management of their IT portfolios. To address this challenge, it is critical that agencies: (1) improve the effectiveness of key IT leadership positions, including the Federal CIO, agency CIOs, and agency chief artificial intelligence (AI) officers; (2) enhance agency efforts to strategically plan for and manage portfolios of IT systems, applications, and software licenses, and to manage existing IT system operations; (3) improve the monitoring of, and transparency into, the performance of IT investments; and (4) strengthen planning and budgeting for the acquisition of IT systems and services.

For more than three decades we have been proponents of having strong agency CIOs and a central federal government CIO in order to address the government's many IT management challenges.²⁵ These positions are vital to achieving better results through IT management. However, we have reported that agency CIO responsibilities have not been fully addressed in agency policies consistent with federal laws and guidance and agency CIOs face numerous challenges that impede their ability to effectively manage IT.²⁶ We have also reported that, because the Federal CIO position is not established in law, its responsibilities are often more limited in key CIO management areas than those of the other types of CIOs.²⁷ In addition to the leadership

²³44 U.S.C. § 3506, 40 U.S.C. §§ 11312 and 11313.

²⁴Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438-3450 (Dec. 19, 2014).

²⁵U.S. General Accounting Office, *Improving Government: Actions Needed to Sustain and Enhance Management Reforms*, [GAO/T-OCG-94-1](#) (Washington, D.C.: Jan. 27, 1994), *Government Reform: Using Reengineering and Technology to Improve Government Performance*, [GAO/T-OCG-95-2](#) (Washington, D.C.: Feb. 2, 1995), and *Government Reform: Legislation Would Strengthen Federal Management of Information and Technology*, [GAO/T-AIMD-95-205](#) (Washington, D.C.: July 25, 1995).

²⁶GAO, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*, [GAO-18-93](#) (Washington, D.C.: Aug. 2, 2018).

²⁷GAO, *Chief Information Officers: Private Sector Practices Can Inform Government Roles*, [GAO-22-104603](#) (Washington, D.C.: Sept. 15, 2022).

provided by agency CIOs and the Federal CIO, OMB recently established a new IT leadership position—the chief AI officer. Specifically, in 2024, OMB issued guidance directing each of the 24 major federal agencies to designate this position, which is to have primary responsibility for coordinating the agency’s use of artificial intelligence.²⁸ However, given the recent establishment of this position, it is unclear how effective it will be.

In addition, annual agency-wide portfolio reviews—including IT systems, applications, and software licenses—are crucial for assessing the performance, cost-effectiveness, and alignment of IT investments with agency missions and goals. By conducting such reviews, agencies can identify areas of duplication within their IT portfolios and develop strategies to streamline operations and optimize resource allocation. However, we have reported that OMB and agencies are not fully following FITARA’s requirements for portfolio management reviews.²⁹ As a result, the federal government may be expending resources on IT investments that could be duplicative or may not fulfill the needs of the government or the public. Moreover, approximately 80 percent of the billions of dollars that the federal government invests in IT each year is reportedly spent on operating and maintaining these systems—many of which are legacy systems (i.e., systems that are outdated or obsolete). Given the magnitude of these investments, it is important that agencies effectively manage their operations and maintenance.³⁰

Further, monitoring and transparency of IT investment performance are critical to identifying poorly performing investments and holding them accountable for their results. By monitoring such performance, agencies can gain the necessary insight to get ahead of critical problems in an investment, turn around underperforming investments, or terminate investments if appropriate. Without such insight into investment performance, agencies are at risk of not being able to properly manage their IT costs, schedule, performance, and security. Moreover, limited insight into the performance of federal IT investments puts hundreds of millions of dollars at risk of mismanagement and potential waste, if any performance problems are not addressed. The executive branch has implemented various initiatives intended to improve the monitoring of IT investments and provide insight into their performance. However, we have reported on numerous instances where agencies need to improve performance measurement and reporting, and address gaps in performance oversight.³¹

Finally, FITARA was intended to strengthen the authority of CIOs to provide needed direction and oversight of covered agencies’ IT budgets. As part of this, FITARA requires the CIOs of major civilian agencies to have a significant role in the decision processes for all annual and multi-year planning and to approve the IT budget requests of the agencies. However, in March 2018—over 3 years after FITARA was enacted—the President’s Management Agenda pointed out that federal executives were challenged by the lack of visibility into, and accuracy of IT spending data.³² Since then, we have also reported on weaknesses in agencies’ processes for

²⁸OMB, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*, M-24-10 (Washington, D.C.: Mar. 28, 2024).

²⁹GAO, *IT Portfolio Management: OMB and Agencies Are Not Fully Addressing Selected Statutory Requirements*, [GAO-25-107041](#) (Washington, D.C.: Nov. 14, 2024).

³⁰Another concern with legacy IT systems is the potential cybersecurity risks they introduce. For example, such systems may have security vulnerabilities or software that is unsupported by the vendor. When computer systems or software are no longer supported, the vendor of the product ceases to provide patches, security fixes, or updates, leaving system vulnerabilities open to exploitation. We monitor the federal government’s efforts to address key cybersecurity challenges facing the nation as part of another critical area on GAO’s High-Risk List.

³¹See, for example, GAO, *Information Technology: IRS Needs to Complete Planning and Improve Reporting for Its Modernization Programs*, [GAO-24-106566](#) (Washington, D.C.: Mar. 19, 2024) and *Unemployment Insurance: DOL Needs to Further Help States Overcome IT Modernization Challenges*, [GAO-23-105478](#) (Washington, D.C.: July 10, 2023).

³²President’s Management Council and Executive Office of the President, *President’s Management Agenda* (Washington, D.C.: Mar. 20, 2018).

developing their IT budgets and instances where agencies procured IT and IT-related assets that were often not approved by their CIOs.³³

What actions should agencies take to improve the effectiveness of key IT leadership positions, including the Federal CIO, agency CIOs, and agency chief artificial intelligence officers?

Federal agencies need to address shortcomings and challenges in implementing CIO responsibilities.

Congress established the CIO position to serve as an agency focal point for IT. Over the past several decades, Congress enacted various laws that established roles and responsibilities for agency CIOs to improve the government's performance in IT and related information management functions. For example, the Clinger-Cohen Act of 1996 required agency heads to designate CIOs to lead reforms that would help control system development risks, better manage technology spending, and achieve measurable improvements in agency performance.³⁴

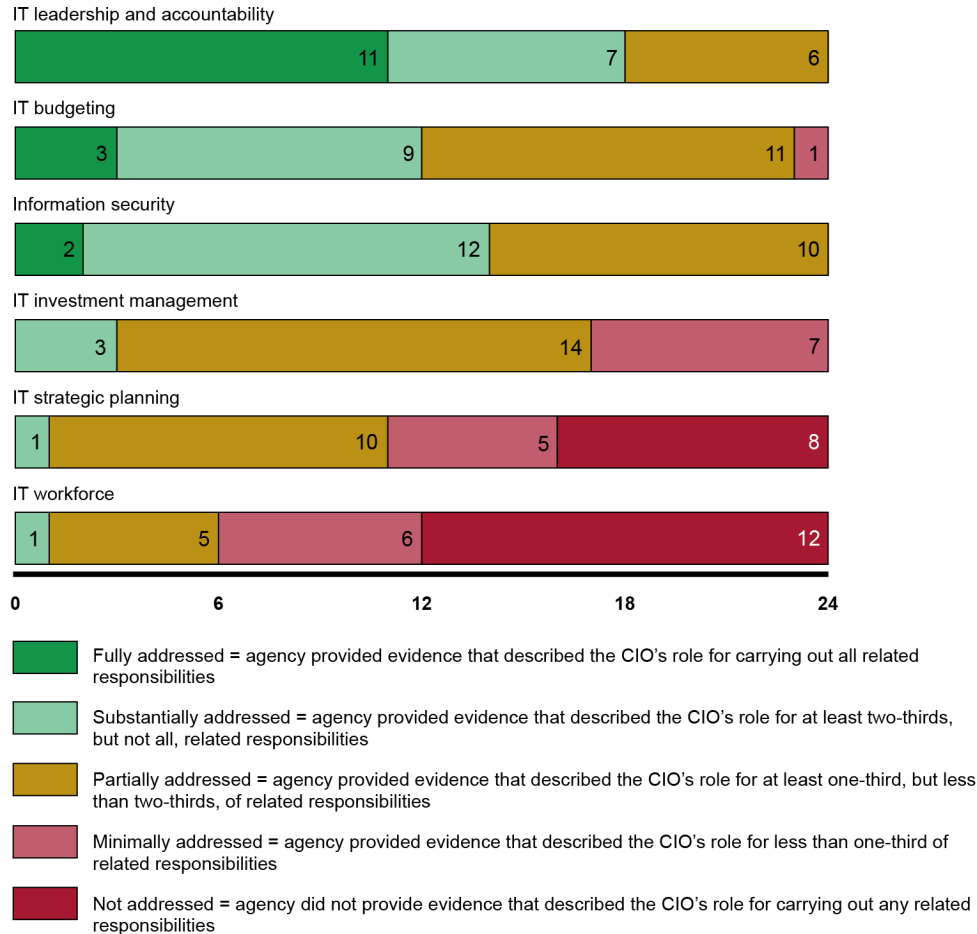
In August 2018, we found that none of the 24 Chief Financial Officers (CFO) Act agencies had policies that fully addressed the role of their CIO consistent with federal laws and guidance.³⁵ In addition, the majority of the agencies did not fully address the role of their CIOs for any of the six key areas that we identified (see figure 3).

³³See, for example, GAO, *IT Management: VA Needs to Improve CIO Oversight of Procurements*, [GAO-23-105719](#) (Washington, D.C.: Mar. 30, 2023).

³⁴44 U.S.C. § 3506, 40 U.S.C. §§ 11312 and 11313.

³⁵GAO, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*, [GAO-18-93](#) (Washington, D.C.: Aug. 2, 2018). The 24 major federal agencies covered by the Chief Financial Officers Act of 1990 are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

Figure 3: Extent to Which 24 Agencies’ Policies Addressed the Role of Their Chief Information Officers (CIO), Presented from Most Addressed to Least Addressed Area (as of August 2018)



Source: GAO analysis of agency IT management policies. | GAO-25-107852

Officials from most agencies stated that their CIOs were implementing the responsibilities even when not required in policy. Nevertheless, the 24 selected CIOs acknowledged in their responses to our survey that they were not always very effective in implementing the six IT management areas.

Shortcomings in agencies’ policies were partially attributable to weaknesses in OMB guidance. We found that OMB guidance did not comprehensively address all CIO responsibilities. For example, OMB guidance did not ensure that CIOs had a significant role in (1) IT planning, programming, and budgeting decisions and (2) execution decisions and the management, governance, and oversight processes related to IT. Until agencies fully address the role of CIOs in their policies, agencies will be limited in addressing longstanding IT management challenges.

➤ **We recommended** that each of the 24 federal agencies address weaknesses related to the six key areas of CIO responsibility. We also recommended that OMB update and issue guidance related to particular CIO responsibilities, including those relating to the IT workforce, among other things. Fourteen agencies agreed with our recommendations and five agencies had no comments on them. Five agencies (including OMB) partially agreed with our recommendations and one agency disagreed. As of December 2024, 10 agencies

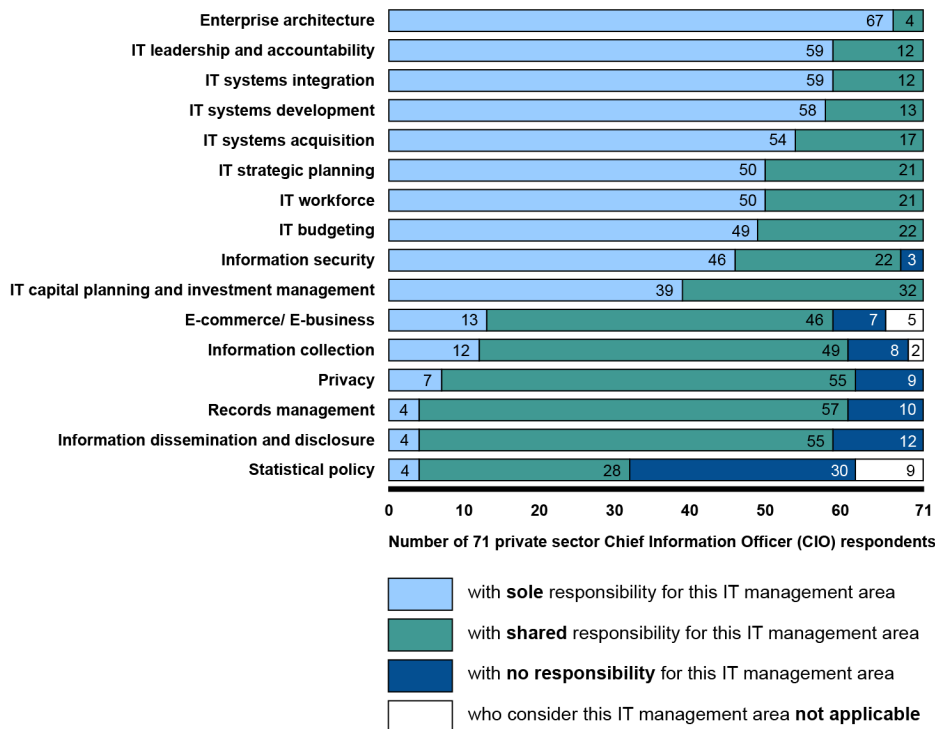
had not yet fully implemented our recommendations to address weaknesses related to the six key areas of CIO responsibility, and OMB had not yet addressed two recommendations.

The federal government should use private sector practices to inform CIO roles.

The Comptroller General convened a forum in September 2016 that explored the challenges and opportunities for CIOs to improve federal IT acquisitions and operations.³⁶ The panel participants—which included private sector IT executives, current and former federal agency CIOs, and members of Congress—identified, among other things, challenges in IT areas such as budget formulation, governance, workforce, operations, and transition planning.

In September 2022, we found that most of the 71 private sector CIOs we surveyed reported having responsibilities that aligned with those of agency CIOs in 13 of 14 key IT management areas.³⁷ These areas included strategic planning, investment management, and IT systems acquisition. The private sector CIO respondents also reported sharing responsibility with other executives in each IT management area (see figure 4).

Figure 4: Extent of Sharing of IT Management Area Responsibilities Reported by 71 Private Sector Chief Information Officer (CIO) Respondents (as of September 2022)



Source: GAO analysis of data from 71 private sector CIO survey respondents. | GAO-25-107852

³⁶The results of the forum are discussed in GAO, *Information Technology: Opportunities for Improving Acquisitions and Operations*, GAO-17-251SP (Washington, D.C.: Apr. 11, 2017).

³⁷GAO, *Chief Information Officers: Private Sector Practices Can Inform Government Roles*, GAO-22-104603 (Washington, D.C.: Sept. 15, 2022).

Responsibilities that were assigned to the Federal CIO (as of September 2022) corresponded to those of agency CIOs in 10 of the 14 key IT management areas. The Federal CIO's responsibilities also corresponded to those of private sector survey respondents in each of the five responsibility areas directly relevant to the roles of both (e.g., identifying, developing, and coordinating projects to improve government performance through use of IT).

However, the Federal CIO position was not established in law, and its main legal authorities remained those established in 2002 for the OMB position from which the role was established. As such, its responsibilities were often more limited in key CIO management areas than those of agency and private sector CIOs.

Private sector and former agency CIOs reported challenges faced by federal agency CIOs. Specifically, private sector CIOs stated that collaboration with other senior executives was essential to driving successful business outcomes. Conversely, former federal CIOs reported difficulty achieving meaningful collaboration with other managers. In addition, private sector CIOs stated that their companies often look for managerial skills, such as project management skills, when hiring CIOs. By contrast, former agency CIOs stated that technical skills were often a primary driver in the selection of agency CIOs. Fostering shared collaboration and increasing focus on managerial skillsets for agency CIOs could assist federal agencies and their CIOs in securing resources and implementing IT priorities.

- **We recommended** that Congress consider formalizing the Federal CIO position and establishing responsibilities and authorities for government-wide IT management. We also recommended that OMB increase the emphasis placed on collaboration between CIOs and other executives, and take steps to ensure that managerial skills, such as communication and program management skills, have an appropriate role in CIO hiring criteria. OMB did not agree or disagree with our recommendations. As of December 2024, OMB and Congress had not yet addressed these issues.

What actions should agencies take to enhance efforts to strategically plan for and manage portfolios of IT systems, applications, and software licenses, and to manage existing IT system operations?









OMB and federal agencies need to address selected statutory requirements for IT portfolio management.

Agency-wide reviews of IT portfolios can be used to, among other things, assess the current maturity of an agency's IT portfolio management processes, reduce duplication, and achieve savings by identifying opportunities to consolidate investments or move to shared services. FITARA includes various requirements for OMB and agencies on performing annual IT portfolio reviews. FITARA also codifies requirements for OMB and agencies on conducting reviews of high-risk IT investments. Such reviews, when implemented effectively, can be used to turn around, halt, or terminate IT projects that are failing or not producing results.

In November 2024, we found that OMB was not fully addressing eight key statutory requirements contained in FITARA.³⁸ Specifically, OMB was partially following four of the five requirements on IT portfolio reviews, and not following the three requirements on high-risk IT investments (see figure 5). Until OMB adheres to FITARA's portfolio management requirements, its oversight of agencies' IT portfolios, including potentially troubled IT investments, will be limited. As a result, the federal government will likely continue to expend resources on IT investments that do not meet the needs of the government or the public.

³⁸GAO, *IT Portfolio Management: OMB and Agencies Are Not Fully Addressing Selected Statutory Requirements*, [GAO-25-107041](#) (Washington, D.C.: Nov. 14, 2024).

Figure 5: Extent to Which the Office of Management and Budget (OMB) Followed Statutory Requirements (as of November 2024)

Requirement	Assessment
IT portfolio reviews	
Implement a process to assist agencies in reviewing their IT portfolios.	 Partially followed
Develop standardized cost savings/avoidance and performance metrics for agencies to implement the process.	 Partially followed
Carry out the Federal Chief Information Officer’s (CIO) role in being involved in an annual review of each agencies’ IT portfolio in conjunction with the agency’s CIO and Chief Operating Officer or Deputy Secretary (or equivalent).	 Not followed
Submit a quarterly report on the cost savings/reductions in duplicative IT investment identified through this review process to key committees in Congress.	 Partially followed
Submit to Congress a report on the net program performance benefits achieved as a result of major capital investments made by agencies for information systems and how the benefits relate to the accomplishment of the goals of the agencies.	 Partially followed
High-risk IT investment reviews	
Carry out consultation responsibilities of the Federal CIO to agency CIOs and program managers of major IT investments that receive high-risk ratings for four consecutive quarters.	 Not followed
Communicate the results of high-risk IT investment reviews to key committees in Congress.	 Not followed
Deny any request of additional development, modernization, or enhancement funding for a major investment that has been rated high-risk for a year after the high-risk IT investment review. Additional funding should be denied until the agency CIO determines that the root causes of the risk have been addressed, and there is capability to deliver the remaining increments within the planned cost and schedule. ^a	 Not followed

Partially followed = the agency demonstrated that it was following some, but not all, of the requirement, Not followed = the agency did not demonstrate that it was following the requirement

Sources: GAO analysis based on OMB data and all icon illustrations. | GAO-25-107852

^aThis requirement does not apply to investments at the Department of Defense.

In addition, as of November 2024, 24 CFO Act agencies had not fully addressed FITARA requirements for IT portfolio management. Specifically, none of the 24 agencies fully met the requirements for annual IT portfolio reviews. In addition, eight agencies with major IT investments rated as high-risk for four consecutive quarters did not follow the FITARA requirements for performing high-risk IT investment reviews. Three of the eight agencies performed the reviews, but they did not address the specific requirements in law. The remaining five agencies did not perform the reviews. Not performing these required reviews can permit investments with substantial cost, schedule, and performance problems to continue unabated without necessary corrective actions.

- **We recommended** that OMB improve its IT portfolio review guidance, processes, and reporting and the 24 agencies improve their IT portfolio processes. OMB neither agreed nor disagreed with the 10 recommendations we made to it. OMB responded on behalf of all the agencies to whom we made 36 recommendations but noted that some agencies might respond to address their own circumstances. Of the 24 agencies, six agencies agreed with our recommendations, two neither agreed or disagreed with the recommendations in their comments, 12 deferred to OMB to provide a response, three agencies stated that they had no comments, and one agency provided comments too late to be included in the report but agreed with its recommendations. As of December 2024, the 46 recommendations had not yet been implemented.

Agencies need to apply leading application rationalization practices to improve their software management and achieve cost savings.

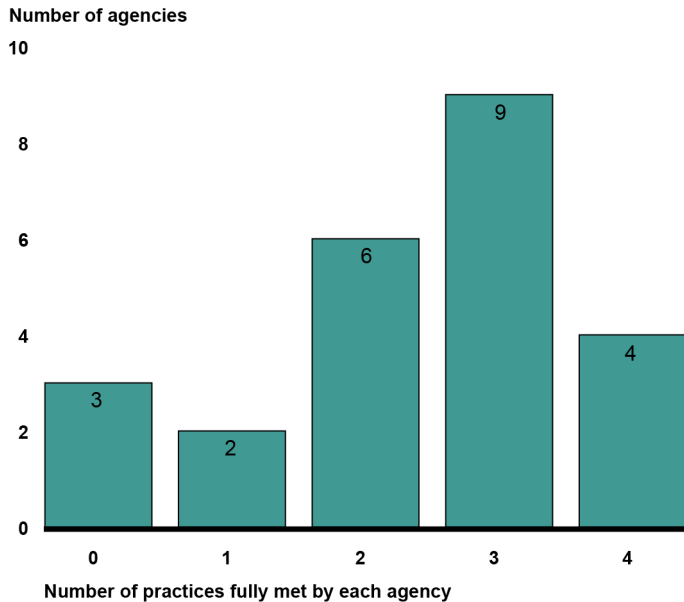
Since 2013, OMB has advocated the use of application rationalization—a process by which an agency streamlines its portfolio of software applications with the goal of improving efficiency, reducing complexity and redundancy, and lowering the cost of ownership.³⁹ Agencies can use application rationalization to identify duplicative, wasteful, and low-value applications in their portfolios and identify opportunities for savings. To effectively perform rationalization, agencies should first establish a complete inventory of applications.

In September 2016, we reported that most of the 24 selected agencies we reviewed had fully met at least three of the four practices we identified for establishing complete application inventories.⁴⁰ To be considered complete, agencies' inventories should (1) include business and enterprise IT systems as defined by OMB; (2) include these systems from all organizational components; (3) specify application name, description, owner, and function supported; and (4) be regularly updated with quality controls in place to ensure the reliability of the information collected. Specifically, four agencies fully met all four practices, nine agencies fully met three practices, six agencies fully met two practices, two agencies fully met one practice, and three agencies did not fully meet any practice (see figure 6). Not accounting for all applications may have resulted in missed opportunities to identify savings and efficiencies.

³⁹OMB, *Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management* M-13-09 (Washington, D.C.: Mar. 27, 2013).

⁴⁰GAO, *Information Technology: Agencies Need to Improve Their Application Inventories to Achieve Additional Savings*, [GAO-16-511](#) (Washington, D.C.: Sept. 29, 2016).

Figure 6: Assessment of Whether Agencies Fully Met Practices for Establishing Complete Software Application Inventories (as of September 2016)



Source: GAO analysis of agency information. | GAO-25-107852

In addition, we found that six selected agencies relied on their investment management processes and, in some cases, supplemental processes to rationalize their applications to varying degrees. However, five of the six agencies acknowledged that their processes did not always allow for collecting or reviewing the information needed to effectively rationalize all their applications. The sixth agency, the National Science Foundation, stated its processes allowed it to effectively rationalize its applications, but agency documentation supporting this assertion was incomplete. Only one agency—the National Aeronautics and Space Administration—had plans to address shortcomings.

- **We recommended** that 20 agencies improve their software application inventories and five agencies improve their processes to rationalize their applications more completely. DOD disagreed with both recommendations made to it. After reviewing additional evidence, we removed the recommendation associated with improving the inventory but maintained the other. The other agencies agreed to or had no comments on the draft report. As of December 2024, all 24 recommendations had been implemented.

By taking action to implement our recommendations, the agencies are better positioned to identify opportunities to rationalize their applications, which could lead to cost savings and efficiencies. Implementing our final recommendation could lead to additional savings and efficiencies.

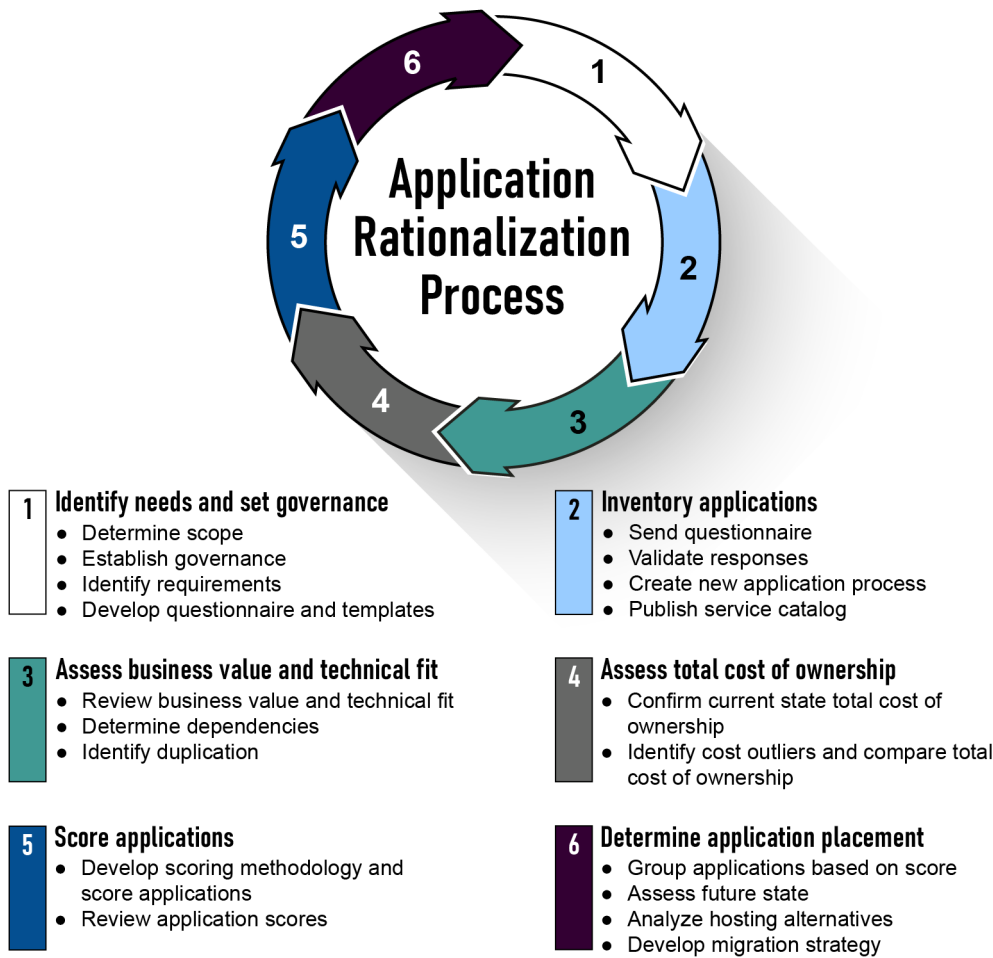
In June 2019, OMB published an update to its *Federal Cloud Computing Strategy*, called Cloud Smart.⁴¹ As part of Cloud Smart, OMB required all federal agencies to rationalize their application portfolios. In doing so, OMB required agencies to assess which applications are best suited for the cloud.

Also in June 2019, the CIO Council issued *The Application Rationalization Playbook* to assist agencies with implementing the application rationalization process to decide which applications belong in the cloud. The

⁴¹Office of Management and Budget, *Federal Cloud Computing Strategy* (June 24, 2019). OMB issued its original *Federal Cloud Computing Strategy* in 2011. Office of Management and Budget, *Federal Cloud Computing Strategy* (Feb. 8, 2011).

playbook included a six-step rationalization process with discrete actions for agencies to consider when undergoing application rationalization (see figure 7).⁴²

Figure 7: CIO Council’s Six-step Application Rationalization Process Outlined in *The Application Rationalization Playbook: An Agency Guide to Portfolio Management*



Source: GAO analysis of Chief Information Officer Council *Application Rationalization Playbook*. | GAO-25-107852

In June 2022, we reported that DOD had reported making progress in implementing an enterprise-wide application rationalization effort.⁴³ However, among other things, DOD had not established a plan to develop and implement an enterprise-wide rationalization process with measurable objectives, milestones, and timelines. DOD also lacked a definition of who was responsible within the department for ensuring application rationalization was successful. Without measurable objectives, milestones, and time frames for rationalization efforts—and holding department components accountable for these efforts—DOD would be less likely to make consistent measurable progress on rationalization or effectively reduce IT duplication.

⁴²CIO Council, *The Application Rationalization Playbook: An Agency Guide to Portfolio Management* (June 2019).

⁴³GAO, *Cloud Computing: DOD Needs to Improve Workforce Planning and Software Application Modernization*, GAO-22-104070 (Washington, D.C.: June 29, 2022).

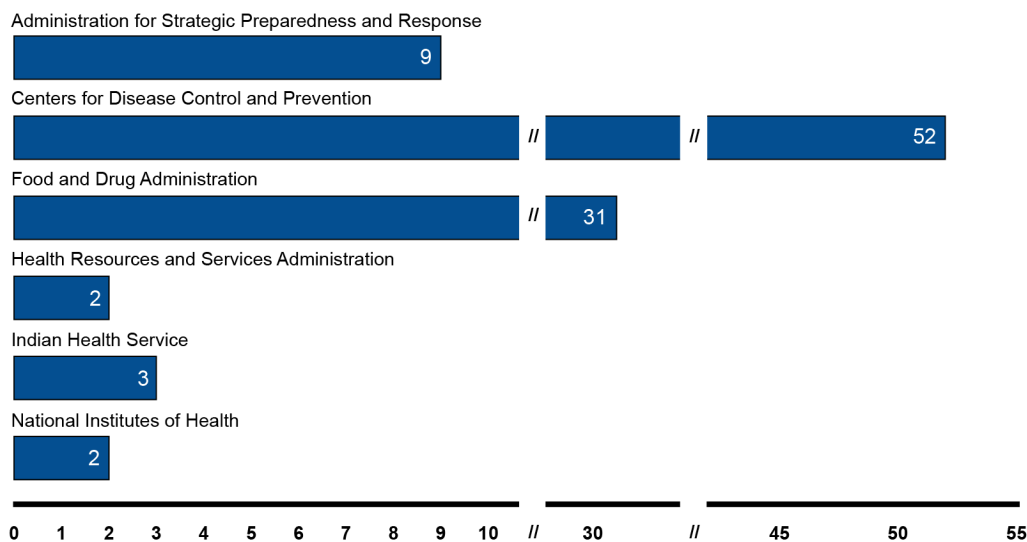
- **We recommended** that DOD improve its application rationalization planning, among other things. DOD partially concurred with the three related recommendations and described planned actions to address them. As of December 2024, the recommendations had not yet been implemented.

The Department of Health and Human Services needs to identify duplicative pandemic IT systems.

The Department of Health and Human Services (HHS) and its component agencies are responsible for managing data collection activities to support public health preparedness and response during public health emergencies, such as the COVID-19 pandemic. The Consolidated Appropriations Act, 2023 reiterated the need for HHS to improve its data collection capabilities and included a provision for us to review those capabilities.⁴⁴

In September 2024, we found, among other things, that HHS had not identified and reduced unnecessary duplication of data in its systems supporting pandemic public health preparedness and response.⁴⁵ Because the department did not have a comprehensive list of these systems, we worked with key HHS component agencies and identified a total of 99 systems (see figure 8).

Figure 8: Number of Department of Health and Human Services Systems Supporting Pandemic Public Health Preparedness and Response, per component (as of September 2024)



Source: GAO analysis of Department of Health and Human Services data. | GAO-25-107852

HHS did not attempt to identify duplication or overlap for these systems. However, in our high-level review of the 99 systems, we identified instances of duplicative pandemic public health preparedness and response data

⁴⁴Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, § 2216, 136 Stat. 4459, 5740 (2022). The data capabilities include the collection of public health preparedness, response, and recovery data regarding disease tracking, hospitalizations, critical care capacity, and testing programs for diseases, such as COVID-19. For the purposes of this report, the systems we discussed were those that assist HHS in pandemic preparedness and response, however, these systems could also have other functions related to public health.

⁴⁵GAO, *COVID-19: HHS Needs to Identify Duplicative Pandemic IT Systems and Implement Key Privacy Requirements*, [GAO-24-106638](#) (Washington, D.C.: Sept. 18, 2024). As part of this review, we also examined the extent to which HHS had instituted privacy safeguards on selected systems when collecting public health preparedness and response data. We made recommendations in response to those findings and are monitoring HHS’s implementation of them as part of the cybersecurity area of GAO’s High-Risk list.

in multiple systems. For example, two pandemic systems that collected similar COVID-19 data, such as cases, deaths, and hospitalization data, were managed by the same program office.

- **We recommended** that HHS (1) develop and maintain an inventory of systems that support pandemic public health preparedness and response, and (2) conduct reviews of such systems across the department to identify and reduce any unnecessary duplication, overlap, or fragmentation and identify mitigation options (e.g., consolidation or elimination of systems). HHS did not agree or disagree with the recommendation to establish a system inventory. The agency agreed with the recommendation to identify duplication, overlap, and fragmentation of pandemic-related data systems and stated that it would analyze the costs and benefits of doing so. As of December 2024, the recommendations had not been implemented.

When these recommendations are implemented, HHS could achieve cost savings by consolidating or decommissioning multiple systems. The agency could also avoid purchasing or developing new systems that would introduce duplication. GAO cannot precisely estimate the savings that could occur. However, given that HHS has identified 99 systems that support pandemic preparedness and response, if even one of these systems could be consolidated or decommissioned, the agency could save hundreds of thousands of dollars over the planned lifespan of the system.

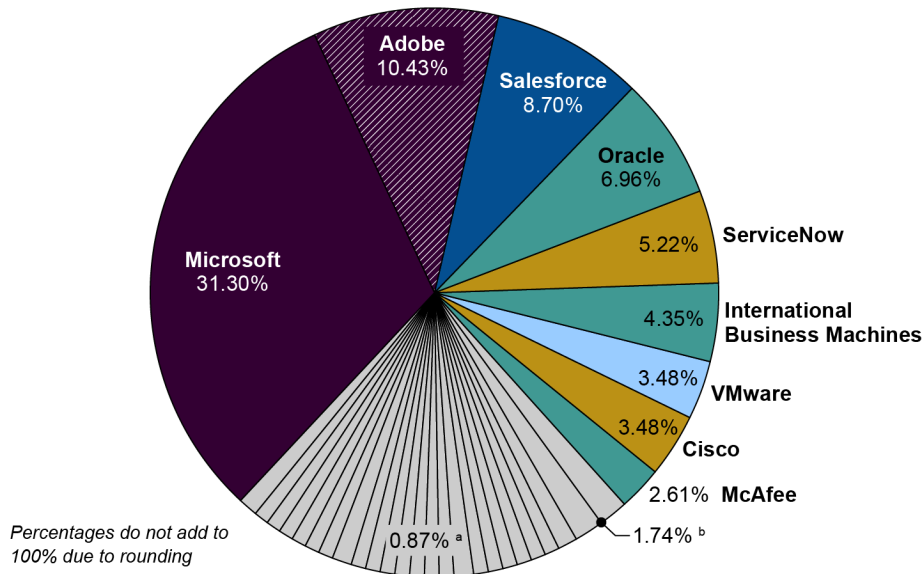
Agencies need to take action to achieve additional savings on software licenses.

Each year, federal agencies purchase thousands of software licenses from vendors. Effective management of commercial software licenses can help organizations avoid purchasing too many licenses—referred to as over-purchasing—that result in unused software. In addition, effective management can help avoid purchasing too few licenses—referred to as under-purchasing—which may result in noncompliance with license terms and cause the imposition of additional fees.

In January 2024, we reported that 24 federal agencies collectively identified 36 software vendors as those with the highest quantity of licenses installed, as of July 2022.⁴⁶ Similarly, agencies reported 34 software vendors that were paid the highest amounts for fiscal year 2021 (see figure 9).

⁴⁶GAO, *Federal Software Licenses: Agencies Need to Take Action to Achieve Additional Savings*, [GAO-24-105717](#) (Washington, D.C.: Jan. 29, 2024).

Figure 9: Software Vendors with the Highest Amounts Paid Reported by Agencies for Fiscal Year 2021



Source: GAO analysis of agency data. | GAO-25-107852

^aThe 23 vendors shown as 0.87 percent are Broadcom, Computer Associates International, Entrust, ESCgov, FCN, Four, Intelligent Editing, LinkedIn, Mercom, MicroStrategy, NCS Technologies, Palantir Technologies, PKWARE, PTC, Quest Software, SAS Institute, Skillsoft, Splunk, Symantec, Thomson Reuters, Unison Software, Zoom Video Communications, and Zscaler.

^bThe two vendors shown as 1.74 percent are Environmental Systems Research Institute and Google.

Key activities for assessing the appropriate number of software licenses are (1) tracking licenses currently in use and (2) regularly comparing the inventory of software licenses currently in use to purchase records. We found that none of the nine selected agencies fully determined whether their five most widely used software licenses were over- or under-purchased.

➤ **We recommended** that the nine selected agencies consistently track software license usage and compare the inventories with purchased licenses. Eight agencies agreed with the recommendations and one neither agreed nor disagreed. As of December 2024, none of the 18 recommendations had been fully implemented.

As of May 2024, two agencies in our review reported millions in cost savings from assessing one of their five widely used software licenses for over- or under-purchasing. If each of the remaining agencies were able to produce similar results for at least one of their widely used licenses, it could amount to millions of dollars of potential savings.

In May 2014, we reported that OMB and the vast majority of the 24 agencies we reviewed did not have adequate policies for managing software licenses.⁴⁷ While OMB had a policy on a broader IT management initiative that was intended to assist agencies in gathering information on their IT investments, including software licenses, it did not guide agencies in developing comprehensive license management policies.

Regarding the 24 agencies, two had comprehensive policies that included the establishment of clear roles and central oversight authority for managing enterprise software license agreements, among other things; 18 agencies had policies but they were not comprehensive; and four had not developed any. The weaknesses in

⁴⁷GAO, *Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide*, GAO-14-413 (Washington, D.C.: May 22, 2014).

agencies' policies were due, in part, to the lack of a priority for establishing software license management practices and a lack of direction from OMB.

In addition, the 24 agencies were generally not following the leading practices we identified for managing their software licenses. Specifically, four agencies had fully demonstrated at least one of the leading practices, and none of the agencies had implemented all of the leading practices. Until weaknesses in how agencies manage licenses are addressed, the most widely used applications cannot be determined and thus opportunities for savings across the federal government may be missed.

- **We recommended** that OMB issue a directive to help guide agencies in managing licenses and that the 24 agencies improve their policies and practices for managing licenses. OMB disagreed with the need for a directive, but we believed it was needed, as discussed in the report. Of the 24 agencies to which we made specific recommendations, 11 agencies agreed, five partially agreed, two neither agreed nor disagreed, and six had no comments. As of December 2024, the agencies and OMB had fully implemented 134 of our 136 recommendations, and two recommendations were not yet implemented.

As of January 2024, agencies had reported about \$2.1 billion in cost savings since our work in 2014 related to better management of software licenses. Fully implementing our two remaining recommendations could lead to additional savings.

OMB and GSA need to strengthen efforts to lead federal adoption of the Technology Business Management framework.

The government has faced longstanding challenges in IT management and spending transparency. In 2017, OMB announced its intention to improve insights into IT spending through government-wide adoption of the Technology Business Management Council's framework. This framework provides a standard taxonomy that is organized into four layers (cost pools, IT towers, products and services, and business units and capabilities) intended to show an organization's total IT spending from different perspectives. These four layers are comprised of spending categories and subcategories.

In September 2022, we found that OMB and the General Services Administration (GSA) had taken steps to lead government-wide Technology Business Management adoption, but progress and results were limited.⁴⁸ For example, OMB's initial plans for government-wide adoption required agencies to report IT spending using categories in the first two layers (cost pools and IT towers). However, 5 years after establishing initial plans, OMB had not expanded on requirements to include the rest of the taxonomy—the categories in layers 3 and 4, and subcategories for all layers (see figure 10).

⁴⁸GAO, *Technology Business Management: OMB and GSA Need to Strengthen Efforts to Lead Federal Adoption*, [GAO-22-104393](#) (Washington, D.C.: Sept. 29, 2022).

Figure 10: Extent to Which the Office of Management and Budget’s (OMB) Plans Addressed Elements of the Technology Business Management Taxonomy Version 3.0 (as of September 2022)

Layer 4: Business units and capabilities	Categories and subcategories in this layer are not defined by the Technology Business Management Council because they are intended to be industry-specific and, therefore, defined by organizations to reflect their respective business units and capabilities	
Layer 3: Products and services	26 categories (e.g., finance services, manufacturing and delivery, and vendor and procurement services)	119 subcategories (e.g., application hosting, business continuity and disaster recovery, contract review, and payroll and time reporting)
Layer 2: IT towers	11 categories (e.g., application, data center, network, security and compliance, and storage)	41 subcategories (e.g., business software, client management, high performance computing, and mobile devices)
Layer 1: Cost pools	9 categories (e.g., facilities and power, hardware, internal labor, software, and telecom)	30 subcategories (e.g., cloud service providers, licensing, maintenance and support, and managed service providers)

 Hashed shading represents elements that were not addressed in OMB’s plans

Source: GAO analysis of OMB guidance and *Technology Business Management Taxonomy, Version 3.0*. Copyright © 2020 Technology Business Management Council (November 2018). | GAO-25-107852

In addition, OMB and GSA assisted agency efforts to implement the Technology Business Management framework by, for example, developing implementation guidance and a maturity model assessment tool. However, OMB and GSA had not assessed agency maturity. Further, they had not analyzed the quality of agencies’ data reported in the first two layers.

OMB and GSA officials maintained that Technology Business Management implementation continues to be a priority. Nevertheless, until OMB establishes documented plans and agency expectations for the remainder of the taxonomy, uncertainty will cloud agency efforts. Further, the continued absence of OMB direction could prevent the federal government from fully achieving intended benefits such as optimizing IT spending.

- **We recommended** that OMB establish requirements for completing the remainder of the taxonomy and assess maturity of agencies’ implementation, among other things. We also recommended that GSA address benchmarking use. We incorporated suggested OMB and GSA revisions for two of the seven total recommendations; the agencies had no comments on the remaining five. As of December 2024, GSA had implemented the one recommendation we made to it and OMB had not implemented any of the six recommendations we made to it.

Federal agencies need to modernize aging legacy systems.

The federal government invests more than \$100 billion on IT annually, with much of this amount reportedly spent on operating and maintaining existing (legacy) IT systems. Given the magnitude of these investments, it is important that agencies effectively manage their operations and maintenance.

In May 2016, we reported that federal legacy IT investments were becoming increasingly obsolete: many used outdated software languages and hardware parts that were unsupported.⁴⁹ Agencies reported using several systems that had components that were, in some cases, at least 50 years old. For example, the Department of Defense (DOD) had one system that was still running on a 1970s computing system and used 8-inch floppy

⁴⁹GAO, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems*, [GAO-16-468](#) (Washington, D.C.: May 25, 2016).

disks, which are a 1970s-era storage device (see figure 11). Replacement parts for the system in 2016 were difficult to find because they were obsolete.

Figure 11: Department of Defense Air Force Strategic Automated Command and Control System



Source: U.S. Department of Defense. | GAO-25-107852

OMB began an initiative to modernize, retire, and replace the federal government's legacy IT systems. As part of this, OMB drafted guidance requiring agencies to identify, prioritize, and plan to modernize legacy systems. However, until this policy is finalized and fully executed, the government runs the risk of maintaining systems that have outlived their effectiveness.

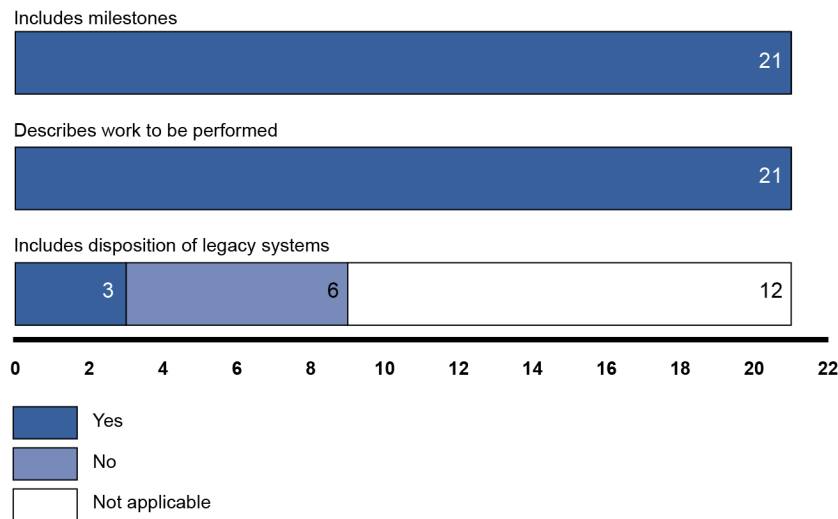
- **We recommended** that OMB finalize draft guidance to identify and prioritize legacy IT needing to be modernized or replaced. We also recommended that 12 selected agencies address at-risk and obsolete legacy investments that spend a significant proportion of their funding on operations and maintenance activities. OMB and eight of the agencies agreed with our recommendations, two partially agreed, and two had no comments. As of December 2024, 11 recommendations had been fully implemented. Of the three remaining open recommendations, two were to OMB. In March 2024, OMB stated that it believed it had met the intent of the recommendations and considered them implemented. However, we disagree and will continue to monitor the implementation of these recommendations.

In January 2023, we reported that IRS's legacy IT environment included applications, software, and hardware that were outdated but still critical to day-to-day operations.⁵⁰ Specifically, IRS relied extensively on IT to annually collect trillions of dollars in taxes, distribute hundreds of billions of dollars in refunds, and carry out its mission of providing service to America's taxpayers in meeting their tax obligations. Our analysis showed that about 33 percent of IRS's applications, 23 percent of its software instances in use, and 8 percent of its hardware assets were considered legacy. This included applications ranging from 25 to 64 years in age.

⁵⁰GAO, *Information Technology: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements*, GAO-23-104719 (Washington, D.C.: Jan. 12, 2023).

Modernization best practices call for documenting plans that include three key elements: milestones, work to be performed, and disposition of legacy systems. As of August 2022, IRS had documented plans for the 21 modernization initiatives that were underway, including nine associated with legacy systems. All 21 plans addressed two key elements. However, the plans for six of the nine initiatives did not address the disposition of legacy systems (see figure 12). Officials stated they would address this key element at the appropriate time in the initiatives' lifecycle; however, they did not identify time frames for doing so.

Figure 12: GAO Assessment of the Internal Revenue Service's (IRS) Modernization Plans (as of August 2022)



Source: GAO analysis of IRS documents. | GAO-25-107852

IRS suspended operations of six modernization initiatives that had been underway, including two that were essential to replacing the 60-year-old Individual Master File—the authoritative data source for individual tax account data. IRS had been working to replace that File for over a decade. According to officials, the suspensions were due to IRS's determination to shift resources to higher priorities; staff members working on these suspended initiatives were reassigned to other projects. As a result, the schedule for these initiatives was unknown. In addition, it was unknown whether the agency would meet the 2030 target completion date for replacing the Individual Master File, which would lead to mounting challenges in continuing to rely on a critical system with software written in an archaic language requiring specialized skills. As of September 2024, IRS had resumed three of the initiatives, including the two that are essential to replacing the Individual Master File.

- **We recommended** that IRS establish time frames to complete selected modernization plans, among other things. IRS agreed with the recommendations. However, as of December 2024, none of the nine recommendations had been fully implemented.

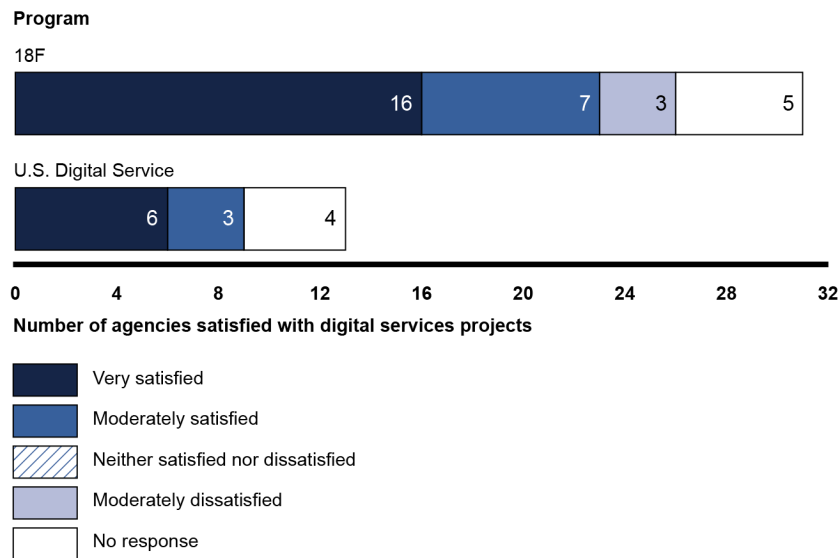
What actions should agencies take to improve the monitoring of, and transparency into, the performance of IT investments?

Digital service programs need to measure performance and assess results.

In an effort to improve IT across the federal government, in March 2014 GSA established 18F, which provides IT services (e.g., develop websites) to agencies. In addition, in August 2014 the Administration established the U.S. Digital Service (USDS), which aims to improve public-facing federal IT services.

In August 2016, we found that 18F and USDS had provided a variety of services to agencies supporting their IT efforts.⁵¹ Specifically, 18F staff helped 18 agencies with 32 projects and generally provided development and consulting services, including software development solutions and acquisition consulting. In addition, USDS provided assistance on 13 projects across 11 agencies and generally provided consulting services, including quality assurance and problem identification and recommendations. According to our survey, managers were generally satisfied with the services they received from 18F and USDS on these projects (see figure 13).

Figure 13: Results of GAO Survey on Satisfaction with Digital Services Projects (as of August 2016)



Source: GAO survey of agency project managers that engaged with 18F and U.S. Digital Service. | GAO-25-107852

We also found that both 18F and USDS had partially implemented practices to identify and help agencies address problems with IT projects. Specifically, 18F had developed several outcome-oriented goals and related performance measures, as well as procedures for prioritizing projects; however, not all of its goals were outcome-oriented and it had not yet fully measured program performance. Similarly, USDS had developed goals, but they were not all outcome-oriented and it had established performance measures for only one of its goals. USDS had also measured progress for just one goal. Without fully implementing these practices, it would be difficult to hold the programs accountable for results.

- **We recommended** that OMB and GSA improve goals and performance measurement. OMB and GSA agreed with the recommendations. As of December 2024, GSA had implemented the two recommendations we made to it. OMB had implemented one of our three recommendations and had not yet implemented the other two.

IRS needs to improve reporting for its modernization programs.

IRS relies extensively on IT to annually collect trillions of dollars in taxes, distribute hundreds of billions of dollars in refunds, and carry out its mission of providing service to America's taxpayers in meeting their tax obligations. In August 2022, Congress appropriated tens of billions of dollars to IRS through the Inflation

⁵¹GAO, *Digital Service Programs: Assessing Results and Coordinating with Chief Information Officers Can Improve Delivery of Federal Projects*, GAO-16-602 (Washington, D.C.: Aug. 15, 2016).

Reduction Act of 2022. These appropriations were intended to be used to bolster taxpayer services and enforcement of the tax code, and modernize IT, among other things.

In March 2024, we reported that, in April 2023, the IRS issued its agency-wide strategic operating plan outlining its vision to use the appropriations contained in the Inflation Reduction Act of 2022.⁵² The plan identified five objectives, including a technology objective underpinning the other four (see figure 14).

Figure 14: Inflation Reduction Act Strategic Operating Plan Transformation Objectives (as of April 2023)



Source: GAO analysis of Internal Revenue Service information and all illustrations. | GAO-25-107852

The IRS plan stated that it would use the technology objective to, among other things, retire and replace legacy systems. Projects under the technology objective included ongoing modernization programs that had been modified to account for the new appropriations.

Regarding cost and schedule performance of IT modernization programs, IRS reported meeting most of its quarterly targets for fiscal years 2022 and 2023. However, while IRS’s quarterly status reports provide important information on modernization progress, they could be improved by including programs’ historical cost and schedule goals and how quarterly performance compares to overall program goals. For example, we previously reported that a key IT investment was within schedule estimates for 2019 and 2020 but that IRS had changed its overall program plans several times. These changes led to a 9-year milestone delay—from 2014 to 2023. However, the quarterly reports did not show this lengthy delay because they did not include programs’ historical cost and schedule goals.

- **We recommended** that IRS improve its reporting on IT modernization program progress, among other things. IRS concurred with our three recommendations. As of December 2024, the recommendations had not been implemented.

The Department of Labor needs to measure the performance of states’ unemployment insurance IT systems.

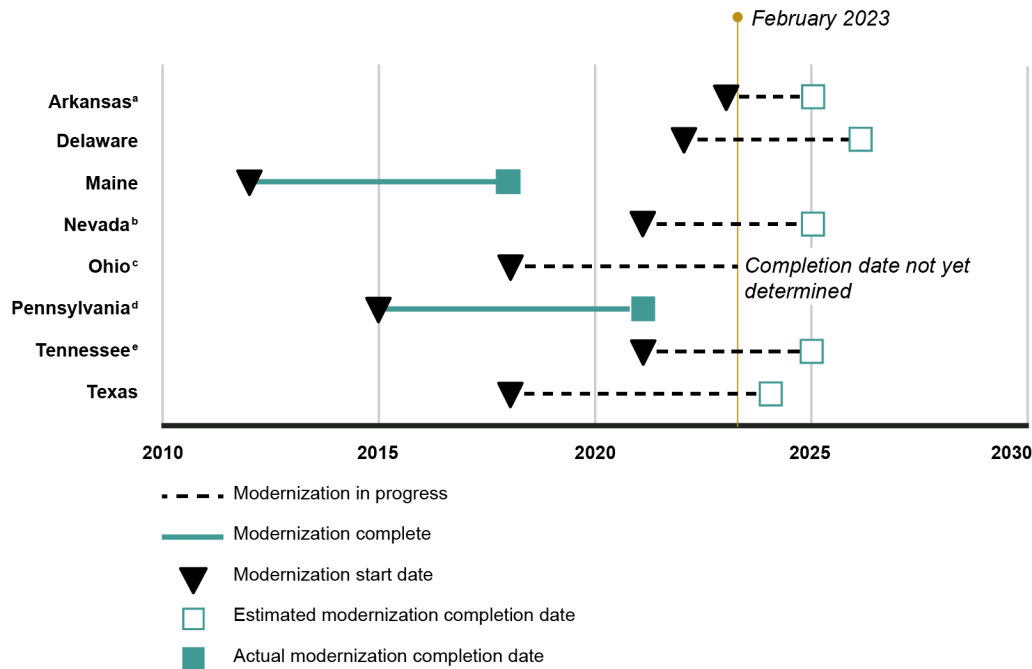
In the wake of the COVID-19 pandemic, the nation experienced historic levels of job loss. According to Labor data, approximately \$878 billion in benefits were paid across all unemployment insurance (UI) programs from April 2020 to September 2022. However, state UI programs with legacy IT systems faced performance issues in processing the unprecedented number of UI claims.⁵³

⁵²GAO, *Information Technology: IRS Needs to Complete Planning and Improve Reporting for Its Modernization Programs*, GAO-24-106566 (Washington, D.C.: Mar. 19, 2024).

⁵³Due to, among other things, the performance challenge that state UI insurance programs with legacy IT systems faced, we added the overarching UI to our High-Risk List in June 2022.

In July 2023, we found that eight selected states were in varying phases of modernizing their UI IT systems, ranging from planning to operations and maintenance.⁵⁴ As of February 2023, six of the eight states had modernization efforts underway, but not yet completed (see figure 15).

Figure 15: Unemployment Insurance System Modernization Timeline for Selected States (as of February 2023)



Source: GAO analysis of state information and interviews with state officials. | GAO-25-107852

Note: Timelines represent state efforts to modernize their unemployment insurance benefits, appeals, and tax systems, unless otherwise noted.

^aArkansas’ modernization effort is focused on its benefits and tax systems only.

^bNevada previously completed a modernization of its benefits, appeals, and tax systems in 2015

^cOhio’s tax system modernization effort was initiated in 2018 and completed in 2021. As of February 2023, the state was in the planning stages of its benefits and appeals system modernization and had not yet determined an anticipated completion date.

^dPennsylvania’s 2015 to 2021 modernization effort focused on its benefits and appeals systems only.

^eTennessee previously completed a modernization of its benefits and appeals system in 2016.

We also found that Labor had gaps in its oversight of states’ UI IT performance. Specifically, although Labor is responsible for overseeing the UI program to ensure that the states are operating the program effectively and efficiently, it had not measured states’ UI IT performance. For example, it had not measured the number of states using cloud infrastructures to support their UI systems. Measuring areas such as this is important because it could help inform Labor of where gaps may exist in states’ IT capabilities and where to commit additional resources.

According to Labor officials, the department had not measured states’ UI IT performance because it had not yet defined IT standards to measure states against. As a result, Labor was limited in its ability to monitor whether states’ UI IT systems were performing efficiently and effectively, identify gaps in UI IT modernization, and ensure that resources are properly allocated to address any gaps.

⁵⁴GAO, *Unemployment Insurance: DOL Needs to Further Help States Overcome IT Modernization Challenges*, GAO-23-105478 (Washington, D.C.: July 10, 2023).

- **We recommended** that Labor (1) define UI IT modernization standards for states and (2) measure states' performance against the established standards. Labor partially agreed with the first recommendation and agreed with the second one. As of December 2024, the recommendations had not yet been implemented.

What actions should agencies take to strengthen planning and budgeting for the acquisition of IT systems and services?

Agencies need to improve CIOs' review and approval of IT budgets.

One of the purposes of FITARA was to strengthen the authority of CIOs at major departments and agencies to provide needed direction and oversight of covered agencies' IT budgets. Among other things, FITARA requires the CIOs of certain major civilian agencies to have a significant role in the decision processes for all annual and multi-year planning and to approve the IT budget requests of the agencies.

In November 2018, we reported that four selected departments—Energy, HHS, Justice, and Treasury—took steps to establish policies and procedures that align with eight selected OMB requirements intended to implement FITARA and to provide the CIO visibility into and oversight over the IT budget.⁵⁵ For example, of the eight OMB requirements, all four departments had established policies and procedures related to the level of detail with which IT resources are to be described in order to inform the CIO during the planning and budgeting processes. However, the departments varied in how fully they had established policies and procedures related to some other OMB requirements, and none of the four departments had yet established procedures for ensuring that the CIO had reviewed whether the IT portfolio includes appropriate estimates of all IT resources included in the budget request (see figure 16).

⁵⁵GAO, *Information Technology: Departments Need to Improve Chief Information Officers' Review and Approval of IT Budgets*, [GAO-19-49](#) (Washington, D.C.: Nov. 13, 2018).

Figure 16: Evaluation of Selected Departments’ Policies and Procedures for Key IT Budgeting Requirements (as of November 2018)

Selected Office of Management and Budget (OMB) requirement	DOE	HHS	DOJ	Treasury
1. Establish the level of detail with which IT resources are to be described in order to inform the Chief Information Officer (CIO) during the planning and budgeting processes.				
2. Establish agency-wide policy for the level of detail with which planned expenditures for all transactions that include IT resources are to be reported to the CIO.				
3. Include the CIO in the planning and budgeting stages for programs that are supported with IT resources.				
4. Include the CIO as a member of governance boards that inform decisions regarding all IT resources, including component-level governance boards.				
5. Document the processes by which program leadership works with the CIO to plan an overall portfolio of IT resources.				
6. Ensure the CIO has reviewed and approved the major IT investments portion of the budget request.				
7. Ensure the CIO has reviewed IT resources that are to support major program objectives and significant increases and decreases in IT resources.				
8. Ensure the CIO has reviewed whether the IT portfolio includes appropriate estimates of all IT resources included in the budget request.				

- Satisfied all = The department provided documentation that satisfied all of the OMB requirement
- Satisfied most = The department provided documentation that satisfied most, but not all of the OMB requirement
- Satisfied none = The department could not provide documentation that satisfied any of the OMB requirement

DOE = Department of Energy, HHS = Department of Health and Human Services, DOJ = Department of Justice, Treasury = Department of the Treasury

Source: GAO analysis of department data and all icon illustrations. | GAO-25-107852

Where the departments had not fully established policies and procedures, it was due, in part, to having not addressed in their FITARA implementation and delegation plans how they intended to implement the OMB requirements.

In addition, all four selected departments lacked quality assurance processes for ensuring their IT budgets were informed by reliable cost information. Specifically, the selected departments did not have IT capital planning processes for (1) ensuring government labor costs had been accurately reported, (2) aligning contract costs with IT investments, and (3) utilizing budget object class data to capture all IT programs. This resulted in billions of dollars in requested IT expenditures without departments having comprehensive information to support those requests, and nearly \$4.6 billion in IT contract spending that was not explicitly aligned with investments in selected departments’ IT portfolios. This was due to a lack of processes for periodically

reviewing data quality and estimation methods for government labor estimates, as well as a lack of mechanisms to cross-walk IT spending data in their procurement and accounting systems with investment data in their IT portfolio management systems.

- **We recommended** that the selected departments address gaps in their IT budgeting policies and procedures, and establish procedures to ensure IT budgets are informed by reliable cost information, among other things. Two agencies and their component agencies agreed with our recommendations. One agency neither agreed nor disagreed with the recommendations, while its component agency agreed with the recommendations made to it. One agency partially agreed with one recommendation and agreed with the other recommendations made to it and its component agency. As of December 2024, the departments had implemented 38 of our 43 recommendations and had not yet fully implemented five.

By implementing these recommendations, we estimate that the agencies have the potential to realize financial benefits of hundreds of millions of dollars in total. These savings could be achieved through better accounting of government labor and contract costs and improved oversight of IT spending.

The Department of Veterans Affairs needs to improve CIO oversight of procurements.

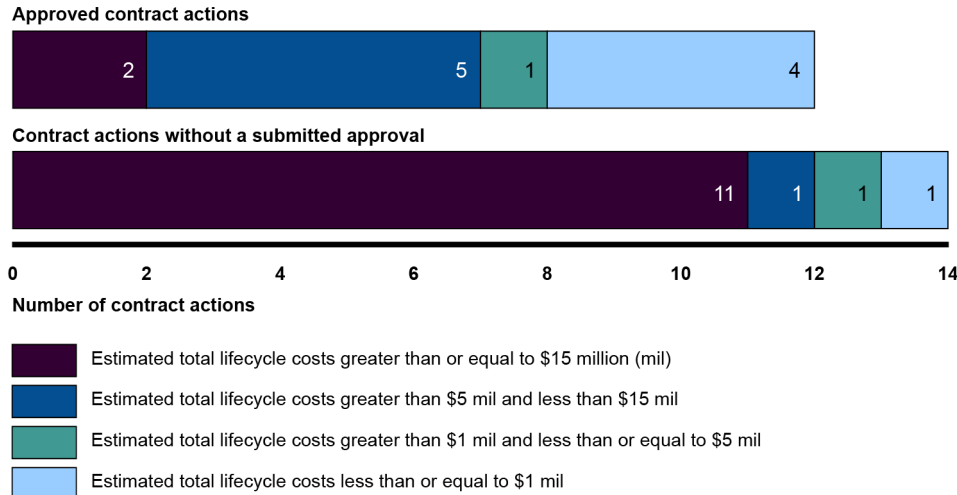
The Department of Veterans Affairs' (VA) mission is to promote the health, welfare, and dignity of all veterans in recognition of their service to the nation by ensuring that they receive benefits, social support, medical care, and lasting memorials. In carrying out this mission, the department operates one of the largest health care delivery systems in America, providing health care to millions of veterans. VA's ability to effectively serve veterans and other eligible individuals depends on the functionality of the underlying IT systems that support its core activities. The department annually spends billions of dollars on IT each year to support the delivery of veterans' benefits and health care services.

In March 2023, we found that VA procured IT and IT-related assets and activities that were often not approved by its CIO,⁵⁶ as required by FITARA. Specifically, between March 2018 and the end of fiscal year 2021, VA awarded 11,644 new contract actions categorized as IT. However, VA did not provide evidence of CIO approval for 4,513 (or 39 percent) of these contract actions.

A more in-depth review of 26 selected IT contract actions from fiscal year 2021 confirmed that 12 had documentation showing approval by appropriate agency officials at the required level of authority. The remaining 14 contract actions lacked CIO approval documentation (see figure 17).

⁵⁶GAO, *IT Management: VA Needs to Improve CIO Oversight of Procurements*, [GAO-23-105719](#) (Washington, DC.: Mar. 30, 2023).

Figure 17: The Department of Veterans Affairs' Documented Chief Information Officer Approvals for Selected Fiscal Year 2021 IT Contract Actions (as of March 2023)



Source: GAO analysis of Department of Veterans Affairs contract data. | GAO-25-107852

Of the 14 contract actions lacking CIO approval, 13 were managed by non-IT contracting offices. According to VA officials, their contracting systems lacked an automated control that would remind contracting officers of CIO review and approval requirements. Without an automated check or control to ensure contracting officer compliance, it is likely that there will continue to be IT procurements that will not be routed for CIO review. This lack of visibility into the procurement of much of VA's IT assets and activities constrained the CIO's opportunity to provide input on current and planned IT acquisitions. This, in turn, could result in awarding contracts that are duplicative or poorly conceived.

- **We recommended** that VA implement automated controls into relevant contracting systems to ensure CIO review of IT procurements. VA concurred with the recommendation. As of December 2024, this recommendation had not yet been implemented.

What ongoing 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 IT acquisition and management efforts in this area. It is essential that executive branch agencies focus on improving the effectiveness of key IT leadership positions, including the Federal CIO, agency CIOs, and agency chief AI officers; enhance efforts to strategically plan for and manage IT portfolios and operations; improve the monitoring of, and transparency into, IT investment performance; and strengthen the planning and budgeting for the acquisition of IT systems and services. These actions are critical to improving federal agencies' oversight and management of their IT portfolios and ensuring the efficient and cost-effective use of the billions of dollars the government spends on IT each year. Table 1 identifies our ongoing work related to each action associated with this challenge area.

Table 1: GAO’s Ongoing Work Related to the Strengthening Oversight and Management of IT Portfolios Challenge Area (as of December 2024)

Critical action	Related ongoing GAO work
1. Improve the effectiveness of key IT leadership positions, including the federal CIO, agency CIOs, and agency chief artificial intelligence officers.	We do not have any ongoing work related to this action area.
2. Enhance agency efforts to strategically plan for and manage portfolios of IT systems, applications, and software licenses, and to manage existing IT system operations.	A review of the extent to which federal agencies have adopted selected key Technology Business Management practices to improve insight into IT investment spending.
3. Improve the monitoring of, and transparency into, the performance of IT investments.	A review of the Social Security Administration’s management and oversight of its IT investments, including the extent to which the agency’s IT investment management process complies with federal laws, guidance, and key practices; and the extent to which the agency is evaluating the outcomes of selected IT investment management efforts.
4. Strengthen planning and budgeting for the acquisition of IT systems and services.	A review of the extent to which federal agencies have identified their legacy IT systems in need of modernization and developed plans for modernizing those most in need.

Source: GAO. | GAO-25-107852



Implementing Mature IT Acquisition and Development Practices

Overview

Over the past two decades the executive branch has undertaken numerous initiatives to better manage the more than \$100 billion that is annually invested in IT. However, agencies have continued to be plagued by IT investments that too frequently fail to deliver capabilities in a timely manner and incur cost overruns or schedule slippages while contributing little to mission-related outcomes. To address the government's challenge in implementing mature IT acquisition and development practices that are essential to successfully acquiring IT, it is critical that agencies improve implementation of leading IT acquisition and development practices to effectively plan and manage IT project costs, schedules, risks, requirements, and testing. It is also imperative that agencies strengthen the planning and management of cloud services, supply chains, and telecommunications services.

Leading IT acquisition and development practices have been developed by both industry and the federal government.⁵⁷ These practices identify key actions that should be taken to effectively and efficiently manage IT project costs, schedules, risks, requirements, and testing. By implementing these practices, agencies can help guide the successful acquisition of IT, thereby increasing the likelihood that systems will meet users' needs and perform as intended. Effective implementation of these practices may also lead to financial benefits for agencies by reducing the risk of cost increases and schedule overruns and enabling agency leadership to make decisions based on quality cost and schedule project control data. However, for decades we have reported on instances of poor program performance that were the results of agencies' inconsistent and incomplete implementation of these practices.

We have also reported on practices that agencies should implement to effectively plan and manage their cloud services, supply chains, and telecommunications. These practices are based on guidance from OMB and the National Institute of Standards and Technology and our prior work. For example, one of the practices is for agencies to establish guidance related to cloud service level agreements (which define the levels of service and performance the agency expects its cloud providers to meet).⁵⁸ Other practices include developing

⁵⁷For example, the Project Management Institute, the Information Systems Audit and Control Association, and the Software Engineering Institute have developed leading practices on project planning, requirements development and management, risk management and testing, among other things. We have also developed guides outlining best practices for developing cost estimates and schedules, and implementing Agile development methodologies. Agile is a form of incremental development.

⁵⁸Office of Management and Budget, *Federal Cloud Computing Strategy* (June 24, 2019).

agency-wide strategies for managing information and communications technology supply chain risks⁵⁹ and developing accurate inventories of telecommunications assets and services.⁶⁰ However, we have reported on limitations in numerous agencies' implementation of these important practices.

What actions should agencies take to improve implementation of leading IT acquisition and development practices to effectively plan and manage IT project costs, schedules, risks, requirements, and testing?

The Small Business Administration needs to implement leading acquisition practices for managing its IT projects' risks, requirements, cost, and schedule.

The Small Business Administration (SBA) administers contracting assistance programs and promotes small business participation in federal contracting through a variety of programs. To certify small businesses for eligibility in its contracting assistance programs, SBA relies on multiple IT systems. However, SBA's past attempts to modernize its IT systems experienced challenges and did not deliver expected results. To help address these shortcomings, in 2023, SBA initiated the Unified Certification Platform project. This project was intended to deploy a new system to allow small businesses to more efficiently apply for and maintain certifications to SBA's contracting assistance programs.

In November 2024, we reported on SBA's efforts to deploy the Unified Certification Platform system.⁶¹ SBA deployed the system on October 18, 2024. However, work remained to develop additional, more complex functionality, secure the system, and migrate data.





Our analyses of SBA's efforts showed that, among other things, leading practices for risk and requirements management and schedule and cost estimation had not been fully implemented (see figure 18).

⁵⁹National Institute of Standards and Technology, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, NIST Special Publication 800-161, Revision 1 (Gaithersburg, MD: May 5, 2022). According to the Federal Acquisition Supply Chain Security Act of 2018, information and communications technology is IT, information systems, and telecommunications equipment and telecommunications services. Examples of such products and services include printed circuit boards, cloud computing services, computing systems, software, satellite communications, and networks.

⁶⁰GAO, *Telecommunications: Full Adoption of Sound Transition Planning Practices by GSA and Selected Agencies Could Improve Planning Efforts*, [GAO-06-476](#) (Washington, D.C.: June 6, 2006).

⁶¹GAO, *IT Modernization: SBA Urgently Needs to Address Risks on Newly Deployed System*, [GAO-25-106963](#) (Washington, D.C.: Nov. 6, 2024).

Figure 18: Extent to Which the Small Business Administration (SBA) Met Selected IT Management Areas for the Unified Certification Platform Modernization (as of November 2024)

IT management area	Overall assessment
Risk management	 Minimally met
Requirements management	 Partially met
Schedule	 Not met
Cost	 Minimally met

Source: GAO analysis of SBA data and all icon illustrations. | GAO-25-107852

Specifically, we identified critical management gaps, including that SBA did not have a project level risk management strategy, a risk mitigation plan, and did not fully identify and document risks. In addition, the agency had not conducted a traceability analysis to ensure project security requirements had been met. Further, the project’s schedule and cost estimates were unreliable and did not follow leading cost and schedule estimating practices. The weaknesses in SBA’s risk, requirements, cost, and schedule management practices were due, in part, to shortcomings in SBA’s policies and procedures.

- **We recommended** that SBA address critical project risk management issues and, among other things, establish and implement policies and procedures to ensure that cost and schedule estimates are developed using leading practices. Of 14 total recommendations, SBA concurred with three, partially concurred with three, and did not concur with eight recommendations. We maintained that the recommendations were warranted. As of December 2024, SBA had not yet implemented any of the recommendations.

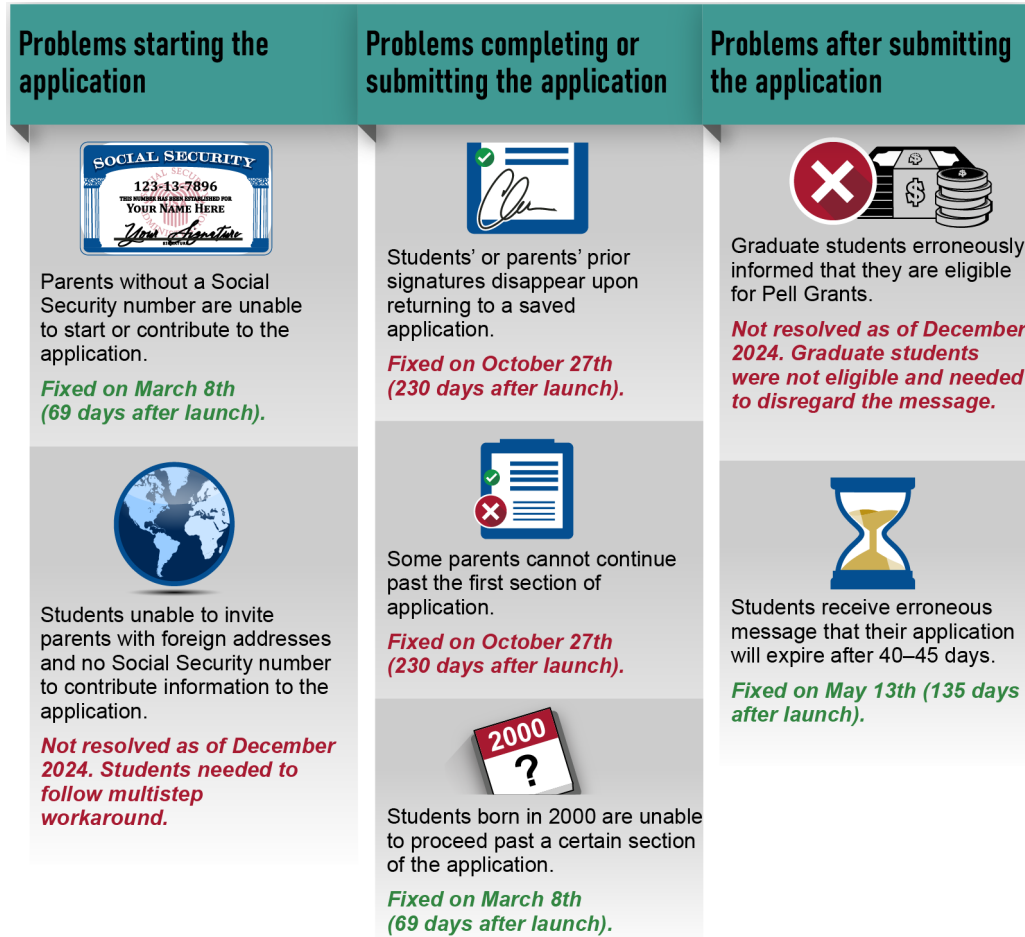
The Department of Education needs to apply disciplined system acquisition practices to its new student aid system.

Students and parents can apply for financial aid by completing the Free Application for Federal Student Aid (FAFSA) form and submitting it to the Department of Education’s Office of Federal Student Aid (FSA). In 2021, FSA initiated an effort to replace the aging system that processes the forms, and in December 2023 the office deployed a new system to process forms for the 2024-2025 school year. However, student aid applicants reported that the new system had availability issues, recurring errors, and long wait times.

In September 2024, we reported that technical problems had impeded students’ ability to complete the FAFSA.⁶² As of August 2024, Education had identified over 40 separate technical issues with the initial rollout of the FAFSA form. These issues included problems that blocked some students from completing the application—or in some cases prevented them from starting it (figure 19 provides examples of the issues users experienced).

⁶²GAO, *FAFSA: Education Needs to Improve Communications and Support Around the Free Application for Federal Student Aid*, GAO-24-107407 (Washington, D.C.: Sept. 24, 2024).

Figure 19: Examples of Technical Issues Affecting the Rollout of the Free Application for Federal Student Aid (FAFSA) (as of December 2024)



Sources: GAO analysis of Department of Education documents and all illustrations; Social Security Administration (logo watermark). | GAO-25-107852

These technical issues led to troubling impacts on students, parents, and schools, including their ability to plan for the upcoming school year. This contributed to about 9 percent fewer high school seniors and other first-time applicants submitting a FAFSA (see figure 20).

Figure 20: Decline in Free Application for Federal Student Aid (FAFSA) Submissions, Current Application Cycle Compared to Prior Year

	High school seniors and other first-time applicants (rounded)		Returning applicants (rounded)		Total applicants (rounded)
<i>Current application cycle</i>	3,177,000	+	11,161,000	=	14,338,000
<i>Change from prior year</i>	↓ 325,000 -9%		↓ 106,000 -1%		↓ 432,000 -3%

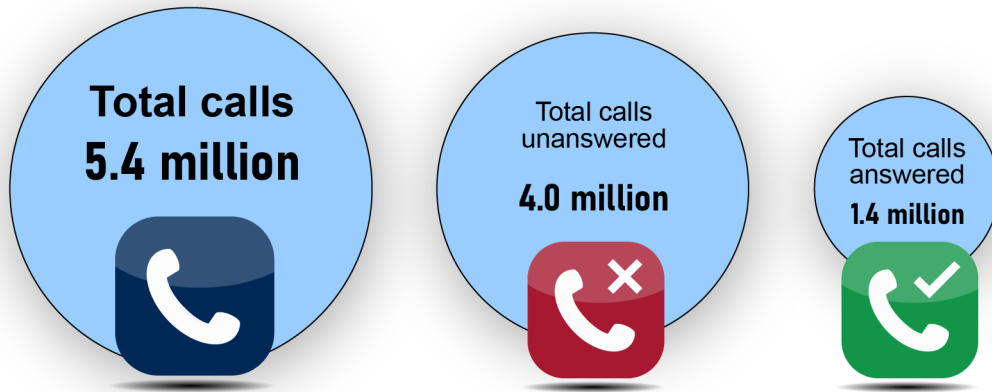
Source: GAO analysis of Department of Education data. | GAO-25-107852

Notes: Numbers may not add up due to rounding. Data are through August 25 of each cycle. The current application cycle refers to applications for the 2024-25 award year and the prior cycle refers to the 2023-24 award year. According to Education, first-time applicants are identified as individuals who

do not have a processed FAFSA from a previous cycle. Education identified high school seniors using several criteria, including those who are no older than 19 years of age and entering college as a freshman with a high school diploma.

In addition, Education did not consistently provide students with timely and sufficient information or support necessary to complete the new FAFSA. Nearly three-quarters of calls to Education’s call center went unanswered during the first 5 months of the rollout due to understaffing (see figure 21).

Figure 21: Total Number of Calls to Education’s Call Center, from January 1, 2024, to May 31, 2024



Sources: GAO analysis of Education data, and all illustrations. | GAO-25-107852

Notes: “Total calls unanswered” is the total of calls that were either automatically disconnected or abandoned by the caller; and “total calls answered” is the total of calls that were answered by a call center agent when offered the call.

In September 2024, preliminary results from our review indicated that FSA identified and reportedly addressed significant defects prior to deploying the new system in December 2023.⁶³ However, the agency also identified numerous defects after deploying it. Specifically, according to documentation compiled in March 2024, the agency identified 55 defects—including seven that were unresolved and categorized as “critical.”

The existence of unresolved defects after system deployment can be traced, in part, to FSA not ensuring disciplined systems acquisition practices were applied. Specifically, FSA did not adequately:

- *Define and manage requirements and carry out testing activities.* FSA guidance states that a requirements oversight review is to be conducted before development begins. However, the agency did not conduct this review until more than a year after development had started. Consequently, FSA completed most development work without assurance that the planned system requirements would fully meet user needs. In addition, FSA authorized system acceptance testing to begin even though 26 of the 48 readiness indicators were not complete—thus increasing the risk that testing would not identify all system problems prior to deployment.
- *Carry out independent acquisition reviews.* One way to manage the risks in acquiring systems is through independent verification and validation. This is a process conducted by a party independent of the acquisition that provides an assessment of a project's processes, products, and risks throughout its life cycle. However, FSA did not establish or implement guidance to carry out independent verification and validation for the new system. In addition, the contractor that performed acquisition reviews for the new system was a subcontractor for the vendor implementing the system—not an independent party. Further,

⁶³GAO, *Department of Education: Preliminary Results Show Strong Leadership Needed to Address Serious Student Aid System Weaknesses*, [GAO-24-107783](#) (Washington, D.C.: Sept. 24, 2024).

FSA did not ensure that this subcontractor fully tested the system code prior to its initial deployment in December 2023. These weaknesses in independent acquisition reviews limited FSA's ability to identify and reduce risks during development of the system.

- **We recommended** that the Department of Education take action to review the FAFSA application process to, among other things:
 - identify ways to reduce the burden on students and families by addressing the remaining technical issues;
 - plan for and ensure hiring of sufficient staff to increase capacity at the FSA call center to be able to meet call demand and improve customer service;
 - adhere to agency policy in managing requirements and testing; and
 - develop policy for independent acquisition reviews.

The department did not agree or disagree with the 13 total recommendations. As of December 2024, none of these recommendations had been implemented.

The Federal Aviation Administration needs to take urgent action to modernize aging air traffic control systems and improve NextGen program management.

The Federal Aviation Administration (FAA), within the Department of Transportation (DOT), safely manages over 50,000 flights daily. Air traffic controllers use a myriad of systems to, among other things, monitor weather, conduct navigation and surveillance, and manage communications. However, recently FAA has been experiencing increasing challenges with aging air traffic control (ATC) systems.

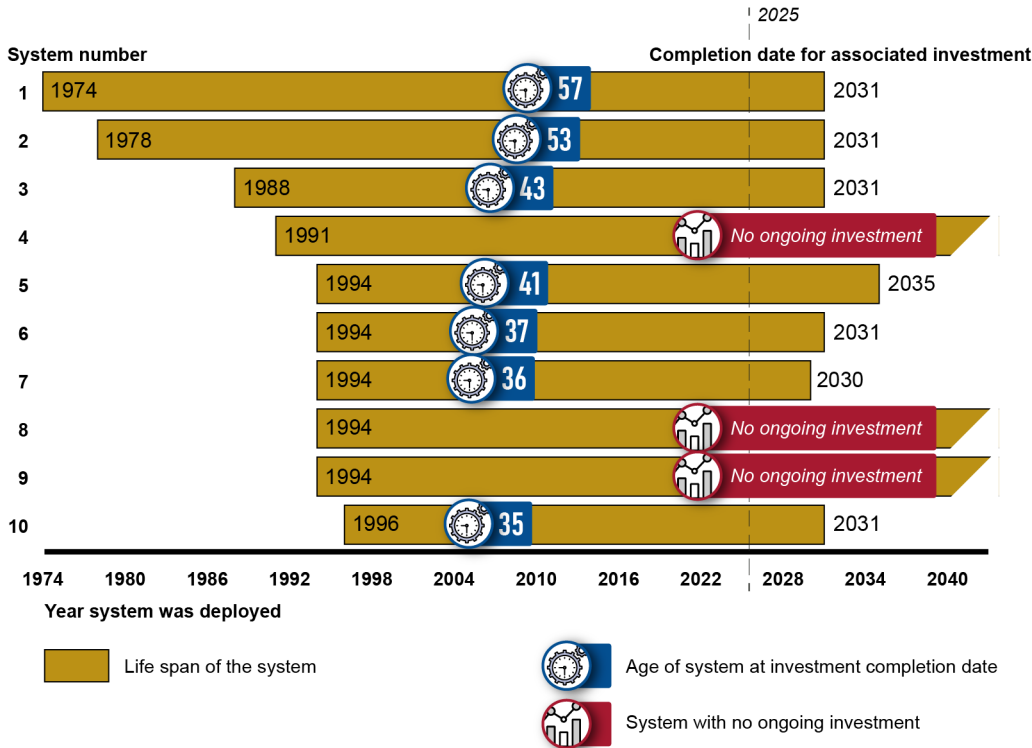
After a shutdown of the national airspace in 2023 due to the outage of an aging ATC system, FAA conducted an operational risk assessment to evaluate the sustainability of all ATC systems. The assessment determined that of its 138 systems, 51 (37 percent) were unsustainable and 54 (39 percent) were potentially unsustainable.⁶⁴ Further, of the 105 unsustainable or potentially unsustainable systems, 58 had critical operational impacts on the safety and efficiency of the national airspace.

In September 2024, we found that FAA had been slow to modernize some of the most critical and at-risk systems.⁶⁵ As of May 2024, FAA had 17 systems that were especially concerning when considering age, sustainability ratings, and operational impact level. However, FAA did not plan to complete modernization efforts of those systems for at least 6 years and, in some cases, they would not be completed for 10 to 13 years. In addition, FAA did not have ongoing investments associated with four of those critical systems and thus it was unknown when the associated systems would be modernized. FAA's reliance on a significant percentage of ATC systems that are unsustainable or potentially unsustainable—76 percent of these systems—introduces risks to FAA's ability to ensure the safe, orderly, and expeditious flow of up to 50,000 flights per day. Figure 22 identifies when FAA expected to complete modernization for 10 of the most critical and at-risk air traffic control systems, as of September 2024.

⁶⁴FAA's assessment of ATC system sustainability generally considered systems as unsustainable if they had significant sparring shortages, shortfalls in funding used to replace aging equipment with in-kind equipment, little or no funding available to refresh technology, and/or significant shortfalls in capability. The assessment identified systems as potentially unsustainable if they had possible shortfalls in capability or funding used to replace aging equipment with in-kind equipment, but had funding available to refresh technology.

⁶⁵GAO, *Air Traffic Control: FAA Actions Are Urgently Needed to Modernize Aging Systems*, [GAO-24-107001](#) (Washington, D.C.: Sept. 23, 2024).

Figure 22: Expected Modernization Completion Dates for 10 of the Most Critical and At-Risk Federal Aviation Administration (FAA) Air Traffic Control Systems (as of September 2024)










Sources: GAO analysis of FAA documentation; 32 pixels/stock.adobe.com (icons). | GAO-25-107852




Moreover, while FAA policy indicates that pre-baselined investments—those that had not yet established a cost, schedule, and performance baseline (which are vitally important for holding investments accountable)—receive limited oversight, many of the 20 selected investments we reviewed that were required to establish such a baseline had been slow to accomplish this. Specifically, the 11 applicable investments took an average of 4 years and 7 months to establish their baselines. In addition, one investment took 6 years and 8 months, and, as of May 2024, two others that were initiated over 6 years ago had not established their baselines. Until FAA establishes a time frame for developing and implementing guidance to increase oversight of pre-baselined investments that require additional resources or time, the agency will continue to experience protracted lengths of time in establishing investment baselines. In addition, until investments establish baselines in an expeditious manner, the agency will be unable to diligently track the execution of plans or mitigate risks.

- **We recommended** that FAA take seven actions to improve its modernization of aging air traffic control systems. Among other things, we recommended that the Administrator of FAA report to Congress on how the agency is mitigating risks of all unsustainable and critical systems that were identified in the annual operational risk assessments. We also recommended that FAA establish a time frame for developing and implementing guidance to increase oversight of pre-baselined investments that require additional resources or time prior to establishing a baseline. DOT concurred with six of the recommendations and partially concurred with one recommendation. As of December 2024, FAA had not yet implemented the seven recommendations.

In November 2023, we reported that program management improvements could help FAA address delays and challenges with its Next Generation Air Transportation System (NextGen).⁶⁶ NextGen is FAA’s multi-decade program to increase the safety and efficiency of air travel by transitioning from a ground-based air traffic control system that uses radar, to a system based on satellite navigation and digital communications. NextGen also relies on many of the legacy systems mentioned earlier that FAA determined to be unsustainable. We found that, since 2018, FAA has made mixed progress meeting implementation milestones for the NextGen program. Further, FAA’s efforts to implement NextGen fully or substantially met four leading practices for program management and partially met five others (see figure 23). Stricter adherence to the leading practices could better position the agency to manage the program.

Figure 23: Extent to Which the Federal Aviation Administration (FAA) Followed Leading Program Management Practices in Managing the Next Generation Air Transportation System (NextGen) Program (as of November 2023)

Leading practices in program management	GAO assessment
Establish a process and database for collecting and sharing lessons learned.	 Fully met
Have an independent oversight body that conducts periodic reviews of the progress of the program.	 Fully met
Develop a program management plan and a roadmap that are updated regularly.	 Substantially met
Establish a reliable, integrated master schedule that is updated on a regular basis. ^a	 Substantially met
Establish a reliable, integrated, comprehensive life-cycle cost estimate that is updated on a regular basis. ^b	 Partially met
Measure program performance against baselines established in an integrated master schedule and against the program’s life-cycle cost.	 Partially met
Conduct program risk management throughout the life of the program and include risk mitigation plans prioritizing risks and analyzing alternatives.	 Partially met
Establish program monitoring and controls, including conducting root cause analyses and developing corrective action plans.	 Partially met
Conduct performance reporting and analysis in a way that provides stakeholders a clear picture of program performance.	 Partially met

-  Fully met = actions have been taken that completely meet the selected practice
-  Substantially met = most but not all actions to meet the selected practice have been taken
-  Partially met = some, but not all, actions necessary to address the practice have been taken

Source: GAO analysis of FAA documentation and interviews and all icon illustrations. | GAO-25-107852

⁶⁶GAO, *Air Traffic Control Modernization: Program Management Improvements Could Help FAA Address NextGen Delays and Challenges*, [GAO-24-105254](#) (Washington, D.C.: Nov. 9, 2023).

^aWe did not assess the reliability of FAA's integrated master schedule.

^bWe did not assess the reliability, integration, or comprehensiveness of FAA's life-cycle cost estimate.

- **We recommended** that FAA take action to improve NextGen program management by addressing the five leading practices it had partially implemented, including, among other things, (1) updating NextGen's life-cycle cost estimate and using it to measure performance (a priority recommendation), and (2) developing a detailed risk mitigation plan to help address challenges to NextGen implementation. FAA concurred with the four total recommendations. As of December 2024, one of the recommendations had been implemented and the other three had not yet been implemented.

The Federal Retirement Thrift Investment Board needs to greatly improve Thrift Savings Plan acquisition management and contractor oversight.

The Thrift Savings Plan (TSP), administered by the Federal Retirement Thrift Investment Board (FRTIB), is the largest retirement plan in the U.S. with about \$895 billion in retirement assets and approximately 7 million participants and beneficiaries. In 2020, FRTIB contracted with a vendor to predominantly own the underlying infrastructure and operate the services for the modernized TSP recordkeeping system.

When the TSP recordkeeping system deployed in 2022, participants encountered a variety of problems (see figure 24). According to FRTIB's vendor, it received about 120,000 calls on the first day of operation. The average wait time went from 35 minutes on the first day to two hours by the third day.

Figure 24: Examples of the Issues Encountered by Thrift Savings Plan (TSP) Participants After System Deployment in 2022



Sources: GAO (analysis and circle illustration); Vladwell/stock.adobe.com (desktop and web browser illustration). | GAO-25-107852

In August 2024, we reported that the FRITB had not fully implemented key acquisition management practices to ensure the success of TSP products and services.⁶⁷ Specifically, while the agency identified its needs and assessed alternatives to meet those needs, it had not:

- developed policies and procedures to govern the way it acquires products and services until after the TSP services acquisition was underway;

⁶⁷GAO, *Thrift Savings Plan: Investment Board Needs to Greatly Improve Acquisition Management and Contractor Oversight*, [GAO-24-106319](#) (Washington, D.C.: Aug. 1, 2024).

- ensured that the new TSP recordkeeping system was consistent with federal requirements for loan repayment, court-ordered benefits, and accessibility;
- verified that the contractor had completed tests in accordance with plans; and
- ensured that all milestones were met before progressing through the acquisition process.

By not fully implementing these practices, FRTIB significantly increased the risk of a problematic rollout of the new system.

- **We recommended** that the FRITB Executive Director take action to improve its acquisition management processes, including developing processes to (1) ensure that any future requirements developed for the new TSP recordkeeping system are consistent with applicable federal requirements and (2) require the FRTIB to review testing documentation to ensure that planned testing is complete and that the solution meets the desired outcome for participants for any system enhancements or upgrades, among other things. FRTIB agreed with our seven recommendations. As of December 2024, none of the recommendations had been implemented.

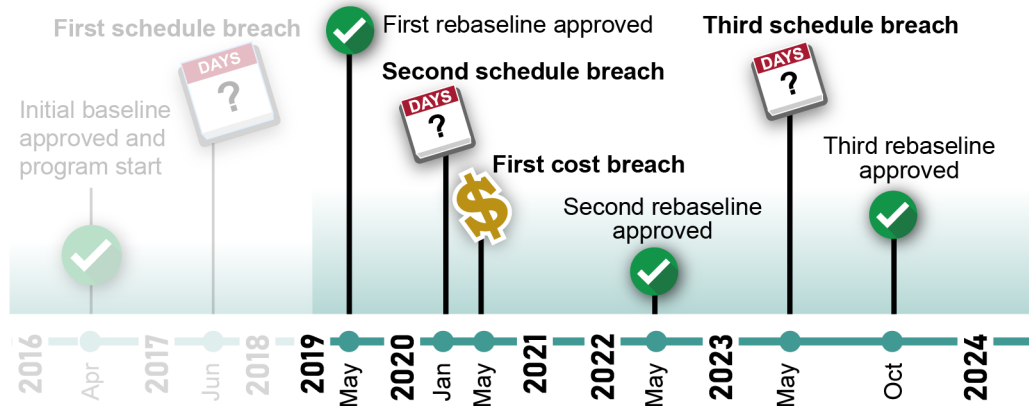
The Department of Homeland Security needs to address significant shortcomings in program management for its modernized biometric identity management system.

The Department of Homeland Security (DHS) currently uses an outdated system, implemented over 30 years ago, for providing biometric identity management services (e.g., fingerprint matching). The system stores over 290 million identities. In 2016, DHS initiated a multi-billion-dollar program known as the Homeland Advanced Recognition Technology (HART), which is intended to replace the legacy system. We previously reported that, due to several challenges, in 2017 the program breached its schedule baseline. In 2019 the program established new cost and schedule commitments with DHS leadership (referred to as a rebaseline). This resulted in delaying the program by 3 years.

In September 2023, we found that, since rebaselining its original cost and schedule commitments in 2019, the HART program has further delayed its schedule.⁶⁸ Specifically, in 2020 the program declared a second schedule breach and its first cost breach. Accordingly, DHS rebaselined the program again. This extended the schedule for delivering the initial capabilities to replace the legacy system by an additional 33 months beyond the 2019 plan. In addition, the 2022 rebaseline did not include an estimate for completing the program. Figure 25 provides a timeline of the HART acquisition program baselines and breaches.

⁶⁸GAO, *Biometric Identity System: DHS Needs to Address Significant Shortcomings in Program Management and Privacy*, [GAO-23-105959](#) (Washington, D.C.: Sept. 12, 2023).

Figure 25: Timeline of Homeland Advanced Recognition Technology (HART) Acquisition Program Baselines and Breaches (as of November 2024)



Source: GAO analysis of Department of Homeland Security data and all icon illustrations. | GAO-25-107852

Regarding costs, the program’s 2022 rebaseline increased its estimated costs by \$354 million. In April 2023, program officials stated that they needed to rebaseline HART’s schedule a third time due to, among other things, higher than expected software defects and performance issues. Moreover, the program’s 2022 cost and schedule estimates did not fully follow our identified cost and schedule best practices and were, therefore, unreliable. Until DHS addresses these weaknesses, the HART cost and schedule estimates will continue to be unreliable.⁶⁹ In turn, this will impair the ability of senior leadership to make informed decisions regarding the program’s future.

- **We recommended** that DHS take action to update the HART program’s cost and schedule estimates to incorporate best practices. DHS concurred with those two recommendations; however, as of December 2024, the recommendations had not yet been implemented.⁷⁰

USDA needs to strengthen program oversight and implement key leading practices for IT modernization in the Farm Production and Conservation mission area.

In 2017, the United States Department of Agriculture (USDA) combined three of its agencies under the Farm Production and Conservation (FPAC) mission area to, among other things, improve customer service for farmers, ranchers, and foresters. In 2018, USDA’s FPAC mission area launched Farmers.gov to provide farmers, ranchers, and foresters with online self-service applications and business tools.

In September 2021, we found that USDA and FPAC had provided minimal oversight of the development of Farmers.gov.⁷¹ Specifically, USDA’s Integrated Advisory Board and Executive Information Technology Investment Review Board—which are responsible for providing executive-level oversight to ensure the accountability and success of IT investments—did not conduct reviews at predefined checkpoints for Farmers.gov, as required by USDA’s governance framework (see figure 26). This lack of oversight had allowed

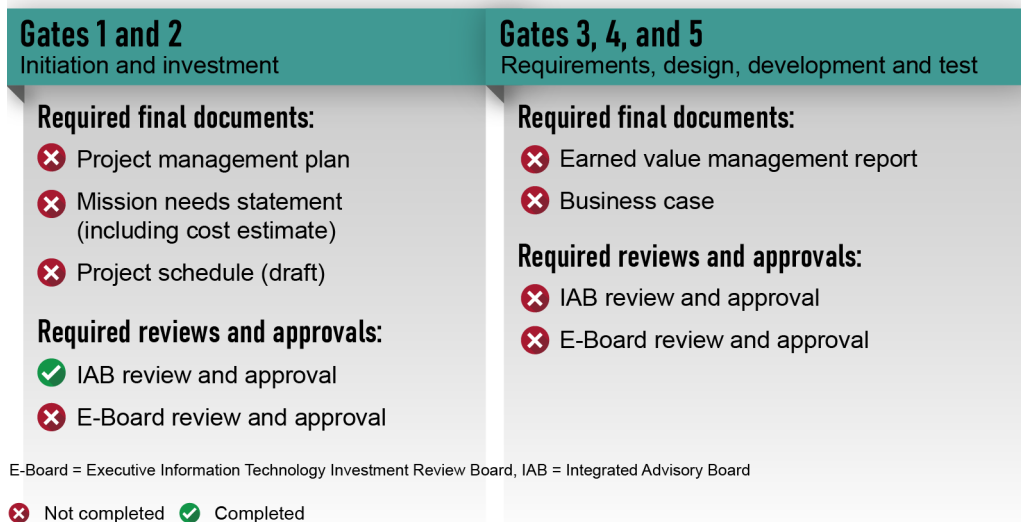
⁶⁹As of December 2024, we have an ongoing review of the HART program’s rebaselined cost estimate and schedule.

⁷⁰In this report, we also made recommendations to DHS to address shortcomings related to privacy requirements that the department had partially implemented for the HART program. We are monitoring DHS’s actions to address these weaknesses as part of the cybersecurity area on GAO’s High-Risk List.

⁷¹GAO, *IT Modernization: USDA Needs to Improve Oversight of Farm Production and Conservation Mission Area*, [GAO-21-512](#) (Washington, D.C.: Sept. 23, 2021). We also made eight recommendations for improving IT workforce planning.

FPAC to proceed without developing key program documentation for Farmers.gov, such as project plans and cost and schedule estimates.

Figure 26: Status of Required Governance Reviews and Key Documentation for the Farm Production and Conservation’s Farmers.gov program (as of April 2021)



Source: GAO analysis of U.S. Department of Agriculture and Farm Production and Conservation mission area data and icon illustrations. | GAO-25-107852

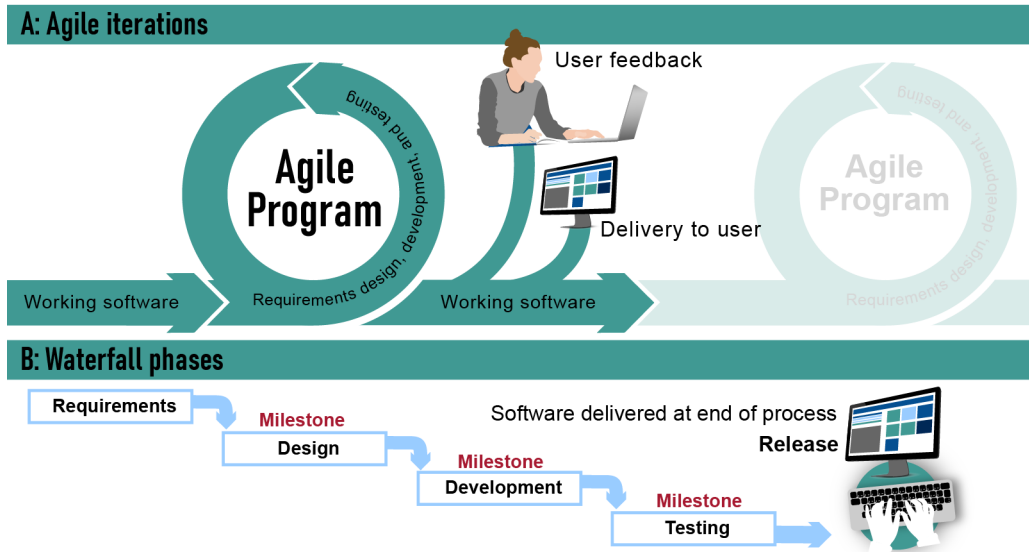
USDA’s and FPAC’s challenges in providing oversight for Farmers.gov were due, in part, to the lack of clearly documented guidance for how a program office should apply Agile development methodologies—a form of incremental development—in a manner that is consistent with the department’s expectations for IT investment oversight. Improving USDA oversight of Farmers.gov and developing repeatable processes that align Agile methodology to USDA’s governance framework could help address these concerns and lead to enhanced service for intended customers.

- **We recommended** that USDA take actions to strengthen IT investment oversight and implement key leading practices that support effective IT modernization. Two of the recommendations were high priority and called for action to improve IT strategic planning and performance measurement for the FPAC mission area. USDA concurred with all of the recommendations and described actions it would take to implement each of them. As of December 2024, 10 of the 15 recommendations—including the two high-priority recommendations—had not yet been implemented.

DHS and DOD need to take additional action to implement leading practices for Agile software development.

Many of DHS’s major IT acquisition programs have taken longer than expected to develop or failed to deliver the desired value. In April 2016, to help improve the department’s IT acquisition and management, DHS identified Agile software development—which is focused on incremental and rapid delivery of working software in small segments—as the preferred approach for all of its IT programs and projects. As shown in figure 27, this quick, iterative approach is to deliver results faster than DHS’s previous waterfall approach that historically delivered usable software years after program initiation.

Figure 27: Comparison of Agile and Waterfall Methods for Developing Software



Source: GAO analysis of U.S. Citizenship and Immigration Services documentation and all icon illustrations. | GAO-25-107852

In June 2020, we found that DHS had addressed four of the nine leading practices that we developed for adopting Agile software development.⁷² For example, the department had modified its acquisition policies to support Agile development methods. However, it needed to take additional steps to, among other things, ensure all staff were appropriately trained and establish expectations for tracking software code quality. By fully addressing leading Agile development practices, DHS can reduce the risk of continued problems in developing and acquiring current, as well as future, IT systems.

- **We recommended** that DHS take action to implement selected leading practices for its transition to Agile software development. DHS agreed with our recommendations. As of December 2024, DHS had implemented eight of our 10 recommendations and had not yet fully implemented two recommendations focused on establishing Agile training requirements.

In addition, we found in July 2024 that 10 selected DOD IT business programs that were actively developing software reported using recommended Agile and iterative approaches, as recommended by the Defense Science Board.⁷³ However, in areas related to tracking customer satisfaction and progress of software development, four of the 10 programs did not use metrics and management tools required by DOD and consistent with GAO’s *Agile Assessment Guide*. As a result, the department risks not having sound information on its Agile software development efforts.

- **We recommended** that DOD ensure that IT business programs developing software use the Agile metrics and management tools required by DOD and consistent with those identified in GAO’s *Agile Assessment*

⁷²GAO, *Agile Software Development: DHS Has Made Significant Progress in Implementing Leading Practices, but Needs to Take Additional Actions*, [GAO-20-213](#) (Washington, D.C.: June 1, 2020).

⁷³GAO, *IT Systems Annual Assessment: DOD Needs to Strengthen Software Metrics and Address Continued Cybersecurity and Reporting Gaps*, [GAO-24-106912](#) (Washington, D.C.: July 11, 2024). DOD’s business systems modernization efforts have been on GAO’s High-Risk List since 1995, in part due to long-standing challenges that the department faces in meeting cost, schedule, and performance commitments, including for its major IT programs.

Guide. DOD agreed with the recommendation. As of December 2024, the recommendation was not yet implemented.

What actions should agencies take to strengthen planning and management of cloud services, supply chains, and telecommunications services?

Agencies need to fully address key procurement requirements in the Federal Cloud Computing Strategy.

Cloud computing can often provide access to IT resources—such as servers that store digital files—through the internet faster and for less money than it would take for federal agencies to own and maintain such resources. As part of a comprehensive effort to transform IT within the federal government, in 2010, OMB began requiring agencies to shift their IT services to a cloud computing service (cloud services) option when feasible.⁷⁴ To accelerate agency adoption of cloud services, in June 2019, OMB published an update to its *Federal Cloud Computing Strategy*, called Cloud Smart.⁷⁵ As part of Cloud Smart, OMB called for agencies to implement five key requirements within the area of procurement to help ensure successful cloud implementation.

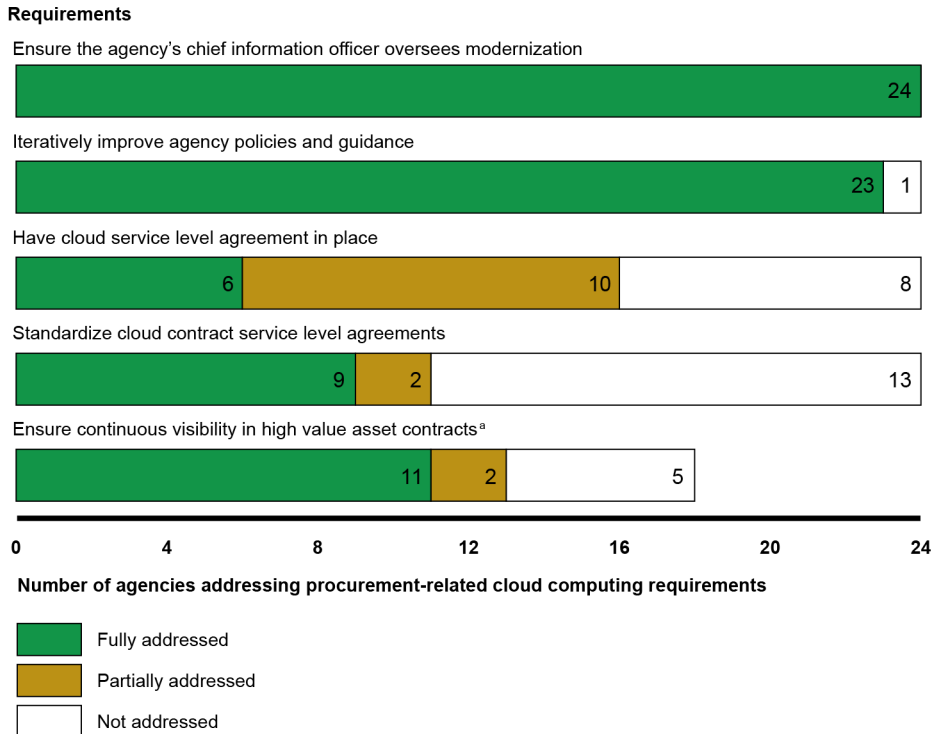
In September 2024, we reported that 24 CFO Act agencies had mixed results in setting policies and guidance that addressed the five key procurement requirements in OMB’s Cloud Smart Strategy (see figure 28).⁷⁶ Specifically, as of July 2024, all 24 agencies had established guidance to ensure the agency CIO oversaw modernization and almost all had guidance in place to improve their policies and guidance related to cloud services. However, most agencies did not establish guidance related to service level agreements, which define the levels of service and performance that the agency expects its cloud providers to meet. In addition, nearly one-third of agencies did not have guidance to ensure continuous visibility in high value assets (systems that process high-value information or serve a critical function in maintaining the security of the civilian enterprise).

⁷⁴Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Dec. 9, 2010).

⁷⁵Office of Management and Budget, *Federal Cloud Computing Strategy* (June 24, 2019). OMB issued the original version of its *Federal Cloud Computing Strategy* in 2011. Office of Management and Budget, *Federal Cloud Computing Strategy* (Feb. 8, 2011).

⁷⁶GAO, *Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements*, [GAO-24-106137](#) (Washington, D.C.: Sept. 10, 2024).

Figure 28: Extent to Which Federal Agencies' Guidance Addressed the Five Procurement-Related Cloud Computing Requirements (as of July 2024)



Source: GAO analysis of agency documentation. | GAO-25-107852

^aThe requirement was not applicable for six agencies because high value assets were not stored in the cloud.

Agency officials provided different reasons as to why guidance had not been developed for the requirements. For example, six agencies reported that they had used service level agreements provided by the cloud service providers. One agency reported that it had included language in its blanket purchase agreement and two agencies reported they were in the process of finalizing guidance. Agency officials reported that additional guidance, including standardized service level agreement language and high value asset contract language, would be helpful. The CIO Council, as a forum for improving agency practices, could facilitate the collection of examples of guidance and language from agencies that have met these requirements.

- **We recommended** that the CIO Council collect and share examples of guidance on cloud service level agreements and contract language. We also made 46 recommendations to 18 agencies to develop or update guidance related to OMB's Cloud Smart procurement requirements. Fourteen agencies agreed with all recommendations, one agency did not explicitly agree but provided planned actions, the CIO Council and three agencies neither agreed nor disagreed, and one agency (the Department of Education) disagreed with our recommendation. We continue to believe our recommendation to Education is warranted. As of December 2024, none of the recommendations had been implemented.

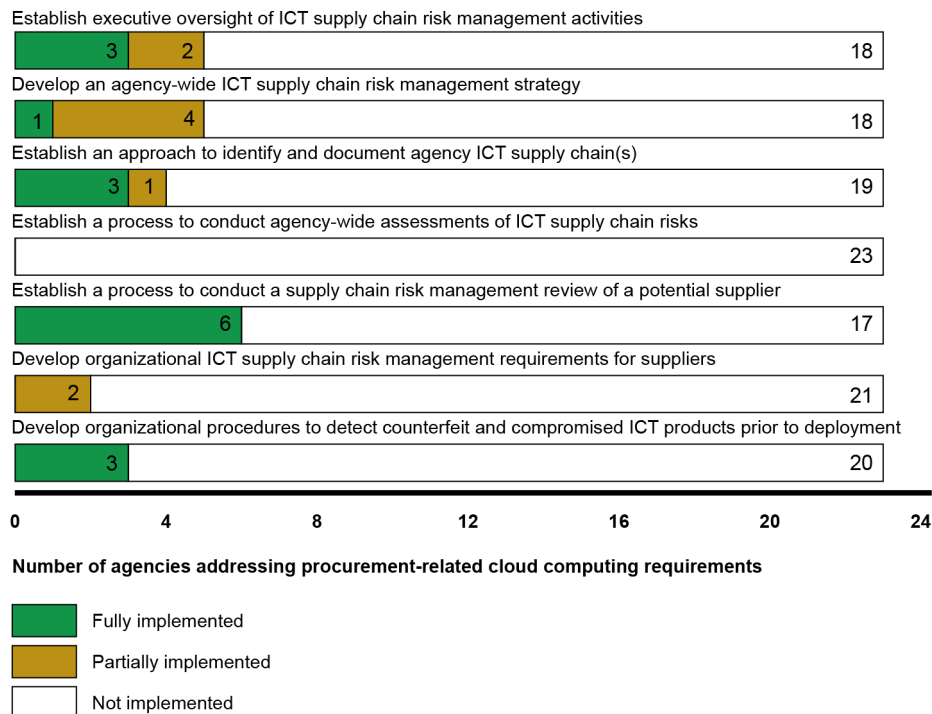
Agencies need to take urgent action to effectively manage supply chain risks.

Federal agencies rely extensively on information and communications technology (ICT) products and services (e.g., computing systems, software, and networks) to carry out their operations. However, agencies face numerous ICT supply chain risks that 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. To address these threats agencies must make risk-based

ICT supply chain decisions about how to secure their systems. 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 December 2020, we reported that none of the 23 civilian CFO Act agencies we reviewed had fully implemented all seven of the selected foundational supply chain risk management practices and 14 had not implemented any of the practices (see figure 29).⁷⁷ Specifically, we found that the practice with the highest rate of implementation—establishing a process to conduct a supply chain risk management review of a potential supplier—was implemented by only six agencies. Conversely, none of the other practices were implemented by more than three agencies. Moreover, one practice—to establish a process to conduct agency-wide assessments of ICT supply chain risks—had not been implemented by any of the agencies.

Figure 29: Extent to Which the 23 Civilian Chief Financial Officers Act Agencies Implemented Information and Communications Technology (ICT) Supply Chain Risk Management Practices (as of December 2020)



Source: GAO analysis of agency data. | GAO-25-107852

⁷⁷GAO, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, [GAO-21-171](#) (Washington, D.C.: Dec. 15, 2020). This report presented a public version of a “limited official use only” report that we issued in October 2020 (GAO, *Information and Communications Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-164SU (Washington, D.C.: October 27, 2020). A number of agencies in our review determined that the information in that report should be protected from public disclosure. Therefore, we did not release that report to the general public because of the sensitive information it contained. The 23 civilian agencies covered by the Chief Financial Officers Act of 1990 and which were included in our review 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; Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

In addition, in May 2023, we reported on DOD's implementation of the same seven selected foundational practices for managing ICT supply chain risks.⁷⁸ Specifically, we found that DOD had fully implemented four of the practices and partially implemented the other three practices. While DOD had begun several efforts to address the three practices that were not fully implemented, these efforts were not yet complete and DOD did not specify time frames for when they would be completed.

As a result of supply chain risk management weaknesses, agencies are at a greater risk that malicious actors could exploit vulnerabilities in the ICT supply chain causing disruption to mission operations, harm to individuals, or theft of intellectual property. Moreover, agencies lack the ability to understand and manage risk and reduce the likelihood that adverse events will occur without reasonable visibility and traceability into supply chains.

➤ **We recommended** that the 23 agencies in our December 2020 report implement the foundational supply chain risk management practices that they had not fully implemented.⁷⁹ Of the 23 agencies, 17 agreed with all of the recommendations made to them; two agencies agreed with most, but not all of the recommendations; one agency disagreed with all of the recommendations; two agencies neither agreed nor disagreed with the recommendations, but stated they would address them; and one agency had no comments. Of the 145 total recommendations we made, as of December 2024, 87 had been implemented and 58 had not yet been implemented.

We also recommended in our May 2023 report that DOD commit to timeframes for fully implementing the remaining foundational practices in its ICT supply chain risk management efforts. DOD concurred with the recommendations. As of December 2024, DOD had implemented one recommendation and had not yet implemented two recommendations.

Agencies need to fully implement established telecommunications transition planning practices.

GSA is responsible for ensuring that federal agencies have access to the telecommunications services and solutions that they need to meet mission requirements. GSA's telecommunications contracts support not only agencies' basic telephone needs, but also provide an acquisition vehicle for wireless and satellite services, as well as managed network services and information IT security services. In preparation for the expiration of the existing telecommunications programs, including one called Networx, GSA developed a successor program, known as Enterprise Infrastructure Solutions (EIS). GSA and agencies need to carry out the task of successfully transitioning to EIS contracts.

In September 2017, we reported that five agencies—the Departments of Agriculture, Labor, and Transportation; the Securities and Exchange Commission, and the Social Security Administration—had partially implemented five established planning practices that can help agencies successfully transition their telecommunications services to new contracts.⁸⁰ These practices are to: (1) develop an accurate inventory of telecommunications services, (2) perform a strategic analysis of telecommunications requirements, (3) develop a structured transition management approach, (4) identify the resources needed for the transition, and (5) develop a transition plan. These five practices have 16 activities associated with them.

In April 2020, we reported that five additional agencies—the Departments of Commerce, Health and Human Services, State, and Veterans Affairs; and the National Aeronautics and Space Administration—had also

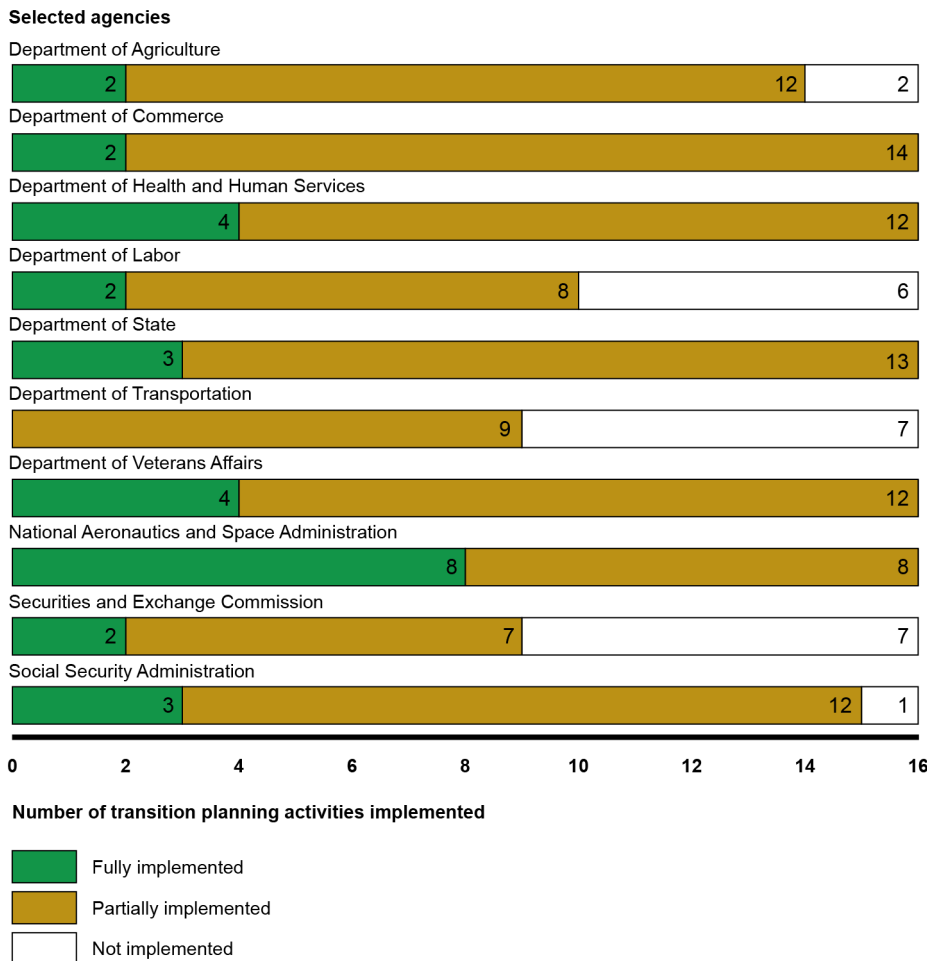
⁷⁸GAO, *Information and Communications Technology: DOD Needs to Fully Implement Foundational Practices to Manage Supply Chain Risks*, [GAO-23-105612](#) (Washington, D.C.: May 18, 2023).

⁷⁹The recommendations were made in the sensitive version of the report issued in October 2020 (GAO-21-164SU).

⁸⁰GAO, *Telecommunications: Agencies Need to Apply Transition Planning Practices to Reduce Potential Delays and Added Costs*, [GAO-17-464](#) (Washington, D.C.: Sept. 21, 2017).

partially implemented the five established planning practices for transitioning to EIS. Across the 10 total agencies whose EIS transition planning practices we assessed in the September 2017 and April 2020 reports, one agency had fully implemented half of the 16 associated transition planning practice activities, two agencies had fully implemented a quarter of the practice activities, and seven agencies had fully implemented less than a quarter of the practice activities (see figure 30).⁸¹

Figure 30: Extent to Which 10 Selected Agencies Fully Implemented 16 Telecommunications Transition Planning Practice Activities



Source: GAO analysis of data provided by agency officials. | GAO-25-107852

These agencies' lack of full implementation of the established planning practices and their associated practice activities increased the risk that they would experience adverse effects—such as schedule delays or cost increases—when transitioning to the new contracts.

- **We recommended** that the 10 selected agencies fully implement the established transition planning practices, among other things. Nine agencies agreed with our recommendations. One agency, the Social Security Administration, agreed with two of its recommendations, partially disagreed with one, and

⁸¹GAO, *Telecommunications: Agencies Should Fully Implement Established Transition Planning Practices to Help Reduce Risk of Costly Delays*, GAO-20-155 (Washington, D.C.: Apr. 7, 2020).

disagreed with two. Of the 49 total recommendations made to these agencies, as of December 2024, 24 recommendations had been implemented and 25 had not yet been implemented.

What ongoing 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 IT acquisition and management efforts in this area. It is essential that executive branch agencies focus on improving implementation of leading IT acquisition and development practices, and strengthen the planning and management of cloud services, supply chains, and telecommunications services. These actions are critical to the federal government’s ability to successfully acquire and implement IT systems and services that provide needed capabilities on time and within budget. Table 2 identifies our ongoing work related to each action associated with this challenge area.

Table 2: GAO’s Ongoing Work Related to the Implementing Mature IT Acquisition and Development Practices Challenge Area (as of December 2024)

Critical action	Related ongoing GAO work
5. Improve implementation of leading IT acquisition and development practices to effectively plan and manage IT project costs, schedules, risks, requirements, and testing.	Reviews of: <ul style="list-style-type: none"> • the extent to which the cost savings estimates for projects awarded funding from the Technology Modernization Fund are reliable; • the essential mission-critical IT acquisitions across the federal government and their key attributes (e.g., cost, schedule, risk level); • the extent to which the Census Bureau implemented leading acquisition practices for a selected enterprise-wide IT modernization program and is managing interdependencies among the Bureau’s upcoming surveys and three enterprise-wide IT programs intended to modernize and consolidate the systems the Bureau uses to carry out the surveys; • the Census Bureau’s development of an enterprise-wide data collection and ingest program; • the extent to which the Department of Defense (DOD) has implemented key software development and cybersecurity practices for selected programs and the actions the department has taken to implement legislative and policy changes that could affect its IT acquisitions; • the extent to which DOD is following leading practices for the modernization of its travel system and for overall improvement of its business systems modernization efforts; • the extent to which the Department of the Navy has developed reliable transition plans for, and is following leading practices in, efforts to modernize its financial management systems; • the extent to which the Department of Homeland Security (DHS) is incorporating key portfolio management practices on its human resources IT investment and addressing any challenges the investment faces; • the extent to which DHS has implemented selected leading collaboration practices within the program implementing its Homeland Advanced Recognition Technology System; • the extent to which DHS has followed best practices for developing reliable cost and schedule estimates for its financial systems modernization programs and the extent to which the department’s data migration and organizational change management activities for these programs are consistent with selected criteria; • the extent to which the Department of Education’s (Education) Office of Federal Student Aid (FSA) applied disciplined systems testing practices prior to deploying the Free Application for Federal Student Aid Processing System and the extent to which Education and FSA provided contract oversight of the effort to develop and deploy that system;

Critical action	Related ongoing GAO work
6. Strengthen the planning and management of cloud services, supply chains, and telecommunications services.	<ul style="list-style-type: none">• the extent to which the Internal Revenue Service has completed plans to implement its vision for IT modernization consistent with best practices and made progress in implementing selected IT modernization programs;• the extent to which the Department of Veterans Affairs (VA) has effectively established plans for acquiring and developing new IT systems to support veterans' appointment scheduling and the reporting of wait times at VA health care facilities;• the extent to which VA has made progress toward improving its new electronic health record system at initial deployment sites;• the extent to which VA's financial and acquisition systems modernization program followed selected leading practices for requirements development and management, independent verification and validation, and cost and schedule management; and• the extent to which the National Aeronautics and Space Administration's and National Oceanic and Atmospheric Administration's collaborative initiative to develop and launch six geostationary satellites adheres to leading planning and management practices. <hr/> <p>Reviews of:</p> <ul style="list-style-type: none">• the extent to which agencies' cloud procurement information is used to inform decision making on cloud acquisitions, the practices that have assisted agencies in procuring cloud services, and the challenges agencies have identified in procuring these services;• leading private sector practices for adopting and implementing cloud computing services, and successes and potential challenges the private sector has faced regarding the adoption and implementation of these services; and• the status of the government-wide transition from legacy telecommunications contracts to new Enterprise Infrastructure Solutions contracts.

Source: GAO. | GAO-25-107852



Building Federal IT Capacity and Capabilities

Overview

Federal agencies rely extensively on IT to carry out operations and their missions. These IT systems provide essential services that are critical to the health, economy, and defense of the nation. However, the federal government has been challenged in building IT capacity and capabilities that are vital to its continued ability to provide these services. To address this challenge, it is critical that agencies address workforce management challenges for the technically-capable workforce, improve federal customer experience for digital services, and ensure effective management of emerging technologies.

We have previously reported that effective workforce planning is key to addressing the federal government's IT challenges and ensuring that agencies have staff with the necessary knowledge, skills, and abilities to execute a range of management functions that support agencies' missions and goals. Further, we have noted that effectively implementing workforce planning activities can facilitate the success of major IT acquisitions.⁸² However, for several years we have reported on significant weaknesses in federal agencies' IT workforce management practices.⁸³

We have also reported that, over time, the manner in which federal agencies provide services to the public has shifted toward digital service delivery, including video conferencing and web-based forms. However, according to OMB, service delivery from agencies has not kept pace with the needs and expectations of those it serves.⁸⁴

Further, we have reported that emerging technologies have the potential to unlock immense societal, environmental, and economic benefits and hold substantial promise for improving government operations.⁸⁵ These technological advancements include, for example, artificial intelligence (AI) (which generally refers to

⁸²GAO, *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps*, [GAO-17-8](#) (Washington, D.C.: Nov. 30, 2016).

⁸³See, for example, GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, [GAO-20-129](#) (Washington, D.C.: Oct. 30, 2019).

⁸⁴Office of Management and Budget, *The Biden-Harris Management Agenda Vision* (Washington, D.C.: November 2021).

⁸⁵For the purposes of this report, we consider emerging technologies to be novel technologies, or new applications of pre-existing technologies, with far-reaching, disruptive potential, and risks and benefits that are not yet fully known.

computing systems that “learn” how to improve their performance) and quantum IT (which build on quantum physics to process and communicate information in ways that existing technologies cannot). However, such technologies also pose risks that can negatively impact individuals, groups, and society. For example, AI systems may be trained on data that can change over time, sometimes significantly and unexpectedly, affecting system functionality and trustworthiness. These technological advancements can often cross multiple agencies’ jurisdictions and multiple sectors of the economy. As such, interagency coordination efforts are important to share knowledge to better anticipate and understand the implications of emerging technologies, and to appropriately prevent and manage duplication and overlap.

What actions should agencies take to address workforce management challenges for the technically-capable workforce?

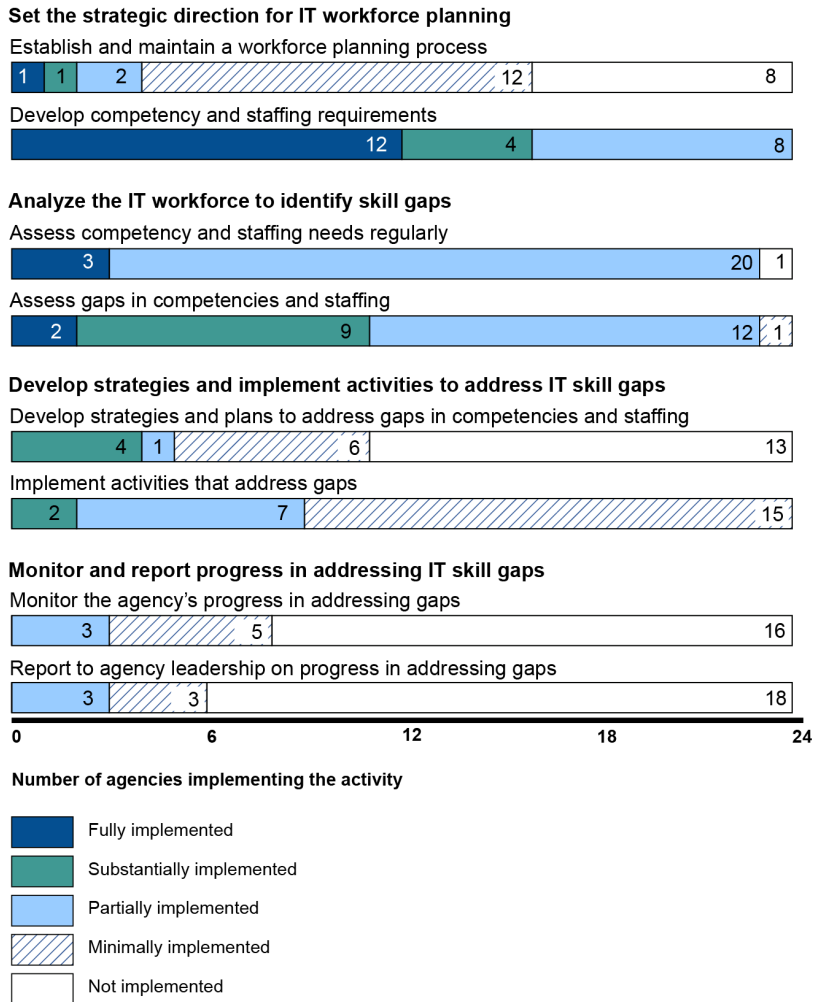
Federal agencies need to fully implement key IT workforce planning activities.

We previously issued an IT workforce planning framework that includes eight key activities, based on federal laws, guidance, and best practices. Implementing these activities is critical to adequately assessing and addressing gaps in IT and technical knowledge, skills, and abilities that are needed to execute a range of management functions that support agencies’ missions and goals.

In October 2019, we found that federal agencies varied widely in their efforts to implement the eight key IT workforce planning activities.⁸⁶ Specifically, at least 23 of the 24 agencies reviewed had partially implemented, substantially implemented, or fully implemented three of the eight key IT workforce activities, including assessing gaps in competencies and staffing. However, most agencies had minimally implemented or had not implemented five other workforce planning activities, including efforts to establish a workforce planning process and address staffing gaps (see figure 31). None of the 24 agencies that we reviewed had fully implemented all eight IT workforce planning activities.

⁸⁶GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, [GAO-20-129](#) (Washington, D.C.: Oct. 30, 2019).

Figure 31: Agencies' Overall Implementation of the Key IT Workforce Planning Activities (as of May 2019)



Source: GAO analysis of agency information technology workforce planning policies and documentation. | GAO-25-107852

Agencies provided various reasons for their limited progress in implementing workforce planning activities, including competing priorities (four agencies) and limited resources (three agencies). Until agencies make it a priority to fully implement all key IT workforce planning activities, they will likely have difficulty anticipating and responding to changing staffing needs and controlling human capital risks when developing, implementing, and operating critical IT systems.









- **We recommended** that 18 of the agencies fully implement the remaining key IT workforce planning activities. Thirteen of the agencies agreed with the recommendations, one partially agreed, and three neither agreed nor disagreed. One agency disagreed with the findings and provided evidence which led to a modification to its recommendation (we modified the recommendation from needing to fully implement eight activities the agency had not implemented to fully implementing seven activities). As of December 2024, 16 of the 18 agencies had fully implemented the recommendations, and two agencies had partially implemented the recommendations.

The National Institutes of Health needs to implement key workforce planning activities for its data science workforce.

The National Institutes of Health (NIH) is the federal government’s leader in supporting biomedical research. The agency had faced a shortage of employees with data science expertise needed to, among other things, analyze and extract insights from increasingly large and complex sets of data. In June 2018, NIH developed a Strategic Plan for Data Science, which included an objective to enhance its data science workforce.

In June 2023, we found that while NIH included a data science workforce goal in its June 2018 Strategic Plan for Data Science, the agency had not fully implemented the eight key workforce planning activities that we previously identified are needed for effective workforce planning (see figure 32).⁸⁷ For example, NIH developed and implemented plans to enhance its data science workforce. However, NIH had not analyzed its workforce to determine what gaps in data science competencies and staffing it may have; as such, the plans to enhance its data science workforce were not linked to any such gaps.

Figure 32: National Institutes of Health’s (NIH) Implementation of Key Activities for Data Science Workforce Planning (as of June 2023)

Key workforce planning practices	Supporting activities	Rating
Set the strategic direction for workforce planning	Establish and maintain a workforce planning process	 Partially implemented
	Develop competency and staffing requirements	 Partially implemented
Analyze the workforce to identify skill gaps	Reassess competency and staffing needs regularly	 Not implemented
	Determine gaps in competencies and staffing regularly	 Not implemented
Develop and implement strategies to address skill gaps	Develop strategies and plans to address gaps in competencies and staffing	 Partially implemented
	Implement activities that address gaps	 Partially implemented
Monitor and report progress in addressing skill gaps	Monitor the agency’s progress in addressing competency and staffing gaps	 Not implemented
	Report to agency leadership on progress in addressing competency and staffing gaps	 Not implemented

Source: GAO analysis of NIH documentation and all icon illustrations. | GAO-25-107852

Fully addressing the workforce planning activities would help ensure that NIH has the data science workforce it needs to effectively meet its mission.

⁸⁷GAO, *Data Science: NIH Needs to Implement Key Workforce Planning Activities*, [GAO-23-105594](#) (Washington, D.C.: June 22, 2023).

-
- **We recommended** that NIH fully implement the eight key workforce planning activities for its data science workforce, among other things. NIH concurred with the recommendations. As of December 2024, NIH had fully addressed one of the recommendations, partially addressed three recommendations, and had not addressed the other four recommendations related to implementing the workforce planning activities.

What actions should agencies take to improve federal customer experience for digital services?

Federal agencies need to modernize government websites and digital services to improve customer experience.

Federal legislation and guidance have focused attention on agencies' efforts to enhance and improve customer experience, particularly in digital spaces. Recent among these efforts was the December 2018 passage of the *21st Century Integrated Digital Experience Act* (21st Century IDEA).⁸⁸ This act was intended to improve public-facing federal digital services. The act required federal websites and digital services to meet eight modernization requirements, including being accessible, consistent, and encrypted (secured connections). The act also required agencies to submit five annual reports between December 2019 and December 2023 that discussed their implementation of the eight website and digital service modernization requirements.

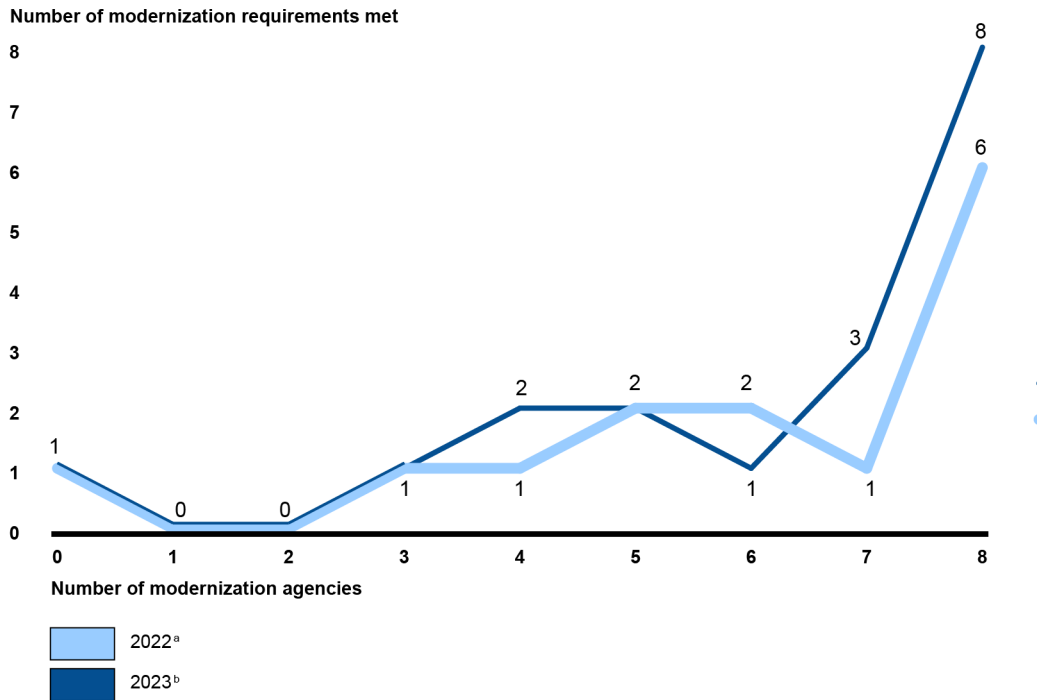
In September 2024, we found that the annual reports submitted by federal agencies in 2022 and 2023 did not consistently address the implementation of the eight modernization requirements.⁸⁹ Specifically, in 2022, 14 agencies submitted reports. Of these 14 agencies, six addressed all eight requirements, one did not address any requirements, and the remaining seven agencies addressed between three and seven of the requirements. Ten agencies did not submit their 2022 annual reports, so their progress towards meeting the eight requirements was unreported and, therefore, unknown.

In addition, in 2023, 18 agencies submitted their annual reports. Of these 18 agencies, eight addressed all eight requirements, one did not address any, and the remaining agencies addressed between three and seven of the requirements. Six other agencies did not submit 2023 reports. Figure 33 shows the extent to which the 24 agencies submitted reports in 2022 and 2023 that addressed the eight modernization requirements.

⁸⁸Pub. L. No. 115-336, 132 Stat. 5025 (2018) (44 U.S.C. § 3501 note).

⁸⁹GAO, *Digital Experience: Agency Compliance with Statutory Requirements*, [GAO-24-106764](#) (Washington, D.C.: Sept. 27, 2024).

Figure 33: Extent to Which 24 Agencies' Submitted Reports in 2022 and 2023 Addressed the Eight Modernization Requirements from the 21st Century Integrated Digital Experience Act



Source: GAO analysis of agencies' submitted 2022 and 2023 21st Century Integrated Digital Experience Act annual reports. | GAO-25-107852 ^aTen of the 24 agencies did not submit reports in 2022.

^bSix of the 24 agencies did not submit reports in 2023.

OMB issued guidance in September 2023 that clarified compliance with the modernization requirements by describing a number of actions that agencies should perform.⁹⁰ Continued oversight consistent with this guidance would likely provide an assessment of the extent of progress towards delivering better digital services to the public.

The Internal Revenue Service needs to improve information on costs and benefits of the Direct File system and expand access to it.

Beginning in 2024, the Internal Revenue Service (IRS) started offering a new online service called Direct File to assist individual taxpayers in preparing and electronically filing their tax returns at no cost. The Inflation Reduction Act of 2022 directed the IRS to report on the cost of developing and running a system that would allow taxpayers to prepare and file their tax returns for free on irs.gov.⁹¹ Once mature, such a tax filing system could save taxpayers time and money, make it easier to claim tax benefits, and provide several benefits to IRS.

In May 2023, IRS initially reported to Congress that the annual costs for developing and running such a system could range from \$64 million to \$249 million depending on the number of taxpayers served and the complexity of tax situations supported. IRS noted several uncertainties in the estimates, such as the number of taxpayers who may choose to use the Direct File system.

⁹⁰Office of Management and Budget, *Delivering a Digital-First Public Experience*, M-23-22 (Washington, D.C.: Sept. 22, 2023).

⁹¹Pub. L. No. 117-169, § 10301(1)(B), 136 Stat. 1818, 1832 (Aug. 16, 2022).

Also in May 2023, the Deputy Secretary of the Treasury directed IRS to pilot a Direct File system during the 2024 tax filing season. The pilot was conducted between February and April 2024 and allowed certain taxpayers to prepare and file their tax returns for free on irs.gov (we discuss the pilot in more detail later).

In April 2024, we identified opportunities for IRS to use the Direct File pilot to improve the agency's initial cost and benefit estimates.⁹² We found that the cost estimates that IRS had provided to Congress in May 2023 were not comprehensive and did not fully align with best practices for cost estimation. IRS's cost estimates addressed certain recommended practices, such as describing underlying assumptions for the estimates to help inform decision-makers of the estimate's scope. However, IRS's cost estimates did not address other recommended practices, such as ensuring all costs were included and documented. We also found that IRS risked missing opportunities to use the pilot to improve cost and benefit estimates for Direct File.

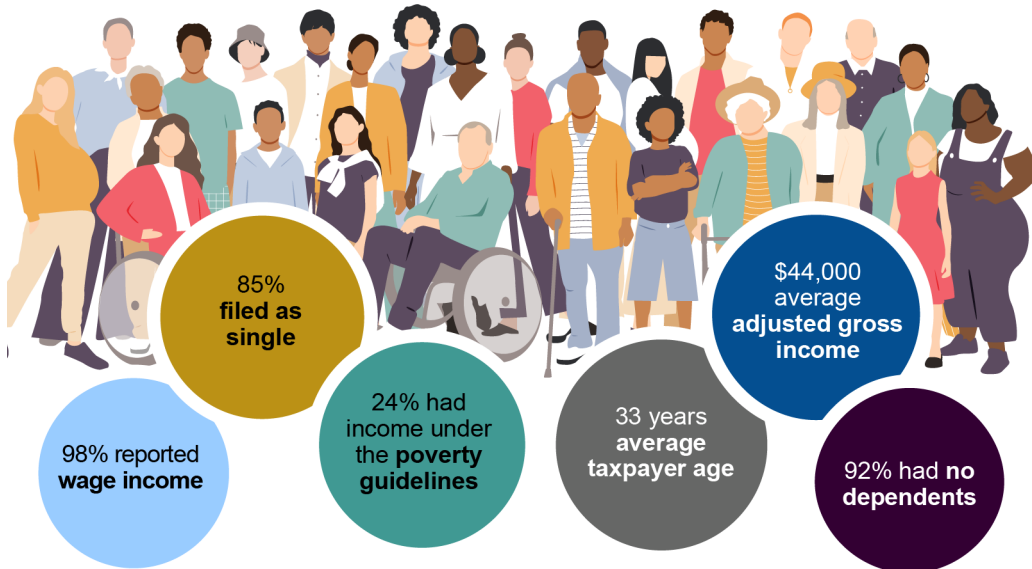
➤ **We recommended** that IRS (1) apply best practices to estimate and document the full costs of developing and operating a Direct File system, (2) estimate and document potential benefits of the system, and (3) use cost and benefit data collected during the pilot to inform future decisions about the system. IRS agreed with the recommendations. As of December 2024, IRS had implemented the recommendation to use cost and benefit data collected during the pilot to inform future decisions about the system and had not yet fully implemented the other recommendations.

In December 2024, we reported that IRS had successfully piloted Direct File from February to April 2024 for taxpayers with simple tax situations residing in one of 12 states.⁹³ Taxpayers reported that Direct File was an easier tax preparation method than they had previously used, a factor that contributed to IRS's decision to make Direct File a permanent filing option starting with the 2025 filing season. Figure 34 shows selected demographics of the Direct File taxpayers during the 2024 filing season.

⁹²GAO, *IRS Direct File: Actions Needed during Pilot to Improve Information on Costs and Benefits*, [GAO-24-107236](#) (Washington, D.C.: Apr. 9, 2024).

⁹³GAO, *Direct File: IRS Successfully Piloted Online Tax Filing but Opportunities Exist to Expand Access*, [GAO-25-106933](#) (Washington, D.C.: Dec. 19, 2024). The pilot was available to people who resided in one of the following 12 states: Arizona, California, Florida, Massachusetts, New Hampshire, New York, Nevada, South Dakota, Tennessee, Texas, Washington, and Wyoming.

Figure 34: Demographics of Direct File Taxpayers During the 2024 Filing Season



Sources: Internal Revenue Service (IRS); Stafeeva/stock.adobe.com (people). | GAO-25-107852

IRS reported in May 2024 that it had spent \$13 million on the 2024 Direct File and estimated that another federal agency—the U.S. Digital Service—used \$7.2 million of its own appropriated funds to support the pilot. In total, IRS estimated that the pilot cost the federal government \$20.2 million.

We also found that IRS followed leading practices in piloting the system, including identifying learning objectives and collecting relevant data such as customer service requests. However, IRS was behind schedule in recruiting and training customer services representatives for the 2025 filing season due, in part, to insufficient coordination among IRS offices. In addition, IRS limited participation in Direct File to taxpayers who live in certain states, which facilitated coordination between federal and state tax filing. However, IRS could face challenges in reaching agreements with all states, which raises equity concerns for taxpayers unable to access Direct File due to where they live.

Further, we found that selected revenue agencies in other countries and Puerto Rico had prepopulated tax returns with information already on file, such as wages reported by employers. IRS began offering limited prepopulation in April 2024 during the pilot. IRS officials told us that they were considering additional prepopulation of taxpayer data, but were still in the early stages of planning. Identifying additional data for prepopulation in Direct File and developing a plan for testing its accuracy could enable IRS to reduce taxpayer burden.

- **We recommended** that IRS improve coordination among relevant offices to ensure the recruitment of customer support employees, open Direct File to all eligible taxpayers in the future, and identify additional data that could be prepopulated in Direct File and test its accuracy, among other things. IRS agreed with three of our four recommendations and neither agreed nor disagreed with the other recommendation. As of December 2024, it had not yet implemented them.

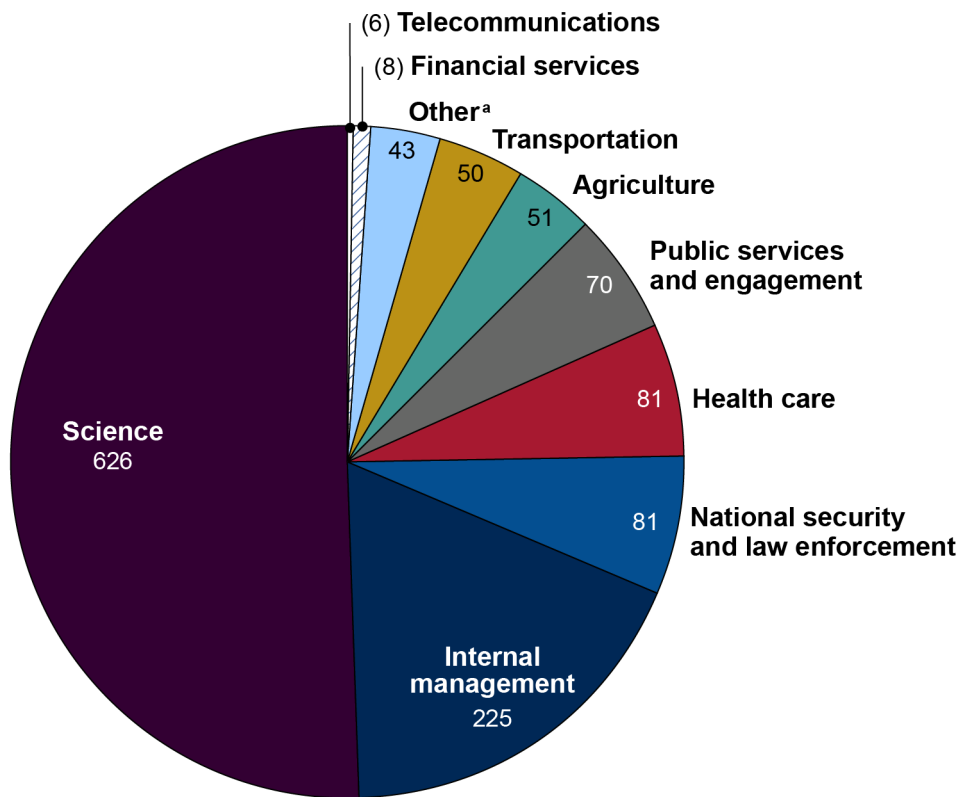
What actions should agencies take to ensure effective management of emerging technologies?

Agencies need to complete key requirements for implementing artificial intelligence.

In December 2023, we found that 20 of 23 agencies reported about 1,200 established and planned AI use cases—specific challenges or opportunities that AI may solve.⁹⁴ The other three agencies reported not having uses for AI. Most of the reported AI use cases were in the planning phase and not yet in production (i.e., currently used).

We also found that agencies were using AI in various areas, such as agriculture, financial services, health care, and national security and law enforcement. Science and internal management were the two most common use case types identified and represented about 69 percent of the use cases. Figure 35 displays the various areas in which agencies were using AI.

Figure 35: Artificial Intelligence (AI) Use Case Application Areas (as of December 2023)



Source: GAO analysis of agency AI use case inventory submissions to Office of Management and Budget. | GAO-25-107852

^a“Other” includes AI use cases that did not clearly fit into one of the identified use case types.

In addition, although the 20 agencies that developed AI use case inventories submitted them to OMB consistent with guidance from the federal CIO Council, they did not always identify and follow requirements within the CIO Council’s guidance. Specifically, our analysis found that five agencies provided comprehensive

⁹⁴GAO, *Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements*, [GAO-24-105980](https://www.gao.gov/products/GAO-24-105980) (Washington, D.C.: Dec. 12, 2023).

information for each of their reported use cases while the other 15 had instances of incomplete and inaccurate data. For example, some inventories did not include required data elements, such as the AI life cycle stage. In addition, two inventories included AI uses that were later determined by the agencies to not be AI. Maintaining comprehensive and accurate AI use case inventories with quality information is critical for the government to have awareness of its AI capabilities and for agency leaders to make important decisions. Without an accurate inventory, the government's implementation, oversight, and management of AI can be based on faulty data.

- **We recommended** that 19 agencies, including OMB, take steps to fully implement federal AI requirements. Among other things, we recommended that 15 agencies update their AI use case inventories to include required information and take steps to ensure the data aligns with guidance. Of the 19 agencies, 10 agreed with their recommendations; three partially agreed with one or more recommendations; four neither agreed nor disagreed; and two disagreed with one of their recommendations. As of December 2024, of the 35 total recommendations made, four had been implemented and 31 had not yet been implemented.

In September 2024, we found that applicable agencies had fully implemented 13 selected management and talent requirements for AI that were due to be implemented by the end of March 2024, as outlined in Executive Order 14110.⁹⁵ By implementing the selected requirements, the federal government should be better positioned to increase its AI workforce, effectively coordinate AI activities across agencies, rapidly increase AI talent, and allocate that talent to high priority mission areas.

Leadership is needed to fully define a quantum computing threat mitigation strategy.

Since 2018, we have reported on the emergence of quantum technology, which builds on the study of the smallest particles of energy and matter to collect, generate, and process information in ways not achievable with existing technologies.⁹⁶ Such technology offers potentially significant benefits, including dramatically increased processing speed compared to a normal, or classical, computer, potentially solving problems that are intractable on a classical computer. Such technology could also have applications in several fields, including medicine, manufacturing, artificial intelligence, defense, and improved cybersecurity.

However, potential drawbacks of quantum technology also exist, including the possibility for malicious use. For example, quantum computers could undermine the security of current, widely used cryptography (e.g., encryption), such as those used for secure website connections.⁹⁷ These current cryptographic methods rely on complex mathematics that are nearly impossible for classical computers to break in reasonable time frames. Quantum computers, in contrast, could break certain types of cryptographic methods in exponentially shorter times because of key differences in information processing.













⁹⁵GAO, *Artificial Intelligence: Agencies Are Implementing Management and Personnel Requirements*, [GAO-24-107332](#) (Washington, D.C.: Sept. 9, 2024) and Exec. Order 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (Oct. 30, 2023). The order was intended to advance and govern the development of AI in accordance with eight guiding principles and priorities, including ensuring the safety and security of AI technology, promoting innovation and competition, supporting workers, and advancing federal government use of AI.

⁹⁶See, for example, GAO, *Quantum Computing and Communications: Status and Prospects*, [GAO-22-104422](#) (Washington, D.C.: Oct. 19, 2021); *Science & Tech Spotlight: Quantum Technologies*, [GAO-20-527SP](#) (Washington, D.C.: May 28, 2020); *Science and Technology: Considerations for Maintaining U.S. Competitiveness in Quantum Computing, Synthetic Biology, and Other Potentially Transformational Research Areas*, [GAO-18-656](#) (Washington, D.C.: Sept. 26, 2018).

⁹⁷We reported on this concern as part of our ongoing work focused on cybersecurity challenges facing the nation—another critical area on GAO's High-Risk List. See, for example, GAO, *Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight*, [GAO-23-106415](#) (Washington, D.C.: Jan. 19, 2023).

In November 2024, we reported on the U.S. national strategy for addressing the threat of quantum computing to cryptography on unclassified systems.⁹⁸ Specifically, we found that the government’s quantum cybersecurity strategy documents partially addressed each of the six desirable characteristics of a national strategy (see figure 36).

Figure 36: Assessment of the Extent to Which the Federal Government’s Quantum Cybersecurity Strategy Documents Addressed GAO’s Desirable Characteristics of a National Strategy (as of November 2024)

Characteristics of a desirable national strategy	Assessment
 <p>Purpose, scope, and methodology Describes why the strategy was produced, the scope of its coverage, and the process by which it was developed.</p>	 Partially implemented
 <p>Problem definition and risk assessment Identifies the national problems and threats the strategy is directed toward and analyzes threats to, and vulnerabilities of, critical assets and operations.</p>	 Partially implemented
 <p>Objectives, activities, milestones, and performance measures Defines the objectives identifying what the strategy is trying to achieve, and activities to achieve those results, as well as the priorities, milestones, and performance measures to gauge results.</p>	 Partially implemented
 <p>Resources, investments, and risk management Summarizes what the strategy’s implementation will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted by balancing risk reductions and costs.</p>	 Partially implemented
 <p>Organizational roles, responsibilities, and coordination Describes who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts.</p>	 Partially implemented
 <p>Implementation and integration Addresses how a national strategy is to be implemented and how the document relates to other strategies’ goals, objectives, and activities—including international strategies.</p>	 Partially implemented

Sources: GAO analysis of relevant documents that comprise the U.S. national quantum computing cybersecurity strategy and shield icon illustrations; SMUX/stock.adobe.com (icons). | GAO-25-107852

A fully comprehensive strategy will provide the nation a better-defined roadmap for allocating and managing resources and holding participants accountable for achieving results.

- **We recommended** that the National Cyber Director (1) lead the coordination of the national quantum computing cybersecurity strategy and (2) ensure that the strategy’s various documents address all the desirable characteristics of a national strategy. The Office of the National Cyber Director did not agree or

⁹⁸GAO, *Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy*, [GAO-25-107703](#) (Washington, D.C.: Nov. 21, 2024).

disagree with the recommendation. As of December 2024, the recommendation had not yet been implemented.

What ongoing 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 IT acquisition and management efforts in this area. It is essential that executive branch agencies focus on addressing workforce management challenges for the technically-capable workforce, improve federal customer experience for digital services, and ensure effective management of emerging technologies. These actions are critical to the federal government’s ability to successfully acquire IT systems and support essential services that are vital to the health, economy, and defense of the nation. Table 3 identifies our ongoing work related to each action associated with this challenge area.

Table 3: GAO’s Ongoing Work Related to the Building Federal IT Capacity and Capabilities Challenge Area (as of December 2024)

Critical action	Related ongoing GAO work
7. Address workforce management challenges for the technically-capable workforce.	Reviews of: <ul style="list-style-type: none"> • the extent to which the Social Security Administration’s efforts for its acquisition workforce supporting IT contracts align with leading practices for strategic workforce planning; • the extent to which selected agencies have implemented applicable cybersecurity workforce management practices and evaluated the effectiveness of their actions to mitigate cybersecurity workforce management challenges; and • the extent to which civilian agencies evaluated the effectiveness of their existing cyber workforce initiatives and whether to expand those initiatives.
8. Improve federal customer experience for digital services.	A review of the extent to which selected agencies’ telework practices and plans align with selected key practices for an effective telework program, and how telework has affected the agencies’ ability to provide high impact services to the public.
9. Ensure effective management of emerging technologies.	Reviews of: <ul style="list-style-type: none"> • the extent to which the federal government has developed an artificial intelligence (AI) national strategy; • selected agencies’ AI procurement-related challenges and workforce issues, and the extent to which the agencies’ AI governance frameworks address key procurement and workforce challenges; and • the Internal Revenue Service’s management of its AI portfolio.

Source: GAO. | GAO-25-107852

Continued Implementation of Our Recommendations Is Needed to Address IT Acquisition and Management Weaknesses

In conclusion, since 2010, we have made over 1,800 recommendations to OMB and federal agencies aimed at improving their management of IT. Nevertheless, many agencies continue to be challenged in effectively acquiring IT and managing IT projects, in part because many of these recommendations have not been implemented. Of the 1,881 recommendations made since 2010 related to this high-risk area, 463 had not been implemented as of January 2025. We have also designated 69 as priority recommendations, and as of January 2025, 32 had not been implemented. If the agencies fully implement all recommendations that have not yet been implemented, we estimate they could potentially achieve hundreds of millions in savings.

The federal government is dependent on IT systems to provide essential services that are critical to the health, economy, and defense of the nation. Given the increasing number of services that the federal government provides to the public by digital means—from filing tax returns to applying for student loans and retirement benefits to enabling veterans to access their medical records online—it is crucial that these services perform as intended to meet citizens' needs. Ineffective management of IT investments and poor performance by systems used for providing digital services can have serious negative implications—eroding public trust in the government, wasting taxpayer dollars, and preventing citizens from getting essential services.

While legislation and executive branch initiatives have been aimed at improving the management of federal IT, OMB's and agencies' implementation of these efforts has been inconsistent. Urgent actions are needed to address the ongoing challenges that the government faces in effective and efficient IT acquisition and management. Specifically, the government needs to strengthen oversight and management of IT portfolios; address weaknesses in agencies' IT acquisition and development practices; and build federal IT capacity and capabilities. Until OMB and federal agencies take the critical actions we identified, they will continue to struggle with IT acquisitions that fail to consistently deliver capabilities in a timely manner, incur cost overruns and/or schedule slippages, and contribute little to mission-related outcomes. The federal government will also be challenged in maximizing the benefits from its substantial investment in IT.

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) 512-4456 or HarrisCC@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.



Carol C. Harris
Director, Information Technology Acquisition Management Issues

Appendix I: Prior GAO Work on IT Acquisitions and Management

We have previously reported on the numerous challenges that the federal government faces in improving its IT acquisitions and management and have made recommendations aimed at addressing these challenges. This appendix identifies the selected GAO products discussed throughout this report that address each of the three challenge areas and associated critical actions.

Challenge 1: Strengthening Oversight and Management of IT Portfolios

Critical action 1: Improve the effectiveness of key IT leadership positions, including the Federal Chief Information Officer (CIO), agency CIOs, and agency chief artificial intelligence officers.

- [GAO-22-104603](#) Chief Information Officers: Private Sector Practices Can Inform Government Roles | U.S. GAO
- [GAO-18-93](#) Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities | U.S. GAO

Critical action 2: Enhance agency efforts to strategically plan for and manage portfolios of IT systems, applications, and software licenses, and to manage existing IT system operations.

- [GAO-25-107041](#) IT Portfolio Management: OMB and Agencies Are Not Fully Addressing Selected Statutory Requirements | U.S. GAO
- [GAO-24-106638](#) COVID-19: HHS Needs to Identify Duplicative Pandemic IT Systems and Implement Key Privacy Requirements | U.S. GAO
- [GAO-24-105717](#) Federal Software Licenses: Agencies Need to Take Action to Achieve Additional Savings | U.S. GAO
- [GAO-23-104719](#) Information Technology: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements | U.S. GAO
- [GAO-22-104393](#) Technology Business Management: OMB and GSA Need to Strengthen Efforts to Lead Federal Adoption | U.S. GAO
- [GAO-22-104070](#) Cloud Computing: DOD Needs to Improve Workforce Planning and Software Application Modernization | U.S. GAO
- [GAO-16-511](#) Information Technology: Agencies Need to Improve Their Application Inventories to Achieve Additional Savings | U.S. GAO
- [GAO-16-468](#) Information Technology: Federal Agencies Need to Address Aging Legacy Systems | U.S. GAO

- [GAO-14-413](#) Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide | U.S. GAO

Critical action 3: Improve the monitoring of, and transparency into, the performance of IT investments.

- [GAO-24-106566](#) Information Technology: IRS Needs to Complete Planning and Improve Reporting for Its Modernization Programs | U.S. GAO
- [GAO-23-105478](#) Unemployment Insurance: DOL Needs to Further Help States Overcome IT Modernization Challenges | U.S. GAO
- [GAO-16-602](#) Digital Service Programs: Assessing Results and Coordinating with Chief Information Officers Can Improve Delivery of Federal Projects | U.S. GAO

Critical action 4: Strengthen planning and budgeting for the acquisition of IT systems and services.

- [GAO-23-105719](#) IT Management: VA Needs to Improve CIO Oversight of Procurements | U.S. GAO
- [GAO-19-49](#) Information Technology: Departments Need to Improve Chief Information Officers' Review and Approval of IT Budgets | U.S. GAO

Challenge 2: Implementing Mature IT Acquisition and Development Practices

Critical action 5: Improve implementation of leading IT acquisition and development practices to effectively plan and manage IT project costs, schedules, risks, requirements, and testing.

- [GAO-25-106963](#) IT Modernization: SBA Urgently Needs to Address Risks on Newly Deployed System | U.S. GAO
- [GAO-24-107783](#) Department of Education: Preliminary Results Show Strong Leadership Needed to Address Serious Student Aid System Weaknesses | U.S. GAO
- [GAO-24-107407](#) FAFSA: Education Needs to Improve Communications and Support Around the Free Application for Federal Student Aid | U.S. GAO
- [GAO-24-107001](#) Air Traffic Control: FAA Actions Are Urgently Needed to Modernize Aging Systems | U.S. GAO
- [GAO-24-106912](#) IT Systems Annual Assessment: DOD Needs to Strengthen Software Metrics and Address Continued Cybersecurity and Reporting Gaps | U.S. GAO
- [GAO-24-106319](#) Thrift Savings Plan: Investment Board Needs to Greatly Improve Acquisition Management and Contractor Oversight | U.S. GAO
- [GAO-24-105254](#) Air Traffic Control Modernization: Program Management Improvements Could Help FAA Address NextGen Delays and Challenges | U.S. GAO
- [GAO-23-105959](#) Biometric Identity System: DHS Needs to Address Significant Shortcomings in Program Management and Privacy | U.S. GAO

- [GAO-21-512](#) IT Modernization: USDA Needs to Improve Oversight of Farm Production and Conservation Mission Area | U.S. GAO
- [GAO-20-213](#) Agile Software Development: DHS Has Made Significant Progress in Implementing Leading Practices, but Needs to Take Additional Actions | U.S. GAO

Critical action 6: Strengthen the planning and management of cloud services, supply chains, and telecommunications services.

- [GAO-24-106137](#) Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements | U.S. GAO
- [GAO-23-105612](#) Information and Communications Technology: DOD Needs to Fully Implement Foundational Practices to Manage Supply Chain Risks | U.S. GAO
- [GAO-21-171](#) Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks | U.S. GAO
- [GAO-20-155](#) Telecommunications: Agencies Should Fully Implement Established Transition Planning Practices to Help Reduce Risk of Costly Delays | U.S. GAO
- [GAO-17-464](#) Telecommunications: Agencies Need to Apply Transition Planning Practices to Reduce Potential Delays and Added Costs | U.S. GAO

Challenge 3: Building Federal IT Capacity and Capabilities

Critical action 7: Address workforce management challenges for the technically-capable workforce.

- [GAO-23-105594](#) Data Science: NIH Needs to Implement Key Workforce Planning Activities | U.S. GAO
- [GAO-20-129](#) Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities | U.S. GAO

Critical action 8: Improve federal customer experience for digital services.

- [GAO-25-106933](#) Direct File: IRS Successfully Piloted Online Tax Filing | U.S. GAO
- [GAO-24-107236](#) IRS Direct File: Actions Needed during Pilot to Improve Information on Costs and Benefits | U.S. GAO
- [GAO-24-106764](#) Digital Experience: Agency Compliance with Statutory Requirements | U.S. GAO

Critical action 9: Ensure effective management of emerging technologies.

- [GAO-25-107703](#) Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy | U.S. GAO
- [GAO-24-107332](#) Artificial Intelligence: Agencies Are Implementing Management and Personnel Requirements | U.S. GAO

- [GAO-24-105980](#) Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirement | U.S. GAO
- [GAO-23-106415](#) Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight | U.S. GAO
- [GAO-22-104422](#) Quantum Computing and Communications: Status and Prospects | U.S. GAO
- [GAO-20-527SP](#) Science & Tech Spotlight: Quantum Technologies | U.S. GAO
- [GAO-18-656](#) Science and Technology: Considerations for Maintaining U.S. Competitiveness in Quantum Computing, Synthetic Biology, and Other Potentially Transformational Research Areas | U.S. GAO

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 the *Improving IT Acquisitions and Management* high-risk area, contact Carol C Harris, Director, Information Technology and Cybersecurity, (202) 512-4456.

Sarah Kaczmarek, Managing Director, Public Affairs, (202) 512-4800
A. Nicole Clowers, Managing Director, Congressional Relations, (202) 512-4400

Contributors: Emily Kuhn (Assistant Director), Amanda Gill (Analyst-in-Charge), Amanda Andrade, Chris Businsky, Rebecca Eyler, Lee Hinga, and Lisa Maine.

Header 1 – page 11: Source: GAO; ximich_natali/stock.adobe.com (center image); 32 pixels/stock.adobe.com (all icons). | GAO-25-107852; Header 2 – page 37: Source: GAO; BestCam/peopleimages.com/stock.adobe.com (center image); 32 pixels/stock.adobe.com (all icons). | GAO-25-107852; Header 3 – page 59: Source: GAO; suththirat/stock.adobe.com (center image); 32 pixels/stock.adobe.com (all icons). | GAO-25-107852.

Appendix II: Accessible Data

Accessible Data for Nine Critical Actions Needed to Address Three Major IT Acquisition and Management Challenges

Strengthening oversight and management of IT portfolios	Implementing mature IT acquisition and development practices	Building federal IT capacity and capabilities
Improve the effectiveness of key IT leadership positions, including the Federal Chief Information Officer (CIO), agency CIOs, and agency chief artificial intelligence officers.	Improve implementation of leading IT acquisition and development practices to effectively plan and manage IT project costs, schedules, risks, requirements, and testing.	Address workforce management challenges for the technically-capable workforce.
Enhance agency efforts to strategically plan for and manage portfolios of IT systems, applications, and software licenses, and to manage existing IT system operations.	Strengthen the planning and management of cloud services, supply chains, and telecommunications services.	Improve federal customer experience for digital services.
Improve the monitoring of, and transparency into, the performance of IT investments.		Ensure effective management of emerging technologies.
Strengthen planning and budgeting for the acquisition of IT systems and services.		

Accessible Data for Figure 2

See previous accessible data for Nine Critical Actions Needed to Address Three Major IT Acquisition and Management Challenges.

Accessible Data for Figure 3

	Fully addressed	Substantially addressed	Partially addressed	Minimally addressed	Not addressed
Information Technology (IT) leadership and accountability	11	7	6	0	0
IT budgeting	3	9	11	1	0
Information security	2	12	10	0	0
IT investment management	0	3	14	7	0
IT strategic planning	0	1	10	5	8
IT workforce	0	1	5	6	12

Fully addressed = agency provided evidence that described the CIO's role for carrying out all related responsibilities

Substantially addressed = agency provided evidence that described the CIO's role for at least two-thirds, but not all, related responsibilities

Appendix II: Accessible Data

Partially addressed = agency provided evidence that described the CIO's role for at least one-third, but less than two-thirds, of related responsibilities

Minimally addressed = agency provided evidence that described the CIO's role for less than one-third of related responsibilities

Not addressed = agency did not provide evidence that described the CIO's role for carrying out any related responsibilities

Accessible Data for Figure 4

Federal Area	sole	shared	No	Not applicable
Enterprise architecture	67	4	0	0
IT leadership and accountability	59	12	0	0
IT systems integration	59	12	0	0
IT systems development	58	13	0	0
IT systems acquisition	54	17	0	0
IT strategic planning	50	21	0	0
IT workforce	50	21	0	0
IT budgeting	49	22	0	0
Information security	46	22	3	0
IT capital planning and investment management	39	32	0	0
E-commerce/ E-business	13	46	7	5
Information collection	12	49	8	2
Privacy	7	55	9	0
Records management	4	57	10	0
Information dissemination and disclosure	4	55	12	0
Statistical policy	4	28	30	9

Accessible Data for Figure 5

Requirement	Assessment
IT portfolio reviews	
Implement a process to assist agencies in reviewing their IT portfolios.	Partially Followed
Develop standardized cost savings/avoidance and performance metrics for agencies to implement the process.	Partially Followed
Carry out the Federal Chief Information Officer's (CIO) role in being involved in an annual review of each agencies' IT portfolio in conjunction with the agency's CIO and Chief Operating Officer or Deputy Secretary (or equivalent).	Not Followed
Submit a quarterly report on the cost savings/reductions in duplicative IT investment identified through this review process to key committees in Congress.	Partially Followed

Appendix II: Accessible Data

Requirement	Assessment
Submit to Congress a report on the net program performance benefits achieved as a result of major capital investments made by agencies for information systems and how the benefits relate to the accomplishment of the goals of the agencies.	Partially Followed
High-risk IT investment reviews	
Carry out consultation responsibilities of the Federal CIO to agency CIOs and program managers of major IT investments that receive high-risk ratings for four consecutive quarters.	Not Followed
Communicate the results of high-risk IT investment reviews to key committees in Congress.	Not Followed
Deny any request of additional development, modernization, or enhancement funding for a major investment that has been rated high-risk for a year after the high-risk IT investment review. Additional funding should be denied until the agency CIO determines that the root causes of the risk have been addressed, and there is capability to deliver the remaining increments within the planned cost and schedule.	Not Followed

Partially followed = the agency demonstrated that it was following some, but not all, of the requirement.
 Not followed = the agency did not demonstrate that it was following the requirement.

Accessible Data for Figure 6

Number of practices	Number of agencies
0	3
1	2
2	6
3	9
4	4

Accessible Data for Figure 7

Application Rationalization Process (1-6).

1. Identify needs and set governance
 - a. Determine scope
 - b. Establish governance
 - c. Identify requirements
 - d. Develop questionnaire and templates
2. Inventory applications
 - a. Send questionnaire
 - b. Validate responses
 - c. Create new application process
 - d. Publish service catalog
3. Assess business value and technical fit
 - a. Review business value and technical fit
 - b. Determine dependencies
 - c. Identify duplication

4. Assess total cost of ownership
 - a. Confirm current state total cost of ownership
 - b. Identify cost outliers and compare total cost of ownership
5. Score applications
 - a. Develop scoring methodology and score applications
 - b. Review application scores
6. Determine application placement
 - a. Group applications based on score
 - b. Assess future state
 - c. Analyze hosting alternatives
 - d. Develop migration strategy

Accessible Data for Figure 8

Administration for Strategic Preparedness and Response = 9.

Centers for Disease Control and Prevention = 52.

Food and Drug Administration = 31.

Health Resources and Services Administration = 2.

Indian Health Service = 3.

National Institutes of Health = 2.

Accessible Data for Figure 9

Microsoft = 31.3 .

Adobe = 10.43 .

Salesforce = 8.7 .

Oracle = 6.96 .

ServiceNow = 5.22 .

IBM = 4.35 .

VMware = 3.48 .

Cisco = 3.48 .

McAfee = 2.61 .

ESRI = 1.74 .

Google = 1.74 .

Broadcom Inc. = 0.87 .

Computer Assisted Legal Research - 5 = 0.87 .

Computer Associates = International, Inc. = 0.87 .

ESCgov, Inc. = 0.87 .

Entrust, Corporation = 0.87 .
 FCN, Inc. Technology Solutions = 0.87 .
 Four, Inc. = 0.87 .
 Intelligent Editing Ltd = 0.87 .
 LinkedIn Corporation = 0.87 .
 MicroStrategy Incorporated = 0.87 .
 NCS Technologies Inc. = 0.87 .
 Palantir Technologies, Inc. = 0.87 .
 PKWARE, Inc. = 0.87 .
 PTC, Inc. = 0.87 .
 Quest Software, Inc. = 0.87 .
 Security Operations Center 0.87 .
 Skillsoft Corporation 0.87 .
 Splunk, Inc. 0.87 .
 SAS Institute, Inc. 0.87 .
 Symantec Corporation 0.87 .
 Unison Software, Inc. 0.87 .
 Zoom Video Communications, Inc. 0.87 .
 Zscaler, Inc. 0.87.

Accessible Data for Figure 10

Layer 4: Business units and capabilities	Categories and subcategories in this layer are not defined by the Technology Business Management Council because they are intended to be industry-specific and, therefore, defined by organizations to reflect their respective business units and capabilities	
Layer 3: Products and services	26 categories (e.g., finance services, manufacturing and delivery, and vendor and procurement services)	119 subcategories (e.g., application hosting, business continuity and disaster recovery, contract review, and payroll and time reporting)
Layer 2: IT towers	11 categories (e.g., application, data center, network, security and compliance, and storage)	41 subcategories (e.g., business software, client management, high performance computing, and mobile devices)
Layer 1: Cost pools	9 categories (e.g., facilities and power, hardware, internal labor, software, and telecom)	30 subcategories (e.g., cloud service providers, licensing, maintenance and support, and managed service providers)

Accessible Data for Figure 12

Modernization	Yes	No	NA
Includes milestones	21	0	0
Describes work to be performed	21	0	0
Includes disposition of legacy systems	3	6	12

Accessible Data for Figure 13

Modernization	very	moderately	neither or	mod dissatisfied	no response
18F	16	7	0	3	5
U.S. Digital Service	6	3	0	0	4

Accessible Data for Figure 16

Selected Office of Management and Budget (OMB) requirement	DOE	HHS	DOJ	Treasury
1. Establish the level of detail with which IT resources are to be described in order to inform the Chief Information Officer (CIO) during the planning and budgeting processes.	Satisfied all	Satisfied all	Satisfied all	Satisfied all
2. Establish agency-wide policy for the level of detail with which planned expenditures for all transactions that include IT resources are to be reported to the CIO.	Satisfied most	Satisfied most	Satisfied most	Satisfied most
3. Include the CIO in the planning and budgeting stages for programs that are supported with IT resources.	Satisfied most	Satisfied most	Satisfied all	Satisfied most
4. Include the CIO as a member of governance boards that inform decisions regarding all IT resources, including component-level governance boards.	Satisfied most	Satisfied most	Satisfied most	Satisfied most
5. Document the processes by which program leadership works with the CIO to plan an overall portfolio of IT resources.	Satisfied most	Satisfied most	Satisfied all	Satisfied all
6. Ensure the CIO has reviewed and approved the major IT investments portion of the budget request.	Satisfied most	Satisfied most	Satisfied all	Satisfied most
7. Ensure the CIO has reviewed IT resources that are to support major program objectives and significant increases and decreases in IT resources.	Satisfied none	Satisfied none	Satisfied all	Satisfied all
8. Ensure the CIO has reviewed whether the IT portfolio includes appropriate estimates of all IT resources included in the budget request.	Satisfied none	Satisfied none	Satisfied none	Satisfied none

Accessible Data for Figure 17

	Greater than or equal to \$15M	Greater than \$5M and less than or equal to \$15M	Greater than \$1M and less than or equal to \$5M	Sum of less than or equal to \$1m?
Approved TAC	2	5	1	4
No approval submitted TAC	11	1	1	1

Accessible Data for Figure 18

IT Management Area	Overall Assessment
Risk management	Minimally met
Requirements management	Partially met
Schedule	Not met
Cost	Minimally met

Accessible Data for Figure 19

Problems starting the application	Problems completing or submitting the application	Problems after submitting the application
Parents without a Social Security number are unable to start or contribute to the application. Fixed on March 8th (69 days after launch).	Students' or parents' prior signatures disappear upon returning to a saved application. Fixed on October 27th (230 days after launch).	Graduate students erroneously informed that they are eligible for Pell Grants. Not resolved as of December 2024. Graduate students were not eligible and needed to disregard the message.
Students unable to invite parents with foreign addresses and no Social Security number to contribute information to the application. Not resolved as of December 2024. Students needed to follow multistep workaround.	Some parents cannot continue past the first section of application. Fixed on October 27th (230 days after launch).	Students receive erroneous message that their application will expire after 40–45 days. Fixed on May 13th (135 days after launch).
	Students born in 2000 are unable to proceed past a certain section of the application. Fixed on March 8th (69 days after launch).	

Accessible Data for Figure 22

System Number	Life Span of the System	Age of System at Investment Completion Date
1	1974-2031	57
2	1978-2031	53
3	1988-2031	43
4	1991	No ongoing investment
5	1994-2035	41
6	1994-2031	37
7	1994-2030	36
8	1994	No ongoing investment
9	1994	No ongoing investment
10	1993-2031	35

Accessible Data for Figure 23

Leading practices in program management	GAO assessment
Establish a process and database for collecting and sharing lessons learned.	Fully met
Have an independent oversight body that conducts periodic reviews of the progress of the program.	Fully met
Develop a program management plan and a roadmap that are updated regularly.	Substantially met
Establish a reliable, integrated master schedule that is updated on a regular basis.	Substantially met
Establish a reliable, integrated, comprehensive life-cycle cost estimate that is updated on a regular basis.	Partially met
Measure program performance against baselines established in an integrated master schedule and against the program's life-cycle cost.	Partially met
Conduct program risk management throughout the life of the program and include risk mitigation plans prioritizing risks and analyzing alternatives.	Partially met
Establish program monitoring and controls, including conducting root cause analyses and developing corrective action plans.	Partially met
Conduct performance reporting and analysis in a way that provides stakeholders a clear picture of program performance.	Partially met

Fully met = actions have been taken that completely meet the selected practice.

Substantially met = most but not all actions to meet the selected practice have been taken.

Partially met = some, but not all, actions necessary to address the practice have been taken

Accessible Data for Figure 24

Some participants reported being unable to:

- Access their TSP retirement accounts
- Complete basic transactions
- Obtain the minimum distributions required by the Internal Revenue Service
- Receive beneficiary benefits and court order awards, and
- Get adequate assistance through TSP contact center — the ThriftLine.

Accessible Data for Figure 26

Gates 1 and 2 Initiation and investment:

Required final documents:

Project management plan. Not completed.

Mission needs statement (including cost estimate). Not completed.

Project schedule (draft). Not completed.

Required reviews and approvals

IAB review and approval. Completed.

E-Board review and approval. Not completed

Gates 3, 4, and 5 Requirements, design, development and test

Required final documents:

Earned value management report. Not completed

Business case. Not completed

Required reviews and approvals:

IAB review and approval. Not completed.

E-Board review and approval. Not completed.

Accessible Data for Figure 28

Requirement	Fully	Partially	Not
Ensure the agency's chief information officer oversees modernization.	24	0	0
Iteratively improve agency policies and guidance.	23	0	1
Have cloud service level agreement in place.	6	10	8
Standardize cloud contract service level agreements	9	2	13
Ensure continuous visibility in high value asset contracts.a	11	2	5

Accessible Data for Figure 29

	Fully implemented	Partially implemented	Not implemented
Establish executive oversight of ICT SCRM activities	3	2	18
Develop an agency-wide ICT SCRM strategy	1	4	18
Establish an approach to identify and document agency ICT supply chain(s)	3	1	19
Establish a process to conduct agency-wide assessments of ICT supply chain risks	0	0	23
Establish a process to conduct reviews of potential suppliers prior to selecting products and services	6	0	17
Develop organizational ICT SCRM requirements for suppliers	0	2	21
Develop organizational procedures to detect counterfeit and compromised ICT products prior to deployment	3	0	20

Accessible Data for Figure 30

	Fully	Partially	Not
Department of Agriculture	2	12	2
Department of Commerce	2	14	0
Department of Health and Human Services	4	12	0
Department of Labor	2	8	6
Department of State	3	13	0
Department of Transportation	0	9	7
Department of Veterans Affairs	4	12	0
National Aeronautics and Space Administration	8	8	0
Securities & Exchange Commission	2	7	7
Social Security Administration	3	12	1

Accessible Data for Figure 30

	Fully	Partially	Not
Department of Agriculture	2	12	2
Department of Commerce	2	14	0
Department of Health and Human Services	4	12	0
Department of Labor	2	8	6
Department of State	3	13	0
Department of Transportation	0	9	7
Department of Veterans Affairs	4	12	0
National Aeronautics and Space Administration	8	8	0
Securities & Exchange Commission	2	7	7
Social Security Administration	3	12	1

Accessible Data for Figure 31

	Fully	Substantially	Partially	Minimally	Not
Establish and maintain a workforce planning process	1	1	2	12	8
Develop competency and staffing requirements	12	4	8	0	0
Assess competency and staffing needs regularly	3	0	20	0	1
Assess gaps in competencies and staffing	2	9	12	1	0
Develop strategies and plans to address gaps in competencies and staffing	0	4	1	6	14
Implement activities that address gaps	0	2	7	15	0
Monitor the agency's progress in addressing gaps	0	0	3	5	16
Report to agency leadership on progress in addressing gaps	0	0	3	3	18

Accessible Data for Figure 32

Key workforce planning practices	Supporting activities	Rating
Set the strategic direction for workforce planning	Establish and maintain a workforce planning process	Partially implemented
	Develop competency and staffing requirements	Partially implemented
Analyze the workforce to identify skill gaps	Reassess competency and staffing needs regularly	Not implemented
	Determine gaps in competencies and staffing regularly	Not implemented
Develop and implement strategies to address skill gaps	Develop strategies and plans to address gaps in competencies and staffing	Partially implemented
	Implement activities that address gaps	Partially implemented
Monitor and report progress in addressing skill gaps	Monitor the agency's progress in addressing competency and staffing gaps	Not implemented
	Report to agency leadership on progress in addressing competency and staffing gaps	Not implemented

Accessible Data for Figure 33

Number of Modernization Agencies	2022	2023
0	1	1
1	0	0
2	0	0
3	1	1
4	1	2
5	2	2
6	2	1
7	1	3
8	6	8

Accessible Data for Figure 35

Telecommunications	Financial services	Other	Transportation	Agriculture	Public services and engagement	Healthcare	National security/ defense/ law enforcement	Internal management	Science
6	8	43	50	51	70	81	81	225	626

Accessible Data for Figure 36

Characteristics of a desirable national strategy	Assessment
Purpose, scope, and methodology Describes why the strategy was produced, the scope of its coverage, and the process by which it was developed.	Partially implemented
Problem definition and risk assessment Identifies the national problems and threats the strategy is directed toward and analyzes threats to, and vulnerabilities of, critical assets and operations.	Partially implemented
Objectives, activities, milestones, and performance measures Defines the objectives identifying what the strategy is trying to achieve, and activities to achieve those results, as well as the priorities, milestones, and performance measures to gauge results.	Partially implemented
Resources, investments, and risk management Summarizes what the strategy's implementation will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted by balancing risk reductions and costs.	Partially implemented
Organizational roles, responsibilities, and coordination Describes who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts.	Partially implemented
Implementation and integration Addresses how a national strategy is to be implemented and how the document relates to other strategies' goals, objectives, and activities—including international strategies.	Partially implemented
