U.S. GOVERNMENT ACCOUNTABILITY OFFICE

MISSION-CRITICAL INFORMATION TECHNOLOGY

Agencies Are Monitoring Selected Acquisitions for Cybersecurity and Privacy Risks

Report to the Ranking Member
Committee on Oversight and Government Reform
House of Representatives

March 2025
GAO-25-106908

GAO Highlights

Highlights of GAO-25-106908, a report to the Ranking Member, Committee on Oversight and Government Reform, House of Representatives

March 2025

MISSION-CRITICAL INFORMATION TECHNOLOGY

Agencies Are Monitoring Selected Acquisitions for Cybersecurity and Privacy Risks

Why GAO Did This Study

The acquisition of IT systems has presented challenges to federal agencies. Accordingly, GAO has identified IT acquisitions and management as a high-risk area since 2015.

GAO was asked to identify and report on selected federal IT acquisitions. GAO's objective was to identify essential mission-critical IT acquisitions across the federal government and their key attributes.

To select acquisitions for the review, GAO administered a survey to the 24 agencies covered by the Chief Financial Officers Act of 1990. GAO asked them to identify their top three most important mission-critical IT acquisitions that had ongoing system development activities. From a total of 72 acquisitions identified, GAO selected 16 mission-critical IT acquisitions across 11 agencies to profile in this report.

These 16 acquisitions are key to achieving the various agencies' missions across the federal government. For each of the 16 selected acquisitions, GAO obtained additional information on cost, schedule, risks, workforce, and related information; and interviewed relevant agency officials.

GAO provided a draft of this report to the 11 agencies with IT acquisitions profiled in this report and the Office of Management and Budget. In response, eight agencies provided technical comments, which we incorporated as appropriate.

View GAO-25-106908. For more information, contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov.

What GAO Found

Federal agencies are undertaking IT acquisitions that are essential to their missions. GAO identified 16 of these acquisitions as particularly critical to missions ranging from national security to public health to the economy (see table). GAO has previously reported on many of these acquisitions. As of February 2025, there were 75 open GAO IT- and cybersecurity-related recommendations pertaining to nine of the 16 acquisitions.

Essential Federal Mission-Critical Information Technology Acquisitions

Agency	Acquisition
Department of Defense	Joint Operational Medicine Information Systems
	Joint Warfighting Cloud Capability
Department of Education	Free Application for Federal Student Aid Processing System
	Title IV Origination and Disbursement Modernization
Department of Health and Human Services	Health Information Technology Electronic Health Records Modernization
Department of Homeland Security	Non-Intrusive Inspection-Integration Program
	Homeland Advanced Recognition Technology
Department of Justice	SENTRY Modernization - Centralized Inmate Case Logistics Operations and Planning System Development
Department of State	Consular Systems Modernization
Department of Transportation	Voice Communications Systems
	Automatic Dependent Surveillance-Broadcast
Department of the Treasury	Individual Master File Modernization
	Business Master File Modernization
Department of Veterans Affairs	Electronic Health Record Modernization
Environmental Protection Agency	Integrated Compliance Information System Modernization
Small Business Administration	MySBA Platform

Source: GAO analysis of agency data. | GAO-25-106908

In total, the 16 acquisitions are expected to cost at least $51.7 billion. For example, the Department of Health and Human Services plans to spend approximately $6.2 billion over 10 years on its electronic health records modernization effort.

Agency officials responsible for these IT acquisitions acknowledged facing a variety of risks and challenges. Specifically, 10 of the 16 acquisitions reported that not proceeding with the acquisition would jeopardize the ability of the agency to meet customer or mission needs, improve customer service, or achieve cost savings.

Further, seven acquisitions identified high risks associated with cybersecurity and information privacy. This means that an adverse cybersecurity or privacy incident could have severe or catastrophic effects on the agency, other agencies, or the nation. For example, both Department of Education acquisitions are intended to modernize systems that (1) are critical to providing federal student aid and (2) contain a large repository of personally identifiable information. Overall, cybersecurity and privacy risks are escalating as agencies' IT infrastructures continue to age and threats and vulnerabilities become more difficult to defend.

Contents

Tables

Figures

Abbreviations

ADS-B	Automatic Dependent Surveillance Broadcast
BMF	Business Master File
CADE	Customer Account Data Engine
CBP	U.S. Customs and Border Protection
CICLOPS	Centralized Inmate Case Logistics Operations and Planning System
CIO	chief information officer
CSM	Consular Systems Modernization
DHS	Department of Homeland Security
DOD	Department of Defense
EHR	Electronic Health Record
EHRM	Electronic Health Record Modernization
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FAFSA	Free Application for Federal Student Aid
FBOP	Federal Bureau of Prisons
FBI	Federal Bureau of Investigation
FITARA	Federal Information Technology Acquisition Reform Act
FPS	FAFSA Processing System
FY	fiscal year
HART	Homeland Advanced Recognition Technology
HHS	Department of Health and Human Services
ICIS	Integrated Compliance Information System
IDENT	Automated Biometric Identification System
IHS	Indian Health Service
IMF	Individual Master File
IRS	Internal Revenue Service
IT	information technology
ITPE	Individual Tax Processing Engine
JOMIS	Joint Operational Medicine Information Systems
JWCC	Joint Warfighting Cloud Capability
NextGen	Next Generation Air Transportation System
NII	Non-Intrusive Inspection
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	personally identifiable information
PMA	President's Management Agenda

SBA	Small Business Administration
TAM-I	Tax Account Management-Individual
TIVOD	Title IV Origination and Disbursement
VA	Department of Veterans Affairs
VCS	Voice Communications System
VistA	Veterans Health Information Systems and Technology Architecture

Cover sources: GAO (background illustration, binary code, map), lucky-photo/stock.adobe.com (capitol background image), Malambopeopleimages.com/stock.adobe.com (hands/lock), Rawpixelcom/stock.adobe.com (hands/ keyboard), Pakin/stock.adobe.com (thumb print), Miha Creative/stock.adobe.com (hands/tax), Gefo/stock. adobe.com (stethoscope), terovesalainen/stock.adobe.com (calculator), JJ Gouin/stock.adobe.com (tax form), VAKSMANV/stock.adobe.com (person on phone), Old Man Stocker/stock.adobe.com (air traffic control tower 1), SergeyBitos/stock.adobe.com (bar chart illustration), blackboard/stock.adobe.com (handcuffs/digital image), Gorodenkof/stock.adobe.com (person headset), M+Isolation+Photo/stock.adobe.com (hands/ipad), Ratchapon/ stock.adobe.com (water collection tank), wavebreak3/stock.adobe.com (hands computer screen), cat027/stock. adobe.com (tractor trailer), Agencies (all agency logos). | GAO-25-106908

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

March 11, 2025

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

Dear Mr. Connolly:

Federal IT systems provide essential services that are critical to the health, economy, and defense of the nation. Each year, the federal government spends more than $100 billion on IT investments. However, investments in IT often result in failed projects that incur cost overruns and schedule slippages, while contributing little to mission-related outcomes. These failed investments often suffer from a lack of disciplined and effective management, such as project planning, requirements definition, and program oversight and governance.

Recognizing the severity of issues related to the government-wide management of IT, in December 2014, Congress enacted the Federal Information Technology Acquisition Reform Act (FITARA) as part of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015.[1] FITARA is intended to improve agencies' acquisitions of IT and enable Congress to monitor agencies' progress and hold them accountable for reducing duplication and achieving cost savings.

We have previously reported that, while agencies have made progress in implementing the law, its further implementation is critical to improving the management of IT acquisitions.[2] This report responds to your request that we identify and report on selected federal IT acquisitions. Our specific objective of this review was to identify essential mission-critical IT

[1]Carl 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, 3438-50 (Dec. 19, 2014).

[2]See, for example, GAO, *Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements*, GAO-24-106137 (Washington, D.C.: Sept. 10, 2024); *Federal Software Licenses: Agencies Need to Take Action to Achieve Additional Savings*, GAO-24-105717 (Washington, D.C.: Jan. 29, 2024); *Data Center Optimization: Agencies Continue to Report Progress*, GAO-23-105946 (Washington, D.C.: Feb. 27, 2023); and *Information Technology: Effective Practices Have Improved Agencies' FITARA Implementation*, GAO-19-131 (Washington, D.C.: Apr. 29, 2019).

acquisitions across the federal government and their key attributes.[3] This review is the second iteration of our 2020 report: Information Technology: Key Attributes of Essential Federal Mission-Critical Acquisitions.[4]

To address our objective, we first developed a survey to distribute to each of the 24 federal agencies covered by the Chief Financial Officers Act of 1990.[5] In the survey, we asked agencies to identify their top three most important mission-critical acquisitions that had ongoing system development activities and had not yet been fully deployed.[6] We also asked agencies to answer specific questions about each identified acquisition. These questions related to, among other things, the acquisition's planned services and capabilities, the total anticipated lifecycle costs for the acquisition, potential risks, deployment timeline, types of acquisition end users, and anticipated impact on the agency and the nation (e.g., public health and safety).

[3]For the purpose of this report, the term "acquisition" is a broad term that also includes IT investments. According to Federal Acquisition Regulation (FAR) § 2.101, an "acquisition" means the acquiring by contract with appropriated funds of supplies or services (including construction) by and for the use of the federal government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, awarding of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract.

[4]GAO, *Information Technology: Key Attributes of Essential Federal Mission-Critical Acquisitions*, GAO-20-249SP (Washington, D.C.: Sept. 8, 2020).

[5]The 24 federal agencies covered by the Chief Financial Officers Act of 1990, 31 U.S.C. § 901(b), 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.

[6]For this report, a mission-critical acquisition is one that furthers the specific mission of the agency and, as such, would be unique to that agency and that the damage to, or disruption of, this acquisition would cause the most impact on the organization, mission, or networks and systems. In addition, a mission-critical system is any telecommunication or information system that is defined as a national security system or that processes any information the loss, misuse, disclosure, or unauthorized access to or modification of would have a debilitating impact on the mission of the agency. See National Institute of Standards and Technology, Volume 1: *Guide for Mapping Types of Information and Information Systems to Security Categories,* Special Publication 800-60, Revision 1 (Gaithersburg, MD: August 2008).

We then pretested the survey with two agencies: the Department of Homeland Security (DHS) and the Nuclear Regulatory Commission. In doing so, we interviewed and coordinated with officials in the offices of the Chief Information Officer (CIO) as well as acquisition oversight officials at these agencies to obtain their views as to whether our questions were clear and logical and to ensure that respondents could answer the questions without undue burden. We incorporated these agencies' feedback, as appropriate. We then administered the survey via email to each of the 24 agencies and received responses from 23.[7] The 23 agencies identified a total of 64 IT acquisitions.

To help ensure that we identified the most critical IT acquisitions for each agency, we also reviewed Federal IT Dashboard[8] data, assessed prior work that we and agencies' Inspectors General have issued, and consulted with our subject matter experts. We also asked each agency's Inspector General to provide us a list of what they believed were their agency's three to five most important mission-critical IT acquisitions. Fifteen of the 24 agencies' Inspectors General provided responses for a total of 54 IT acquisitions. These actions resulted in our selection of three additional acquisitions each from the Departments of Defense (DOD) and the Department of Transportation and one each from the Department of the Treasury and DHS. With these additional selections, the total number of identified acquisitions we considered for our study was 72 from all 24 agencies.

To assess the criticality of each acquisition, we developed a set of criteria focused on several factors, including the acquisition's impact on the agency and the nation, cost and budget data, and risk factors. We developed these criteria based on our reviews of federal continuity planning guidance; agencies' Inspectors General reports; Federal IT Dashboard data (e.g., the agency's annual IT spending, acquisition-specific spending, and CIO risk ratings); and the 2021 President's Management Agenda. We also reviewed our April 2023 High-Risk Series report; our other relevant prior reports, including our September 2020

[7]Although the Department of Defense did not provide a survey response designating its top three most important mission-critical acquisitions supported by IT within the audit time frame, we selected three as explained in the next paragraph.

[8]The Federal IT Dashboard is a public, government website previously operated by the Office of Management and Budget and currently by the General Services Administration at https://itdashboard.gov. It includes streamlined data to enable agencies and Congress to understand and manage federal IT portfolios and make better IT planning decisions and includes information on the performance of major IT investments.

report on key attributes of essential federal mission-critical IT acquisitions; critical infrastructure sectors identified in the Presidential Policy Directive 21, Critical Infrastructure Security and Resilience; and federal agencies' survey responses.[9] We then arranged the criteria into 14 categories.[10]

For each criterion within the 14 categories, we assigned a total point value ranging from zero to 16. We assigned point values based on the criticality of the criteria in terms of impact on the agency's mission. Our point values and criteria selection were informed by discussions with internal subject matter experts and methodologists.

We then analyzed information regarding the acquisitions from agency-provided survey responses, the Federal IT Dashboard, and prior reports that we and the agencies' Inspectors General have issued. For each acquisition, we used this information to assign point values based on either the presence of the criteria within an acquisition or the criticality of the acquisition's impact, such as to the agency's mission or the nation. The criteria used to evaluate each acquisition and their respective point values are in appendix I.

To select a subset of 16 of the 72 acquisitions on which to gather additional data for potential profiling in our report, we first calculated the total point values associated with the criteria for each acquisition. In order to provide a larger representation of agencies' acquisitions across the federal government, we limited our selection to the two IT acquisitions

[9]U.S. Department of Homeland Security Federal Emergency Management Agency, *Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements* (Jan. 17, 2017); Office of Management and Budget, *The Biden-Harris Management Agenda Vision* (Washington, D.C.: November 2021); GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023); *Information Technology: Key Attributes of Essential Federal Mission-Critical Acquisitions*, GAO-20-249SP (Washington, D.C.: Sept. 8, 2020); and The White House, Presidential Policy Directive 21*: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013). National Security Memorandum 22 replaced Presidential Policy Directive 21 in April 2024, after we developed our criteria and analyzed each acquisition. See The White House, *National Security Memorandum 22: National Security Memorandum on Critical Infrastructure Security and Resilience* (Washington, D.C.: Apr. 30, 2024).

[10]The categories under which we developed criteria used to assess acquisitions were: National Essential Functions, Agency Office of Inspector General, IT Dashboard/Chief Information Officer Risk Rating, President's Management Agenda, Government Accountability Office, Critical Infrastructure Sectors, Designation of Mission-Critical, Cost, Agency Oversight, Office of Management and Budget Oversight, Capabilities and Acquisition Type, Scope of End Users, Potential Risks to Agency and Nation, and Risk Factors.

with the highest point values per agency.[11] As a result of these activities and based on the highest point totals, we selected 16 IT acquisitions across 11 agencies that are key to achieving the various agencies' missions across the federal government.[12]

For each of the 16 selected acquisitions, we provided the relevant agencies with a second survey that inquired about the agency's basis for initiating the acquisition, dates of key milestones, cost and budget data, performance measures, and government and contract workforce. We also obtained and analyzed supporting documentation regarding acquisition implementation and strategy, cost and schedule, risks and issues, and related information. Additionally, we interviewed relevant agency officials, as necessary. We then summarized key attributes provided in agency responses and documentation into acquisition profiles that are included in this report.

Appendix I provides more details regarding our objective, scope, and methodology. Appendix II includes a copy of the questionnaire that we administered to the 24 federal agencies.

We conducted this performance audit from June 2023 to March 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Federal agencies and the nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on IT systems to carry out their operations. These systems and the data they use are vital to public confidence and national security, prosperity, and well-being. While investments in IT have the potential to improve lives and organizations, federally funded IT projects have often become risky, costly, and unproductive. We have previously reported that

[11]We also excluded acquisitions that did not have ongoing or planned system development activities at the time of our review or had sensitivity concerns.

[12]The 11 federal agencies from which we selected acquisitions are the Departments of Defense, Education, Health and Human Services, Homeland Security, Justice, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; and the Small Business Administration.

the federal government has spent billions of dollars on failed or troubled IT investments.[13]

In February 2015, we added improving the management of IT acquisitions and operations to our list of high-risk areas for the federal government, a designation it still retains.[14] In 2023, we noted that some progress had been made in addressing this high-risk area.[15] However, challenges persisted and agencies needed to take significant actions to build on this progress. Specifically, we continued to identify weaknesses in agencies' IT planning and management practices, including inadequate oversight of IT programs, cost estimates and schedules, testing, performance measurement, and risk management. Further, we noted that considerable work remained in the areas of enhancing IT workforce planning practices and developing plans for modernizing or replacing legacy systems.

In January 2025, we issued an update to the IT acquisitions and operations high-risk area.[16] In our report, we 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 identified nine critical actions that the federal government urgently needs to take, such as improving the planning and budgeting for the acquisitions of IT systems and services. Based on the results of our work, we changed the name of this high-risk area from *Improving the Management of IT Acquisitions and Operations* to *Improving IT Acquisitions and Management.*

Our report also noted that Office of Management and Budget (OMB) had not maintained its level of leadership commitment to ensure that agencies improve IT acquisitions and management. In addition, agencies had not maintained efforts to develop and implement action plans to address IT

[13]See, for example, GAO, *Information Technology: Agencies and OMB Need to Continue Implementing Recommendations on Acquisitions, Operations, and Cybersecurity,* GAO-20-311T (Washington, D.C.: Dec. 11, 2019); GAO-19-131; and *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C. Feb. 11, 2015).

[14]GAO-15-290 and GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023). More information on our high-risk list can be found at https://www.gao.gov/highrisk/overview.

[15]GAO-23-106203.

[16]GAO, *High-Risk Series: Critical Actions Needed to Urgently Address IT Acquisition and Management Challenges*, GAO-25-107852 (Washington, D.C.: Jan. 23, 2025).

management issues. In February 2025, we issued an updated assessment of this high-risk area against the five criteria for removal from the high-risk list.[17]

In addition, when acquiring and managing IT, the security of systems and data is also vital to safeguarding individual privacy and protecting the nation's security, prosperity, and well-being. However, risks to our nation's essential IT systems are increasing—in particular, malicious actors are becoming more willing and capable of carrying out cyberattacks. Recognizing the growing threat, we have designated information security as a government-wide high-risk area since 1997. We expanded this high-risk area in 2003 to include protecting the cybersecurity of critical infrastructure.[18] In 2015, we expanded it again to include protecting the privacy of personally identifiable information (PII).[19] In June 2024, we issued our latest report highlighting the most critical cybersecurity challenges facing the nation.[20]

Federal Efforts to Improve IT Acquisition Management and Oversight

FITARA was enacted in 2014 and established specific requirements for covered federal agencies. These requirements included enhancements to CIO authority and transparency, improved risk management, portfolio review, federal data center consolidation, and government-wide software purchasing. We have issued numerous reports on agencies' efforts to address the requirements of FITARA, highlighting their successes as well

[17]GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, GAO-25-107743 (Washington, D.C.: Feb. 25, 2025). In November 2000, we identified five criteria for removal from the high-risk list: leadership commitment, capacity, action plan, monitoring, and demonstrated progress. 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. See GAO, *Determining Performance and Accountability Challenges and High Risks*, GAO-01-159SP (Washington, D.C.: Nov. 1, 2000).

[18]The term "critical infrastructure" as defined in the Critical Infrastructures Protection Act of 2001 refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. § 5195c(e).

[19]In general, PII is any information that can be used to distinguish or trace an individual's identity, such as name, date or place of birth, and Social Security number; or that otherwise can be linked to an individual. Also, see GAO-15-290.

[20]GAO, *High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation*, GAO-24-107231 (Washington, D.C.: June 13, 2024).

as challenges in implementing selected provisions of the act.[21] These reports, along with scorecards issued by the Committee on Oversight and Government Reform, indicate variations in the extent to which covered agencies have implemented the FITARA provisions.[22]

Since the enactment of FITARA, OMB and covered federal agencies have paid greater attention to IT acquisitions and operations, resulting in improvements to the government-wide management of this significant annual investment. These efforts have been motivated, in part, by sustained congressional support for improving implementation of this law.

The executive branch has issued various plans to improve federal IT acquisition management and oversight, including the:

- **President's Management Agenda.** In November 2022, the prior administration issued its President's Management Agenda.[23] One priority the agenda identified was to continue to enhance federal IT and cybersecurity as key enablers of mission delivery for the federal government. The agenda stated that cybersecurity and IT modernization are critical tools that must be at the foundation of government management. It further stated that the executive branch would continue to bolster federal cybersecurity and ensure that secure systems help deliver government services. In addition, to better prepare for our future, the agenda stressed the importance of identifying and addressing critical skills gaps across the federal IT and cybersecurity workforce.
- **National Cybersecurity Strategy.** In March 2023, the prior administration issued the National Cybersecurity Strategy that outlined how the administration would manage the nation's cybersecurity through five pillars and 27 underlying strategic

[21]See, for example, GAO-24-106137, GAO-24-105717, GAO-23-105946, and GAO-19-131.

[22]In November 2015, the House of Representatives Committee on Oversight and Reform released the first biannual FITARA scorecard that assigned letter grades to federal agencies on their implementation of FITARA, among other things. For more information, see GAO, *Information Technology and Cybersecurity: Evolving the Scorecard Remains Important for Monitoring Agencies' Progress*, GAO-23-106414 (Washington, D.C.: Dec.15, 2022) and *Information Technology: Biannual Scorecards Have Evolved and Served as Effective Oversight Tools*, GAO-22-105659 (Washington, D.C.: Jan. 20, 2022).

[23]President's Management Council, President's Management Agenda (Washington, D.C.: November 2022).

objectives.[24] Among other things, the strategy discussed the need for the federal government to replace or update IT systems that were not defensible against sophisticated cyber threats. It noted that replacing legacy systems with more secure technology, including through accelerated migration to cloud computing based services, would elevate the cybersecurity posture across the federal government.

- **National Security Memorandum on Critical Infrastructure Security and Resilience.** In April 2024, the prior administration issued the National Security Memorandum on Critical Infrastructure Security and Resilience, which described the approach the federal government would take to protect U.S. critical infrastructure against threats and hazards.[25] Among other things, the memorandum reaffirmed the designation of the existing 16 critical infrastructure sectors, while calling for a periodic evaluation of changes to critical infrastructure sectors.[26] The memorandum emphasized the importance of integrating security and resilience into federal acquisition programs relating to critical infrastructure.

By law, OMB is to oversee federal agencies' acquisition and management of IT.[27] Within OMB, the Administrator of the Office of Electronic Government, or Federal CIO,[28] has primary responsibility for oversight of federal IT.[29] According to OMB, this oversight responsibility covers about 6,500 IT investments across the federal government, including about 600

[24]The White House, National Cybersecurity Strategy (Mar. 1, 2023).

[25]See The White House*, National Security Memorandum on Critical Infrastructure Security and Resilience, National Security Memorandum 22* (Washington, D.C.: Apr. 30, 2024).

[26]The 16 critical infrastructure sections are: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[27]*See, e.g.*, 40 U.S.C. §§ 11302, 11303; 44 U.S.C. §§ 3504, 3553.

[28]The office was established by the E-Government Act of 2002, Pub. L. No. 107-347, tit. I, § 101(a), 116 Stat. 2899, 2902 (Dec. 17, 2002), codified at 44 U.S.C. § 3602.

[29]OMB's Office of Information and Regulatory Affairs also has certain responsibilities for IT management.

major IT investments.[30] As a part of its oversight responsibilities, OMB develops policy and reviews federal agencies' IT strategic plans. In addition, OMB has established processes to analyze, track, and evaluate the risks and results of IT investments made by executive agencies, and issues guidance on processes for selecting and overseeing agency privacy and security protections for information and information systems.

OMB has also implemented a series of initiatives intended to improve the oversight of underperforming investments and more effectively manage IT. These initiatives include the following:

- **Federal IT Dashboard.** In June 2009, OMB deployed the Federal IT Dashboard, a public website with information on the performance of major federal investments to further improve the transparency into, and oversight of, federal agencies' IT investments. Subsequently, in March 2022, the operation of the IT Dashboard was transferred to the General Services Administration which released a modernized version. The dashboard is intended to provide information on the health of IT investments and the impact of federal IT portfolios, among other things. The dashboard displays information on the cost, schedule, and performance of nearly 600 major IT investments at 26 federal agencies.[31]

  Over the past 15 years, we have issued a series of reports about the IT Dashboard. These reports noted both the significant steps OMB has taken to enhance the oversight, transparency, and accountability of federal IT investments by creating the Federal IT Dashboard, aswell as issues with the accuracy and reliability of the data it

[30]According to OMB, a major IT investment is one that requires special management attention because of its importance to the mission or function to the government; has significant program or policy implications; has high executive visibility; has high development, operating, or maintenance costs; has an unusual funding mechanism; or is otherwise defined as major by the agency's capital planning and investment control process. Investments not considered major are non-major.

[31]The investments displayed on the IT Dashboard are identified and tracked by a three-digit agency code and a nine-digit unique investment number, called a unique investment identifier. Unique investment identifier refers to a persistent numeric code applied to an investment that allows the identification and tracking of an investment across multiple fiscal years of an agency's investment portfolio. The identifier is composed of a three-digit agency code linked with a nine-digit unique investment number generated by the agency.

contains.[32] We made a total of 22 recommendations to OMB and the associated agencies. Twenty of the recommendations were implemented, and two were closed but not implemented.

- **TechStat reviews.** In January 2010, OMB began conducting TechStat reviews in an effort to turn around, halt, or terminate IT projects that were failing or not producing results. OMB envisioned TechStats as face-to-face, evidence-based reviews of an at-risk IT investment. 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.[33] We have previously reported on OMB's and agencies' efforts to hold TechStat reviews. For example, in June 2013, we reported that while the selected agencies were generally conducting TechStats in accordance with OMB guidance, there was room for improvement.[34] We made four recommendations to the selected agencies to address the weaknesses we identified. The agencies implemented our recommendations.

  As previously mentioned, in December 2014, FITARA was enacted and included requirements for OMB and agencies on IT portfolio management. While FITARA does not specifically use the term "TechStat," it codified similar requirements for OMB and agencies on performing high-risk IT investment reviews on major investments that are rated as high risk for four consecutive quarters.

[32]GAO, *IT Dashboard: Agencies Need to Fully Consider Risks When Rating Their Major Investments*, GAO-16-494 (Washington, D.C.: June 2, 2016); *IT Dashboard: Agencies Are Managing Investment Risk, but Related Ratings Need to Be More Accurate and Available*, GAO-14-64 (Washington, D.C.: Dec. 12, 2013); *IT Dashboard: Opportunities Exist to Improve Transparency and Oversight of Investment Risk at Select Agencies*, GAO-13-98 (Washington, D.C.: Oct. 16, 2012); *IT Dashboard: Accuracy Has Improved, and Additional Efforts Are Under Way to Better Inform Decision Makin*g, GAO-12-210 (Washington, D.C.: Nov. 7, 2011); *Information Technology: OMB Has Made Improvements to Its Dashboard, but Further Work Is Needed by Agencies and OMB to Ensure Data Accuracy*, GAO-11-262 (Washington, D.C.: Mar. 15, 2011); and *Information Technology: OMB's Dashboard Has Increased Transparency and Oversight, but Improvements Needed*, GAO-10-701 (Washington, D.C.: July 16, 2010).

[33]The 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 *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*, M-17-26 (Washington, D.C.: June 15, 2017).

[34]GAO, *Information Technology: Additional Executive Review Sessions Needed to Address Troubled Projects*, GAO-13-524 (Washington, D.C.: June 13, 2013).

More recently, in November 2024, we reported that eight agencies did not follow the FITARA requirements for performing high-risk IT investment reviews.[35] Three of the eight agencies performed the reviews but did not address the specific requirements in law. The remaining five agencies did not perform the reviews. Further, we reported that OMB was not following any of its three statutory requirements for high-risk investment reviews, including communicating the results of these reviews to Congress. We noted that by not properly performing these required reviews, agencies are not following the law and are at risk of not being able to properly manage their IT cost, schedule, performance, and security. In our report, we made four recommendations to OMB and 12 recommendations to eight agencies to improve their high-risk investment review processes.

- **PortfolioStat sessions.** 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.[36] This required agency CIOs to conduct an annual agency-wide review of their IT portfolio to, among other things, assess the current maturity of their IT portfolio management process, reduce duplication, demonstrate how investments align with the agency's mission, and achieve savings by identifying opportunities to consolidate investments or move to shared services.

  We have previously reported on OMB's efforts to conduct PortfolioStat sessions. For example, in November 2013, we reported that agencies had taken actions to implement OMB's PortfolioStat guidance. However, there were shortcomings in their implementation of selected requirements, such as addressing all required elements of the final PortfolioStat action plan. We made 64 recommendations to OMB and 24 agencies to take steps to improve their PortfolioStat implementation. The agencies have implemented their recommendations.

  FITARA also included requirements for OMB and agencies on annual IT portfolio reviews. Similar to TechStats, while FITARA does not specifically use the term "PortfolioStat," it codified similar

[35]GAO, *IT Portfolio Management: OMB and Agencies Are Not Fully Addressing Select Statutory Requirements,* GAO-25-107041 (Washington, D.C.: Nov. 14, 2024). The eight agencies are the Departments of Homeland Security, Housing and Urban Development, the Interior, Labor, and State; Small Business Administration; Office of Personnel Management; and U.S. Agency for International Development.

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

requirements for OMB and agencies on performing annual IT portfolio reviews.

More recently, in November 2024, we reviewed the extent to which OMB and agencies were following statutory requirements for IT portfolio management oversight, including annual IT portfolio reviews (PortfolioStat).[37] We found that agencies had not fully addressed FITARA requirements for IT portfolio management. Specifically, none of the 24 agencies fully met the requirements for conducting annual IT portfolio reviews. In addition, we reported that OMB was partially following its FITARA requirements on IT portfolio review. We noted that, until portfolio management requirements are followed, the federal government is more likely to expend resources on IT investments that do not meet the needs of the government or the public. In our report, we made six recommendations to OMB and 24 recommendations to 24 agencies to, among other things, improve their IT portfolio management processes.

- **Guidance on incremental software development.** OMB has issued guidance on incremental software development—one approach to reducing the risks from broadly-scoped, multiyear projects.[38] An incremental development approach delivers software products in smaller modules with shorter time frames. Agile development, a type of incremental development, is built iteratively by refining or discarding portions as required based on user feedback and is intended to deliver software in increments throughout the project, unlike traditional software development processes, such as waterfall. Since 2000, OMB Circular A-130 has directed agencies to incorporate an incremental development approach into their policies and ensure that investments implement them. In addition, since 2012, OMB has required that functionality be delivered at least every 6 months.

We have issued various reports and testified on the status of agencies' efforts to implement incremental development.[39] We have also noted challenges related to improving federal IT acquisitions with use of incremental development. For example, management and organizational

[37]GAO-25-107041.

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

[39]GAO-23-106414, GAO-22-105659, and GAO, *Information Technology Reform: Agencies Need to Improve Certification of Incremental Development*, GAO-18-148 (Washington, D.C.: Nov. 7, 2017) and *Information Technology Reform: Agencies Need to Increase Their Use of Incremental Development Practices*, GAO-16-469 (Washington, D.C.: Aug. 16, 2016).

challenges and project complexity and uniqueness can impact agencies' ability to deliver incrementally.

Assessing IT Acquisition Risks

According to the National Institute of Standards and Technology, threats to information systems can include purposeful attacks, environmental disruptions, and human/machine errors, and can result in harm to the national and economic security interests of the United States. Therefore, it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing the risk associated with the operation and use of information systems that support the missions and business functions of their organizations. We have previously identified categories of risk to be considered by agencies when planning for and evaluating IT acquisitions to ensure the security of their sensitive information and systems. These categories are:

- **Organizational risk:** the impact of the acquisition on the agency. Agencies assess the risk that the proposed system will fail due to disruption.
- **Cybersecurity risk:** the level of security established for all information systems that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in these information systems. Identifying and assessing information security risks are essential steps in determining what controls are required to mitigate the risks.
- **Information privacy risk:** risks, including disclosure to unknown third parties for unspecified uses, tracking, identity theft, threats to physical safety, and surveillance. Agencies determine the risks and effects of collecting, maintaining, and disseminating information in an identifiable form in an electronic information system.
- **Technical risk:** the risk to complete the system from a technical point of view.
- **Cost/budget risk:** the sensitivity or quality of the cost estimates.
- **Schedule risk:** the probability that the acquisition will remain on schedule.
- **Risk of not implementing:** the risk to the agency of not proceeding with this acquisition. An evaluation of "very risky" in this area would mean that if the system is not built or is delayed for a year, the organization will likely not be able to meet customer needs, improve customer service, or achieve cost savings, among other impacts.

Key Attributes of Selected Mission-Critical IT Acquisitions

Federal agencies are undertaking IT acquisitions that are essential to meeting their mission and we have selected 16 of these key acquisitions to profile in our report. These acquisitions include IT systems that have a significant impact on the United States' national security interests, such as those that support improving the military's warfighting capabilities; foreign relations, such as those that collect and process information regarding visas; the economy, such as those that process taxes; and public health, such as those that are intended to provide reliable health care records, among other things. Table 1 provides a summary of the selected acquisitions and the agencies that are responsible for them.

Table 1: Federal Agency Mission-Critical IT Acquisitions

Department of Defense	Joint Operational Medicine Information Systems
	Joint Warfighting Cloud Capability
Department of Education	Free Application for Federal Student Aid Processing System
	Title IV Origination and Disbursement Modernization
Department of Health and Human Services	Indian Health Service Electronic Health Records Modernization
Department of Homeland Security	Homeland Advanced Recognition Technology
	Non-Intrusive Inspection Integration Program
Department of Justice	SENTRY Modernization - Centralized Inmate Case Logistics Operations and Planning System
Department of State	Consular Systems Modernization
Department of Transportation	Automatic Dependent Surveillance Broadcast
	Voice Communications Systems
Department of the Treasury	Business Master File Modernization
	Individual Master File Modernization
Department of Veterans Affairs	Electronic Health Record Modernization
Environmental Protection Agency	Integrated Compliance Information System Modernization
Small Business Administration	MySBA Platform

Source: GAO analysis of agency data. | GAO-25-106908

These 16 acquisitions are critical to the health, economy, and defense of the nation. For example, the Department of Veterans Affairs' (VA) Electronic Health Record Modernization acquisition is intended to improve healthcare outcomes for more than 9 million veterans by modernizing the collection and standardization of their health records. The Department of the Treasury expects its Individual Master File Modernization acquisition to modernize the technology environment that enables the IRS to process individual tax returns each year. Furthermore, DOD anticipates that the

Joint Warfighting Cloud Capability acquisition will modernize the military's cloud infrastructure to improve national security.

We have previously issued numerous reports on these acquisitions and the programs they support and have made a multitude of recommendations to agencies for improvements. For example, our recent work highlighted shortcomings in the DHS's implementation of program management best practices on its Homeland Advanced Recognition Technology acquisition and challenges related to the implementation of VA's Electronic Health Record Modernization.[40] As of February 2025, we had a total of 75 open IT- and cybersecurity-related recommendations pertaining to nine of the 16 acquisitions. Further, four of these acquisitions were also highlighted in a previous report on the most important mission-critical acquisitions issued in September 2020.[41]

We also have ongoing work looking specifically at IT- and cybersecurity-related topics at five of the 16 acquisitions.[42] For example, we have ongoing work looking at the extent to which VA has made progress toward improving its electronic health record system at initial deployment sites. We also have ongoing work evaluating Treasury's Internal Revenue Service's progress in implementing its modernization program for fiscal year 2024, which includes Individual Master File Modernization and Business Master File Modernization.

The 16 selected acquisitions can also be described across several key attributes, including their

- relating to GAO high-risk areas,

[40]See, for example, GAO, *Biometric Identity System: DHS Needs to Address Significant Shortcomings in Program Management and Privacy,* GAO-23-105959 (Washington, D.C.: Sept. 12, 2023) and *Electronic Health Records: VA Needs to Address Management Challenges with New System*, GAO-23-106731 (Washington, D.C.: May 18, 2023).

[41]GAO-20-249SP. The Department of State's Consular System Modernization, the Department of Transportation's Automatic Dependent Surveillance Broadcast, the Department of the Treasury's Individual Master File Modernization, and the Department of Veterans Affairs' Federal Electronic Health Record Modernization System were highlighted in our prior report.

[42]We have ongoing work related to the following five acquisitions: the Department of Education's Free Application for Federal Student Aid Processing System, the Department of Homeland Security's Homeland Advanced Recognition Technology, the Department of Veterans Affairs' Electronic Health Record Modernization, and the Department of the Treasury's Business Master File Modernization and Individual Master File Modernization.

- varying life cycle costs and deployment dates,
- using and storing PII,
- relying on multiple system development solutions (e.g., commercial-off-the-shelf and contractor-developed software),[43]
- using incremental development methodologies,
- having varying acquisition purposes,
- having critical risk factors,
- facing notable challenges, and
- having the potential for cost savings or cost avoidances.[44]

GAO high-risk areas. As previously stated, since 2015 we have identified improving IT acquisitions and management as a high-risk area. The continued struggle to effectively acquire IT systems means the missions they support are vulnerable to fraud, waste, abuse, and mismanagement, or are in need of transformation. Furthermore, the security of our federal cyber assets has been on our list of high-risk areas since 1997. Cybersecurity and privacy risks are escalating as agencies' IT infrastructures continue to age and threats and vulnerabilities become more difficult to defend. Mission-critical systems, especially those which use and or store large amounts of PII, require increased levels of cybersecurity activity to safeguard sensitive information.

[43]Commercial off-the-shelf software is sold in substantial quantities in the commercial marketplace. Contractor-developed software refers to software specifically designed for an agency by a third party under contract.

[44]Cost savings are a reduction in actual expenditures below the projected level of costs to achieve a specific objective. Cost avoidance is an action taken in the immediate time frame that will decrease costs in the future.

In addition to those high-risk areas, 10 of the 16 acquisitions and the programs they support relate to an additional programmatic area that we have designated as being high-risk.[45] These areas include, for example, DOD's business systems modernization, strengthening the DHS's IT and financial management functions, and the enforcement of tax laws. See table 2 for a list of acquisitions and related high-risk areas.

Table 2: Mission-Critical IT Acquisitions Related to Programmatic GAO High-Risk Areas

Acquisition (agency)	Related high-risk area
Joint Operational Medicine Information Systems (Department of Defense)	DOD Business Systems Modernization
Indian Health Service Electronic Health Records Modernization (Department of Health and Human Services)	Improving Federal Management of Programs that Serve Tribes and Their Members
Homeland Advanced Recognition Technology (Department of Homeland Security)	Strengthening Department of Homeland Security IT and Financial Management Functions
Non-Intrusive Inspection Integration Program (Department of Homeland Security)	Strengthening Department of Homeland Security IT and Financial Management Functions
SENTRY Modernization - Centralized Inmate Case Logistics Operations and Planning System (Department of Justice)	Strengthening Management of the Federal Prison System
Business Master File Modernization (Department of the Treasury)	Enforcement of Tax Laws
Individual Master File Modernization (Department of the Treasury)	Enforcement of Tax Laws
Electronic Health Record Modernization (Department of Veterans Affairs)	Managing Risks and Improving VA Healthcare
Integrated Compliance Information System Modernization (Environmental Protection Agency)	Transforming EPA's Process for Assessing and Controlling Toxic Chemicals
	U.S. Government's Environmental Liability
MySBA Platform (Small Business Administration)	Emergency Loans for Small Businesses

Source: GAO analysis of agency data and GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023). | GAO-25-106908

Anticipated life cycle costs and deployment dates. The amount agencies expect to spend on the selected acquisitions varies greatly depending on their scope and complexity, as well as the extent of transformation and modernization that agencies envision once the acquisitions are fully deployed. For example, the Department of Health and Human Services plans to spend approximately $6.2 billion over 10 years on its Indian Health Service Electronic Health Records Modernization effort, while the Department of Homeland Security intends

[45]GAO-23-106203.

to spend $2.2 billion over 23 years on its Homeland Advanced Recognition Technology acquisition.

The total anticipated life cycle costs across all 16 acquisitions are approximately $51.7 billion, but this figure is likely higher. Specifically, our total reflects VA's 2019 estimate for the Electronic Health Record Modernization program of about $16.1 billion over 10 years. However, in 2022, the Institute for Defense Analyses independently determined that the 28-year life cycle costs for the program were $49.8 billion. This includes $32.7 billion for a 13-year implementation period and $17.1 billion for 15 years of sustainment. As of February 2025, VA was not able to provide a time frame for when it would update the program life cycle cost estimate.

Regarding planned deployment dates, nine of the 16 acquisitions were able to provide projected dates for achieving full operational capability, while 11 acquisitions were able to provide projected dates for initial operational capability, and three were unable to provide either projected date.[46] Agencies provided various reasons for not having planned deployment dates, including that the dates were still being determined or that they were not planning to have an initial operational capability milestone. Further, although certain acquisitions planned to achieve full operational capability in 2024, additional mission-critical development work is underway or planned. Table 3 shows the total anticipated life cycle costs, actual or planned initial and full operational deployment dates, and whether we have ongoing acquisition-specific IT or cybersecurity-related reviews of the acquisition.

[46]Initial operational capability is achieved when a system is implemented with some minimal capabilities and additional capabilities are planned before the system is determined to have reached full operational capability. Once the capability has been fully developed, it may be declared to be in full operational capability.

Table 3: Mission-Critical IT Acquisitions' Planned Costs, Expected Deployment Dates, and Status of Acquisition-Specific GAO IT and Cybersecurity Reviews (as of January 2025)

Agency	Acquisition	Anticipated life cycle costs (in millions, rounded)	Actual or planned initial operational capability date[a]	Actual or planned full operational capability date[b]	Ongoing acquisition-specific GAO IT or cybersecurity review?
Department of Defense	Joint Operational Medicine Information Systems	$1,647	November 2025	Not yet determined	No
	Joint Warfighting Cloud Capability	8,974	December 2022	March 2025	No
Department of Education	Free Application for Federal Student Aid Processing System	203	December 2023	Not yet determined	Yes
	Title IV Origination and Disbursement Modernization[c]	Not yet determined	Not yet determined	Not yet determined	No
Department of Health and Human Services	Indian Health Service Electronic Health Records Modernization	6,204	June 2026	Not yet determined	No
Department of Homeland Security	Homeland Advanced Recognition Technology	2,245	September 2026	September 2027[d]	Yes
	Non-Intrusive Inspection Integration Program	5,701[e]	Not yet determined	Not yet determined	No
Department of Justice	SENTRY Modernization - Centralized Inmate Case Logistics Operations and Planning System	69	July 2025	December 2026	No
Department of State	Consular Systems Modernization	385	Not applicable[f]	Not applicable[f]	No
Department of Transportation	Automatic Dependent Surveillance Broadcast	3,555	November 2009	March 2014[g]	No
	Voice Communications Systems	2,962	January 2027	2035[h]	No
Department of the Treasury	Business Master File Modernization	561	Not yet determined	January 2029	Yes
	Individual Master File Modernization	2,930	Not yet determined	2028	Yes
Department of Veterans Affairs	Electronic Health Record Modernization	16,138[i]	October 2020	Not yet determined	Yes
Environmental Protection Agency	Integrated Compliance Information System Modernization	42	March 2026	March 2029	No
Small Business Administration	MySBA Platform	43	August 2024	January 2025[g]	No
	Total:	**$51.7 billion**			

Source: GAO analysis of agency data. | GAO-25-106908

[a]Initial operational capability is achieved when a system is implemented with some minimal capabilities and additional capabilities are planned before the system is determined to have reached full operational capability.

[b]Once the capability has been fully developed, it may be declared to be in full operational capability.

[c]Title IV Financial Aid Origination and Disbursement is in the pre-planning stage and had not yet determined anticipated life cycle costs and expected deployment dates.

[d]This date reflects full operational capability for increment 1 only.

[e]The Department of Homeland Security indicated that this figure is preliminary because the program had not yet been baselined.

[f]Agency officials stated that this date is not applicable because the acquisition is comprised of multiple projects.

[g]Additional mission-critical development work is underway or planned after full operational capability, according to agency officials.

[h]This date represents when the replacement of legacy radio control equipment under the Voice Communication Systems program is planned to be completed.

[i]This total reflects the Department of Veteran Affairs' 2019 estimate over a 10-year life cycle. However, in 2022, the Institute for Defense Analyses independently determined that the 28-year life cycle costs for the program were $49.8 billion. This includes $32.7 billion for a 13-year implementation period and $17.1 billion for 15 years of sustainment. As of February 2025, the department was not able to provide a time frame for when it would update the program life cycle cost estimate.

Use and storage of PII. Most of the acquisitions—13 of 16—are expected to use and store PII to meet the purpose of the acquisition. For example, the VA's electronic health record system will use and store PII to orchestrate and document the medical care for approximately 9 million veterans nationwide. Further, the Department of State's Consular Systems Modernization will use and store PII to streamline and digitize core business processes related to passport and visa applications at the agency for citizens and non-citizens alike.

As mentioned earlier, the security of our federal cyber assets has been on our list of high-risk areas since 1997. In 2015, we expanded this high-risk area to include protecting the privacy of PII that is collected, maintained, and shared by both federal and nonfederal entities. We have previously reported that advances in technology have dramatically enhanced the ability of both government and private sector entities to collect and process extensive amounts of PII. This increase in the amount of PII collected poses challenges to ensuring the privacy of such information.

System development solutions. Agencies reported using numerous system development solutions for the IT acquisitions profiled in our report. These solutions include using commercial off-the-shelf software, contractor-developed software, open-source software, and customized software development by agency personnel. All acquisitions reported the use of at least one system development solution. Multiple acquisitions reported the use of more than one of these development solutions. The different development solutions used and the number of acquisitions using each can be found in table 4.

Table 4: Development Solutions Reported by Agencies

Development solutions	Number of acquisitions out of 16 using the development solution[a]
Commercial off-the-shelf software[b]	11
Contractor-developed software[c]	11
Open-source software[d]	8
Customized software development by agency personnel	6

Source: GAO analysis of agency data. | GAO-25-106908

[a]Multiple acquisitions reported the use of more than one type of development solution.

[b]Commercial off-the-shelf software is sold in substantial quantities in the commercial marketplace.

[c]Contractor-developed software refers to software specifically designed for an agency by a third party under contract.

[d]Open-source software refers to software which has the source code freely available for possible modification and redistribution by the public.

Project management methodologies. Nearly all agencies reported using an incremental system development lifecycle methodology, such as Agile.[47] The use of incremental software development can help to reduce the risks from broadly-scoped, multiyear projects. Specifically, 11 of the 16 acquisitions are governed by an Agile or other type of incremental systems development lifecycle methodology. Four agencies reported using a combination of Agile and waterfall approaches.[48] For example, officials from the Environmental Protection Agency stated that a waterfall approach was used for certain aspects of the Integrated Compliance Information System acquisition, such as developing policy requirements. The remaining acquisition—the Department of Education's Title IV Origination and Disbursement Modernization—had not yet determined the development approach because it was in the pre-project phase.

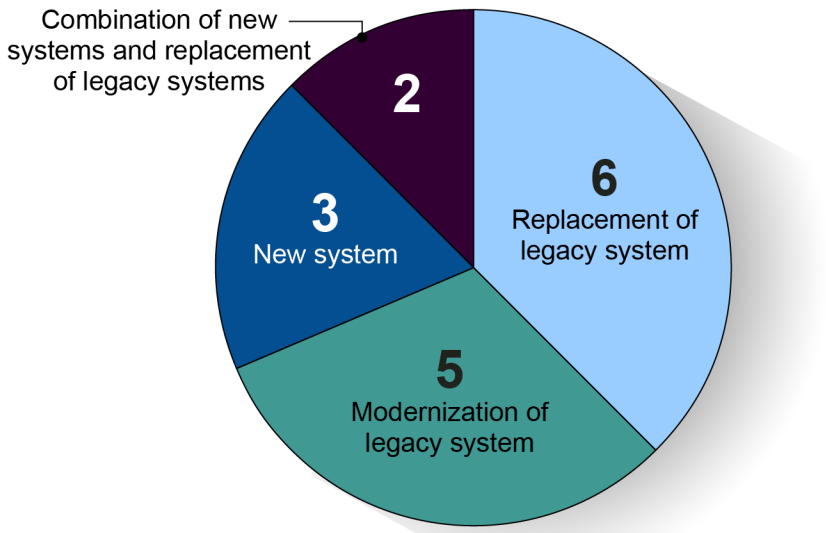
System acquisition purpose. The extent to which agencies are replacing older systems or continuing the development of an existing system varies across the agencies and type of acquisition. However, most of these investments are intended to either modernize or replace existing legacy systems. In particular, 11 of the 16 major IT acquisitions

[47]Agile, a type of incremental development, is built iteratively by refining or discarding portions as required based on user feedback and is intended to deliver software in increments throughout the project.

[48]A waterfall approach uses linear and sequential phases of development that may be implemented over a longer period of time before resulting in a single delivery of software capability.

profiled in this report are either modernizations or replacements of existing legacy systems, three are new systems with new capabilities, and two are a combination of new and replacement systems. Figure 1 provides the number of acquisitions reported as modernizations, replacements, or new systems with new capabilities by the agencies:

Figure 1: System Acquisition Purpose Reported by Agencies



Source: GAO analysis of agency data. | GAO-25-106908

Risk factors. Nearly all acquisitions—15 of 16—identified at least one high-risk factor that, if realized, would have a catastrophic impact to their agency's ability to carry out its mission. Moreover, all 16 acquisitions identified at least one moderate risk factor. These risk factors are related to the categories of risk we previously discussed. Agencies identified the risk of not implementing the acquisition as a high-risk factor for 10 of the 16 total acquisitions. This means that not proceeding with the acquisition would jeopardize the ability of the agency to meet customer needs, improve customer service, or achieve cost savings, among other impacts.

Cybersecurity, information privacy, and cost/budget were tied as the second most identified high-risk factor, with seven of the 16 total acquisitions identifying each of these. For acquisitions that identified cybersecurity and information privacy as high-risk, this means that an adverse cybersecurity or privacy incident could have severe or catastrophic effects on the agency, other agencies, or the nation. Regarding cost/budget, this means that the cost estimate is at higher risk of requiring changes due to the complexity of the acquisition. The

complete list of high-risk factors and the number of agencies reporting each factor can be found in table 5. The acquisition profiles in this report contain more specific examples of the risks for each acquisition.

Table 5: Acquisition Risks Reported by Agencies

Risk factor	Number of the 16 total acquisitions reporting this factor as a high-risk
Not implementing	10
Cybersecurity	7
Information privacy	7
Cost/budget	7
Technical	4
Schedule	4
Organizational	2

Source: GAO analysis of agency data. | GAO-25-106908

Challenges. While risks are related to adverse events that may occur, agencies also face challenges which are related to adverse events that the acquisition has already experienced. Thirteen of the 16 acquisitions reported that they faced at least one challenge in effectively implementing these acquisitions. For example, agencies reported challenges with schedule slippages, technical issues, inadequate funding, and workforce issues. The two most common challenges—identified by 11 of the 13 acquisitions—were technical issues and schedule slippages. Agency officials cited experiencing technical issues with updating existing infrastructure to support new systems and transitioning to a cloud environment, among other areas. Officials cited schedule slippages due to, for example, receiving annual appropriations later than anticipated, contractor performance issues, and hiring delays.

Further, the third most common challenge area identified across 10 of the 13 acquisitions was related to funding and budget, including obtaining adequate funding, the imposition of budget cuts during the COVID-19 pandemic, and others. Lastly, eight of the 13 acquisitions reported facing workforce issues including a lack of available government full time equivalents, inadequate skills among staff, or changes in leadership that impacted implementation of the acquisitions. The complete list of challenges and the number of agencies reporting each can be found in table 6. The acquisition profiles in this report contain more specific examples of challenges for each acquisition.

Table 6: Acquisition Challenges Reported by Agencies

Challenge	Number of the 16 total acquisitions reporting this challenge
Technical issues	11
Schedule slippages	11
Obtaining adequate funding/budget	10
Workforce issues	8
Organizational alignment and structure	6
Cost constraints	6
Providing oversight and governance	3
Implementation of chosen system development methodology	3

Source: GAO analysis of agency data. | GAO-25-106908

As previously mentioned, we have 75 IT and cybersecurity-related open recommendations pertaining to the 16 acquisitions. Many of these recommendations, if implemented, could help to address the challenges mentioned above. For example:

- We recommended that VA establish user satisfaction targets (i.e., goals) for its Electronic Health Record Modernization and ensure that the program demonstrates improvement toward meeting those targets prior to future system deployments.[49] Implementing this recommendation could help address challenges with schedule slippages.
- We recommended that DHS update the cost estimate for the Homeland Advanced Recognition Technology program to account for all costs and incorporate the best practices called for in the GAO *Cost Estimating and Assessment Guide*.[50] Implementing this recommendation could help address challenges with obtaining adequate funding/budget as well as cost constraints.[51]

[49]GAO, *Electronic Health Records: VA Needs to Address Management Challenges with New System*, GAO-23-106731 (Washington, D.C.: May 18, 2023).

[50]GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*, GAO-20-195G (Washington, D.C.: Mar. 12, 2020).

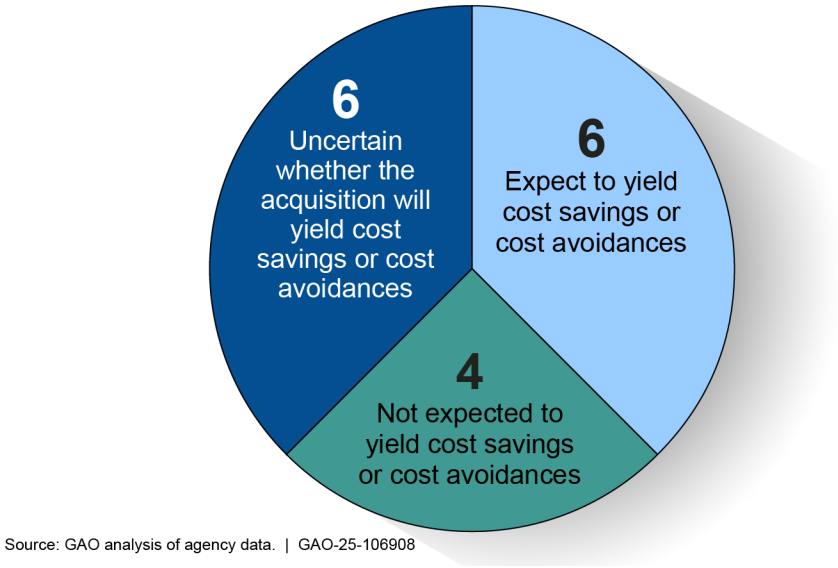
[51]GAO, *Biometric Identity System: DHS Needs to Address Significant Shortcomings in Program Management and Privacy*, GAO-23-105959 (Washington, D.C.: Sept. 12, 2023).

- We recommended that Education expeditiously (1) assess the role of the department's and Office of Federal Student Aid's CIOs in the continuing development of the Free Application for Federal Student Aid processing system (FPS), and (2) based on that assessment, develop and implement a plan for providing the department's CIO with a significant role in the governance and oversight of FPS while clarifying the responsibilities between the departmental and agency CIO. Implementing this recommendation could help address challenges with organizational alignment and structure.[52]

Cost savings and cost avoidances. Agencies also identified the potential for the IT acquisitions to yield cost savings or avoidances after full deployment. Six of the 16 profiled acquisitions are expected to yield cost savings or cost avoidances while four are not. The remaining six acquisitions were uncertain whether full deployment would result in cost savings or avoidances. Agencies cited various factors that are expected to yield cost savings or avoidances as a result of the acquisitions, such as the transition from costly legacy systems, adoption of new technology such as cloud-based infrastructure, and the streamlining of tasks at the agency. Figure 2 includes information regarding the cost savings and cost avoidances information reported by agencies.

[52]GAO, *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).

Figure 2: Cost Savings and Cost Avoidances Expected by Agencies' Acquisitions After Deployment



Source: GAO analysis of agency data. | GAO-25-106908

The six acquisitions expected to yield cost savings or cost avoidances after full deployment include the following:

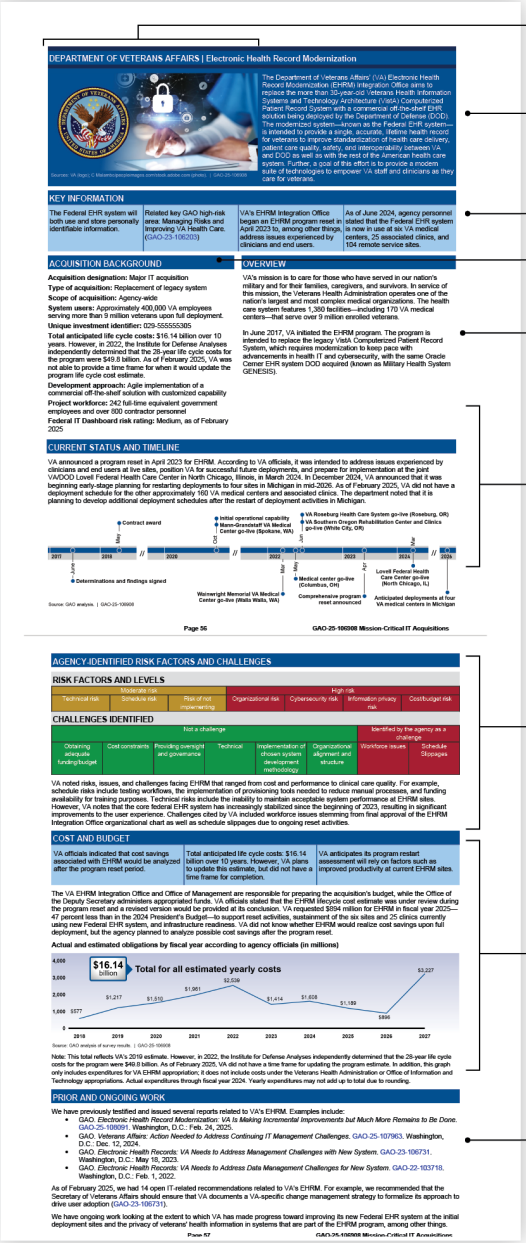
- Joint Operational Medicine Information Systems (Department of Defense)
- Joint Warfighting Cloud Capability (Department of Defense)
- Homeland Advanced Recognition Technology (Department of Homeland Security)
- Automatic Dependent Surveillance Broadcast (Department of Transportation)
- Integrated Compliance Information System Modernization (Environmental Protection Agency)
- MySBA Platform (Small Business Administration)

For example, Transportation officials reported approximately $29 million in cost avoidances from removing legacy airport surveillance radars as part of its Automatic Dependent Surveillance Broadcast acquisition. In addition, the officials anticipated cost avoidances of over $400 million by fiscal year 2035 if remaining candidate radars are removed. The remaining acquisitions previously mentioned are unable to provide

accurate cost savings or cost avoidances information until the acquisition reaches full deployment.

The following section contains profiles of the 16 mission-critical IT acquisitions that we selected and reviewed, grouped by federal departments and agencies, in alphabetical order. The profiles and the data presented in this report reflect key attributes of the selected federal IT acquisitions as of January 2025, unless otherwise noted. Each profile presents an overview of the acquisition, its current status, and its life cycle cost estimates, among other information. Figure 3 provides an illustration of the layout of each profile. The agency profiles follow the figure.

Figure 3: Illustration of Acquisition Profile



A Agency logo and acquisition-specific illustration

B Acquisition description

C Key information such as use and storage of personally identifiable information, GAO high-risk area, rebaselining information, etc.

D Type and scope of acquisition, system users, life cycle costs, among other attributes

E Description of how the acquisition supports the agency's mission

F Current status of acquisition and timeline of key events

G Risk factors and challenges identified by agency officials

H Overview of acquisition cost and budget

I Prior or ongoing GAO reporting, as applicable

Source: GAO. | GAO-25-106908

DEPARTMENT OF DEFENSE | Joint Operational Medicine Information Systems

Sources: DOD (logo); wavebreak3/stock.adobe.com (photo). | GAO-25-106908

The purpose of the Joint Operational Medicine Information Systems (JOMIS) is to provide software products that support the Department of Defense's (DOD) operational medicine needs. Initiated in 2015, JOMIS addresses capability gaps in knowledge management activities needed to support DOD operational healthcare functions. DOD officials did not report a date when JOMIS will reach full operational capability but noted that multiple components are expected to achieve initial deployment by November 2025.

KEY INFORMATION

JOMIS will both use and store personally identifiable information.	Related key GAO high-risk area: DOD Business System Modernization (GAO-23-106203)	JOMIS is part of the Program Executive Office, Defense Healthcare Management Systems, which operates under the DOD's Defense Healthcare Agency.	Agency officials anticipate that the Theater Medical Information Program-Joint, which JOMIS is replacing, is expected to be phased out between 2025 and 2030, with the exception of U.S. Navy ships.

ACQUISITION BACKGROUND

Acquisition designation: Major acquisition

Type of acquisition: Combination of new systems and replacement systems

Scope of acquisition: U.S. Army, Navy, Air Force, Marine Corps, and Combatant Commands

System users: Approximately 3,500 users across the operational medicine community

Unique investment identifier: 007-000100540

Total anticipated life cycle costs: $1.647 billion over 7 years

Development approach: Waterfall and Agile development using software from multiple sources, including contractor-developed, commercial off-the-shelf, open-source, and agency personnel-developed solutions

Project workforce: 46 government full-time equivalents and 357 contractor personnel

Federal IT Dashboard risk rating: Medium, as of November 2024

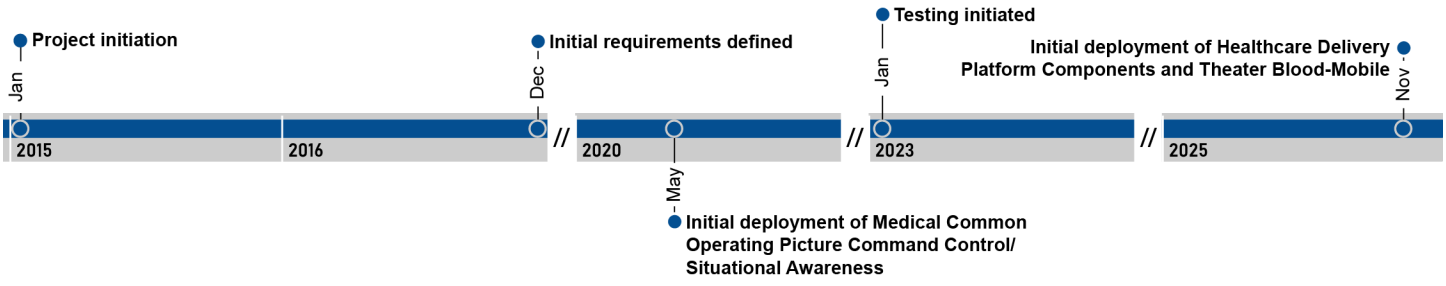
OVERVIEW

JOMIS is intended to modernize, deploy, and sustain DOD operational medicine information systems while also developing and fielding new theater capabilities that enable comprehensive health services to meet warfighter requirements. JOMIS is expected to replace the Theater Medical Information Program-Joint, which is the primary tactical medical system used to provide DOD operational medicine health care functions.

JOMIS is intended to provide several capabilities, referred to as managed applications, to the warfighter. Warfighters are expected to use the managed applications acquired through JOMIS to support the five operational medicine healthcare functions: Medical Command and Control, Medical Situational Awareness, Medical Logistics, Healthcare Delivery, and Patient Movement.

CURRENT STATUS AND TIMELINE

JOMIS uses a mix of waterfall and Agile development and is currently carrying out development, testing, implementation, and maintenance concurrently. Within the next year, JOMIS plans to continue the implementation of Medical Common Operating Picture, which is intended to provide real-time visibility of unit health, equipment, and supplies. Furthermore, JOMIS plans to carry out additional testing of additional components, such as: Theater Blood-Mobile, which is intended to provide overall blood management services to deployed personnel; and Operational Medicine Data Service, which is intended to provide critical data transport and management services.



Source: GAO analysis. | GAO-25-106908

Note: In accordance with the JOMIS Acquisition Strategy signed in 2021, JOMIS is a portfolio of products and does not have overarching milestone dates. Dates presented are the latest milestones of the products in the JOMIS portfolio.

AGENCY IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk		Moderate risk				High risk
Organizational risk	Cost/budget risk	Cybersecurity risk	Information privacy risk	Technical risk	Schedule risk	Risk of not implementing

CHALLENGES IDENTIFIED

Not a challenge					Identified by the agency as a challenge		
Workforce issues	Schedule slippages	Providing oversight and governance	Implementation of chosen system development methodology	Organizational alignment and structure	Obtaining adequate funding/budget	Cost constraints	Technical

DOD officials identified the risk of not implementing as the highest risk factor, stating that by not implementing JOMIS, new capabilities such as enroute care and point of injury care would not be delivered. Furthermore, not implementing JOMIS would result in the continued use of aging legacy systems and infrastructure that will impact patient care of active military personnel when those systems reach end of life.

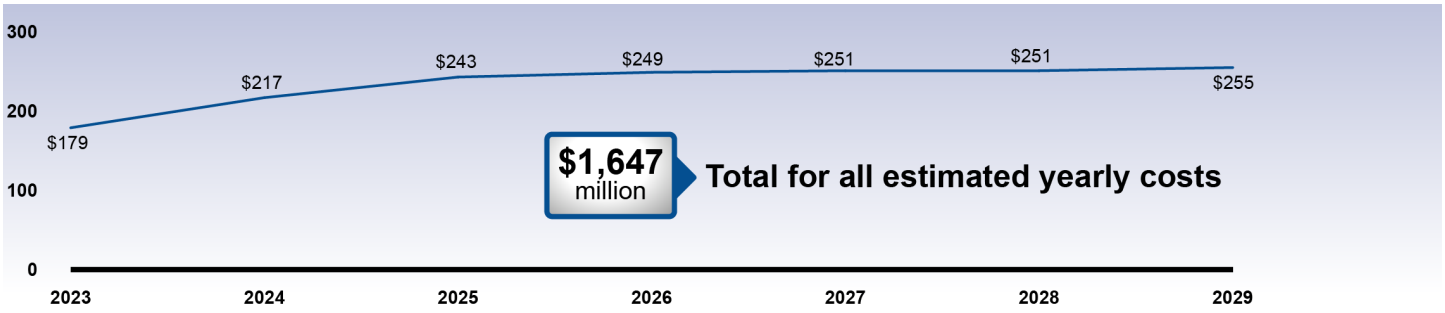
DOD officials identified multiple challenges being faced by JOMIS. For example, officials stated that the management of life cycle costs when receiving funding from three different appropriations creates additional administrative burden when project planning and budget forecasting.

COST AND BUDGET

DOD anticipates cost savings as a result of the lowered sustainment costs of the modern portfolio once legacy products are decommissioned but has not yet determined the expected amount.	JOMIS obligations equaled 0.61% of DOD's total fiscal year 2024 IT budget	Total anticipated life cycle costs: $1.647 billion over 7 years	DOD anticipates quantitative benefits with JOMIS, such as increased efficiency when moving patient data and increased interoperability with other federal agencies and international partners.

The Program Executive Office, Defense Healthcare Management Systems is responsible for both planning JOMIS's budget and providing the funding allocated for it. DOD officials stated that cost savings are expected from JOMIS due to the replacement of the Theater Medical Information Program-Joint legacy systems with the modernized portfolio of capabilities. These include, for example, the Theater Blood-Mobile capability and the Operational Medicine Data Service. Officials added that cost savings are expected to be calculated once new capabilities have been fully deployed and legacy systems have been decommissioned.

Estimated expenditures by fiscal year according to agency officials (in millions)



Source: GAO analysis of agency documentation. | GAO-25-106908

PRIOR AND ONGOING WORK

We previously issued two reports related to JOMIS. Specifically:

- GAO. *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.
- GAO. *IT Systems Annual Assessment: DOD Needs to Improve Performance Reporting and Development Planning*. GAO-23-106117. Washington, D.C.: June 13, 2023.

As of February 2025, we had one open recommendation to DOD from these reports. Specifically, we recommended that the Secretary of Defense should direct the DOD Chief Information Officer and Under Secretary of Defense for Acquisition and Sustainment to ensure that IT business programs developing software use the metrics and management tools required by DOD and consistent with those identified in GAO's *Agile Assessment Guide*.

We also have ongoing work summarizing the overall status and progress of JOMIS.

DEPARTMENT OF DEFENSE | Joint Warfighting Cloud Capability

Sources: DOD (logo); Nelson/stock.adobe.com (photo). | GAO-25-106908

The Joint Warfighting Cloud Capability (JWCC) provides the Department of Defense (DOD) with an enterprise-wide acquisition environment consisting of multiple indefinite delivery/indefinite quantity contracts for globally available, commercial cloud services. JWCC was initiated in November 2021 and DOD officials expect the acquisition to reach full operational capability by March 2025.

KEY INFORMATION

JWCC will use and store personally identifiable information.	Related key GAO high-risk area: Improving IT Acquisitions and Management. (GAO-25-107852)	JWCC is an Acquisition of Services contract, which was awarded to multiple cloud service providers in December 2022.	JWCC is the first enterprise contract vehicle that the entire DOD will be able to use to rapidly provision and access commercial cloud services directly from providers.

ACQUISITION BACKGROUND

Acquisition designation: Special interest acquisition[53]

Type of acquisition: New system with new capabilities

Scope of acquisition: Agency-wide

System users: DOD officials responded that the number of users is not applicable because JWCC is used to generate task orders

Unique investment identifier: 007-000103949

Total anticipated life cycle costs: $8.974 billion over 6 years

Development approach: Hybrid Agile processes using customized development by agency personnel

Project workforce: 46 government full-time equivalents and 32 contractor personnel

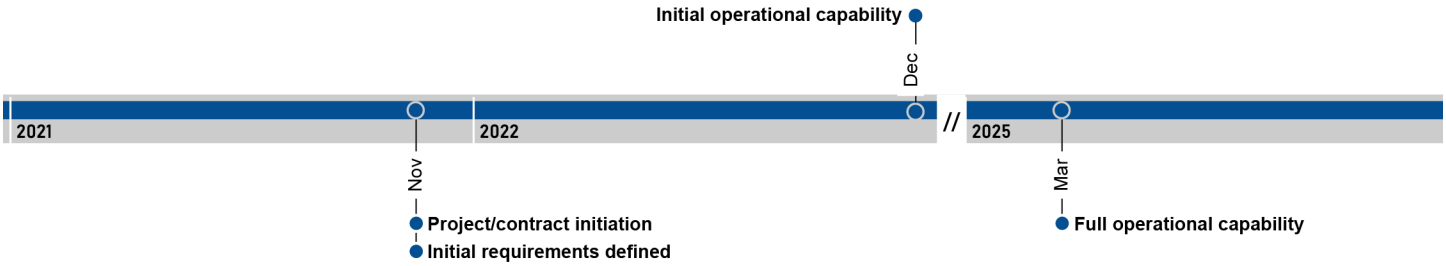
Federal IT Dashboard risk rating: According to DOD officials, JWCC did not receive a chief information officer (CIO) risk rating due to being a cloud delivery service

OVERVIEW

JWCC's mission is to provide a global, multi-vendor cloud capability with attributes that enable access to crucial warfighting data by those who need it anywhere in the world, and to secure data exchange at all classification levels. In this regard, JWCC is intended to provide cloud services that can rapidly expand to meet demand across all security domains and at all classification levels. The services are also expected to operate in disconnected, disrupted, intermittent, or limited network situations. In addition, JWCC is expected to provide the foundation to support multiple Secretary of Defense strategic initiatives, including artificial intelligence and machine learning.

CURRENT STATUS AND TIMELINE

JWCC continues working to develop the relationship with the cloud service providers, onboard more mission partners, and increase the use of cloud service offerings on JWCC. As of October 2024, DOD stated that JWCC has surpassed $1 billion in total life cycle value, of a maximum value of approximately $9 billion, with over 65 task orders issued by various components across DOD.



Source: GAO analysis. | GAO-25-106908

[53]Designated a special interest acquisition under DOD Instruction 5000.74, Defense Acquisition of Services. A special interest acquisition involves services that, by their nature or the circumstances related to their acquisition, deserve increased attention or care during planning, review, approval, and oversight.

AGENCY IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk				Moderate risk		High risk
Cybersecurity risk	Information privacy risk	Technical risk	Schedule risk	Organizational risk	Cost/budget risk	Risk of not implementing

CHALLENGES IDENTIFIED

Not a challenge							
Implementation of chosen system development methodology	Organizational alignment and structure	Cost constraints	Schedule slippages	Technical	Providing oversight and governance	Obtaining adequate funding/budget	Workforce issues

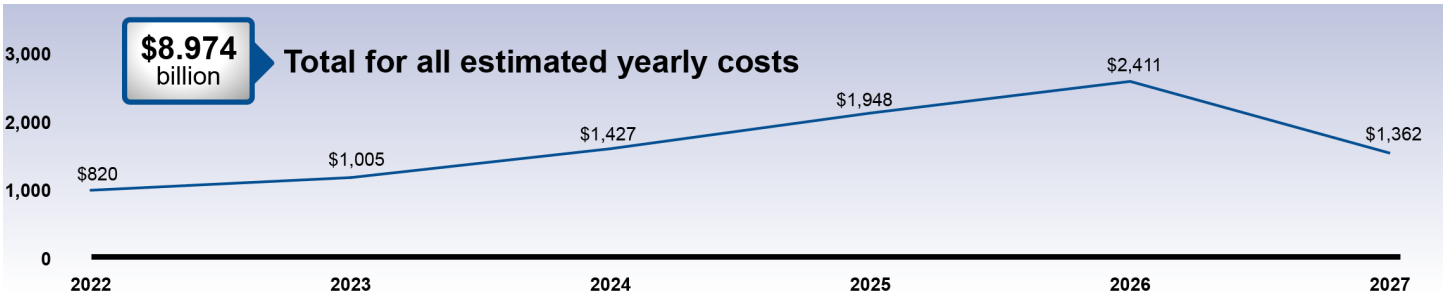
DOD identified several risks related to JWCC, such as organizational risk, cost/budget risks, and the risk of not implementing. For example, DOD officials stated that if JWCC is prematurely discontinued, the department would have to revert to a decentralized service model, which would significantly impede its ability to bridge critical capability gaps for the warfighter. Furthermore, new contracts would need to be established to foster innovation at a pace and scale that is aligned with the rapidly changing threat landscape. Officials estimated that such a shift in strategy could result in years of delays, hindering the department's ability to carry out its mission. DOD officials did not identify challenges faced by JWCC.

COST AND BUDGET

DOD anticipates cost savings at the task order level via specific discounts included by each cloud service provider but has not yet determined the expected amount.	JWCC obligations equaled 0.32% of DOD's total fiscal year 2024 IT budget.	Total anticipated life cycle costs: $8.974 billion over 6 years.	JWCC's key performance measures include determining whether cloud service providers have direct control over cloud infrastructure and capabilities at all three classification levels.

The Office of the Chief Financial Officer is responsible for both preparing JWCC's budget and funding the budget. JWCC is a new system providing new capabilities. Cost savings are expected to be generated at the task order level by specific discounts given by each cloud service provider, but DOD is not able to provide specific savings since they vary by cloud service provider and contract. JWCC is an indefinite delivery/indefinite quantity contract awarded to four commercial cloud service providers with a maximum value of approximately $9 billion.

Estimated expenditures by fiscal year according to agency officials (in millions)



Source: GAO analysis of survey results. | GAO-25-106908

PRIOR WORK

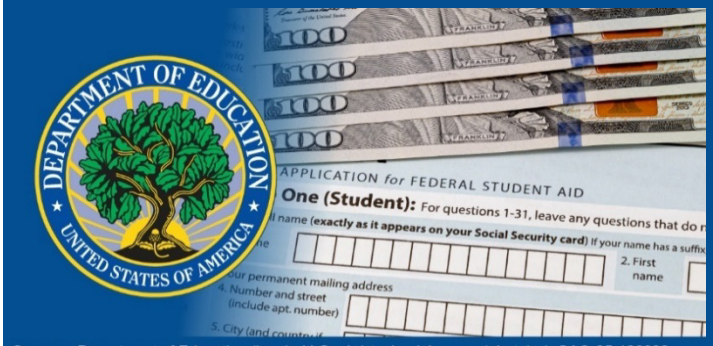
We have previously issued two reports related to DOD's JWCC:

- GAO. *Cloud Computing: DOD Needs to Improve Tracking of Data User Fees.* GAO-23-106247. Washington, D.C.: Sept. 12, 2023.
- GAO. *Cloud Computing: DOD Needs to Improve Workforce Planning and Software Application Modernization.* GAO-22-104070. Washington, D.C.: June 29, 2022.

As of February 2025, we had nine open recommendations to DOD related to JWCC. For example, we recommended that the Secretary of Defense should direct the DOD CIO to:

- develop a plan and time frame for adopting a tool to track and report cloud data egress fees across the department (GAO-23-106247);
- develop and execute a communication plan that will help employees understand the planned changes that will occur for the implementation of the department's enterprise-wide cloud environment (GAO-22-104070);
- ensure that all department components are held accountable for meeting the objectives, milestones, and time frames included in the department's enterprise-wide application rationalization process (GAO-22-104070).

DEPARTMENT OF EDUCATION | Free Application for Federal Student Aid Processing System



Sources: Department of Education (logo); JJ Gouin/stock.adobe.com (photo). | GAO-25-106908

The purpose of the Department of Education's Free Application for Federal Student Aid (FAFSA) Processing System (FPS) is to calculate student applicant's eligibility for federal student aid once their FAFSA is submitted and processed. Education officials reported that FPS was initiated due to statutory changes and to address GAO audit findings from June 2019. FPS achieved initial operating capability in December 2023 and is undergoing multiple stages of development of additional functionality and implementation. Education had not yet determined the full operational capability date.

KEY INFORMATION

FPS uses and stores personally identifiable information.	FPS has been rebaselined. The initial operating capability date was adjusted from October 2023 to December 2023.	In September 2024, we testified before the House of Representative's Subcommittee on Higher Education and Workforce Development on the need to address significant student aid IT system weaknesses. (GAO-24-107783)	FPS consists of 12 distinct products, which all contribute to the overall mission of creating, maintaining, and advancing the technical systems that process student FAFSA forms and determine student eligibility for Title IV financial aid.

ACQUISITION BACKGROUND

Acquisition designation: Major acquisition

Type of acquisition: Replacement of legacy system

Scope of acquisition: Office of Federal Student Aid

System users: Over 17 million students who complete the FAFSA annually and 5,400 institutions of higher education

Unique investment identifier: FPS is a subcomponent of the Award Eligibility Determination project (018-000003116)

Total anticipated life cycle costs: $203.3 million over 11 years

Development approach: Agile software development using contractor developed and open-source solutions

Project workforce: 21 government full-time equivalents and 212 contractor personnel full-time equivalents

Federal IT Dashboard risk rating: Not applicable. However, the Award Eligibility Determination project has a CIO risk rating of Medium, as of January 2025

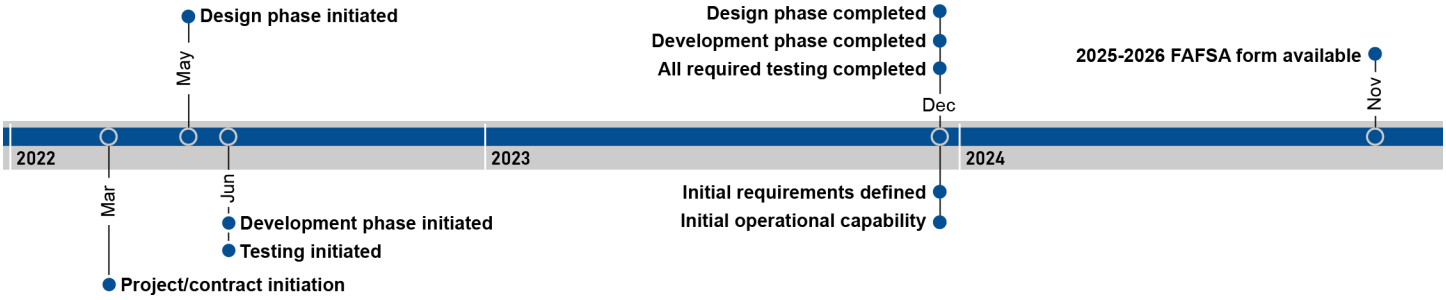
OVERVIEW

FPS replaced the Central Processing System, which calculates student eligibility for Title IV federal aid, or aid designated for postsecondary students.[54] A student's application process includes applying through the FAFSA form (electronic or paper format), or with help from a school's financial aid office. The calculation of federal aid directly impacts the financial support provided to individuals, organizations, and institutions.

In late December 2023, Education's Office of Federal Student Aid deployed FPS to process the 2024-2025 FAFSA forms. According to the office, in late March and early April 2024, processing and data errors were identified that affected approximately 30 percent of FAFSA forms. In September 2024, we testified that student aid applicants reported availability issues, submission errors, and significant load times, among other things.

CURRENT STATUS AND TIMELINE

FPS is undergoing development, testing, implementation, and maintenance efforts concurrently. FPS officials stated that functionality for the 2024-2025 FAFSA processing capability has been implemented. By replicating the 2024-2025 code in a separate environment, officials stated that Federal Student Aid is able to make modifications needed for the annual updates to FPS and implement a small number of improvements more efficiently. On November 21, 2024, Federal Student Aid made the 2025-2026 FAFSA form available to students seeking federal aid. Officials stated that they plan to continue to improve and upgrade the system throughout its lifecycle.



Source: GAO analysis. | GAO-25-106908

[54]Title IV of the Higher Education Act of 1965, codified as amended at 20 U.S.C. §§ 1070-1099d, authorizes programs that provide financial assistance to students attending a variety of postsecondary schools.

AGENCY IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Moderate risk		High Risk				
Organizational risk	Risk of not implementing	Cybersecurity risk	Technical risk	Information privacy risk	Cost/budget risk	Schedule risk

CHALLENGES IDENTIFIED

Identified by the agency as a challenge							
Implementation of chosen system development methodology	Organizational alignment and structure	Cost constraints	Schedule slippages	Technical	Providing oversight and governance	Obtaining adequate funding/budget	Workforce issues

FPS officials identified multiple high-risk areas, including cybersecurity, information privacy, technical, and the risk of not implementing. Officials reported that the impact of not implementing FPS would result in the Office of Federal Student Aid's inability to process student applications and determine eligibility, which is a core mission-critical business function for the office. Additionally, it may also result in financial penalties, damages, and delays that could have a ripple effect on other projects.

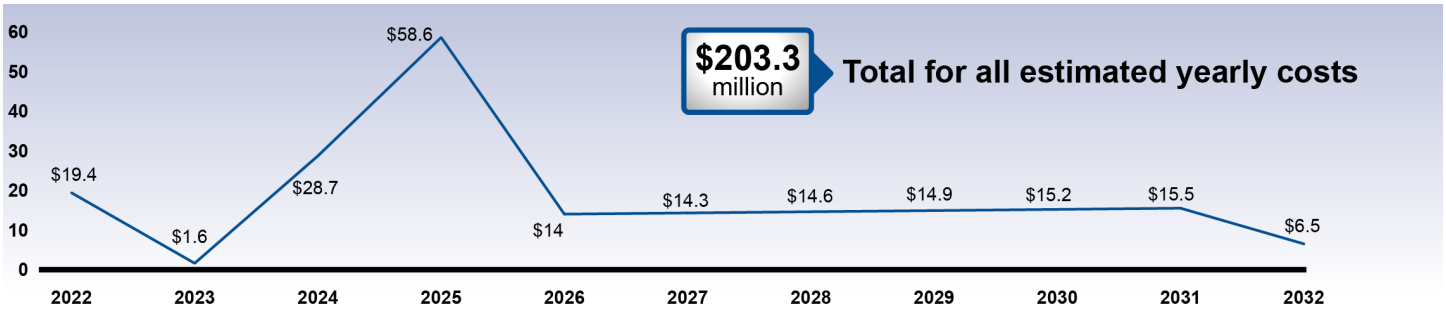
FPS officials also identified multiple challenges related to FPS. For example, officials reported experiencing challenges related to oversight and governance due to coordinating with highly matrixed subject matter experts, meaning those who work across multiple business units, managing different internal and external stakeholders. Additionally, officials reported challenges obtaining adequate funding and needing to adjust priorities in response to being funded under continuing resolutions for fiscal years 2022 and 2023.

COST AND BUDGET

Education has not yet determined if there will be cost savings associated with the implementation of FPS.	FPS is a subcomponent of the Award Eligibility Determination project. The project's obligations equaled 5.16% of Education's total fiscal year 2024 IT budget.	Total anticipated life cycle costs: $203.3 million over 11 years

Within the Office of Federal Student Aid, the Office of Student Experience and Aid Delivery, Technology Directorate, and Finance Directorate are responsible for preparing the budget for FPS. The Office of Federal Student Aid's Finance Directorate is responsible for allocating the funding for FPS.

Actual and estimated expenditures by fiscal year according to agency officials (in millions)



Source: GAO analysis of survey results. | GAO-25-106908

PRIOR AND ONGOING WORK

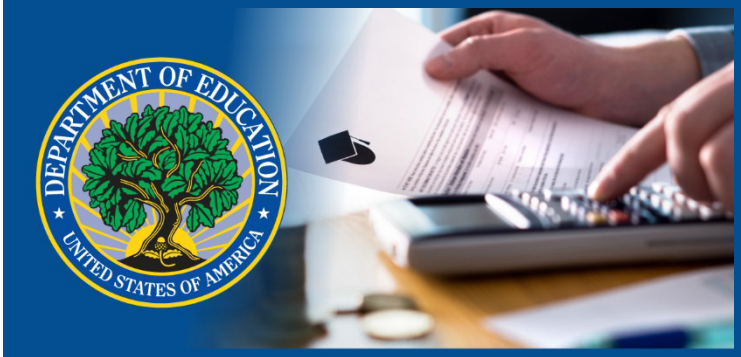
We previously issued several reports related to Education's federal student aid systems. Examples include:

- GAO. *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.
- GAO. *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.
- GAO. *Department of Education: Federal Student Aid System Modernization Project Should Better Estimate Cost and Schedule.* GAO-23-106376. Washington, D.C.: June 21, 2023.
- GAO. *Information Technology: Education Needs to Address Student Aid Modernization Weaknesses.* GAO-23-105333. Washington, D.C.: Oct. 20, 2022.

As of February 2025, we had six open IT and cybersecurity-related recommendations to Education related to FPS. For example, we recommended that the Secretary of Education should expeditiously (1) assess the role of the department's and Office of Federal Student Aid's CIOs in the continuing development of FPS, and (2) based on that assessment, develop and implement a plan for providing the department's CIO with a significant role in the governance and oversight of FPS while clarifying the responsibilities between the departmental and agency CIO.

We also have ongoing work looking at the Free Application for Federal Student Aid Processing System.

DEPARTMENT OF EDUCATION | Title IV Origination and Disbursement Modernization



Sources: Department of Education (logo); terovesalainen/stock.adobe.com (photo). | GAO-25-106908

The Department of Education's Title IV Origination and Disbursement (TIVOD) modernization acquisition provides cybersecurity and technology upgrades for several IT information systems maintaining a large repository of personally identifiable information on student loans. According to Education, in fiscal year 2023, the department's Federal Student Aid office delivered more than $114.1 billion to more than 9.7 million students attending approximately 5,600 postsecondary institutions. The modernization effort is in the pre-project phase and Education has not yet determined the life cycle cost estimate or planned completion dates for design, development, testing, and deployment.

KEY INFORMATION

TIVOD modernization will both use and store personally identifiable information.	In September 2024, we testified before the House of Representative's Subcommittee on Higher Education and Workforce Development on the need to address significant student aid IT system weaknesses. (GAO-24-107783)	TIVOD Modernization is a long-term project to review the systems in the current TIVOD contract and determine if, and how, they should be separated into distinct, manageable parts.	Education's federal student loan portfolio totals more than $1.6 trillion.

ACQUISITION BACKGROUND

Acquisition designation: Major acquisition

Type of acquisition: Replacement of legacy system

Scope of acquisition: Office of Federal Student Aid

System users: Institutions of higher education, state grant agencies, eligible and approved guarantee agencies, federal loan servicers, lenders and lender servicers, third-party software providers, and the Office of Federal Student Aid and its contractors, all serving over 43 million student customers

Unique investment identifier: TIVOD modernization does not have a Federal IT Dashboard entry

Total anticipated life cycle costs: Education has not determined the total anticipated life cycle costs associated with TIVOD modernization

Development approach: Education has not determined a development approach for TIVOD modernization

Project workforce: Education has not determined the project workforce needed to develop and implement TIVOD modernization

Federal IT Dashboard risk rating: TIVOD modernization does not have a Federal IT Dashboard entry or CIO risk rating because it is in the pre-project phase

OVERVIEW

Education's Federal Student Aid office is tasked with ensuring that eligible and participating students enrolled in postsecondary educational schools benefit from federal financial assistance for education and training. Specifically, the office is responsible for managing the student financial assistance programs authorized under Title IV of the Higher Education Act of 1965, as amended.[55] Education officials reported that, as federal student loans have become a core component of postsecondary education financing, it is now serving over 43 million student customers.

The scope of the TIVOD modernization effort encompasses multiple Federal Student Aid systems, such as the Common Origination and Disbursement system, which is used to process and disburse funds from various loans and grants maintained by Education. It also includes the following systems: the Enterprise Data Management and Analytics Platform service, the Federal Taxpayer Information Data Mart, the National Student Loan Data system, the Enterprise Data Warehouse and Analytics platform, the personal Master Data Management, and the Document Repository and Partner Customer Service. Additionally, TIVOD modernization includes the centralization of customer service desks multiple systems, serving internal staff and external partners. According to Education, the TIVOD modernization effort is part of a long-term strategy to meet evolving business needs, provide enhanced cybersecurity, increase flexibility and efficiency, and provide a strong foundation for future operations.

CURRENT STATUS AND TIMELINE

Education has not yet determined what type of system development lifecycle TIVOD Modernization will use. Currently, Education is mapping interdependencies between the components of TIVOD and developing a roadmap for how to proceed. Education plans to publish requests for information to solicit feedback from the vendor community on potential options for modernizing TIVOD. Education has not yet determined acquisition milestone dates, such as when the TIVOD modernization will initiate the design phase, initiate the development phase, or reach initial and full operational capability.

[55]Title IV of the Higher Education Act of 1965, codified as amended at 20 U.S.C. §§ 1070-1099d, authorizes programs that provide financial assistance to students attending a variety of postsecondary schools.

AGENCY IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk	High risk					
Organizational risk	Cybersecurity risk	Information privacy risk	Technical risk	Cost/budget risk	Schedule risk	Risk of not implementing

CHALLENGES IDENTIFIED

Identified by the agency as a challenge							
Obtaining adequate funding/budget	Workforce issues	Cost constraints	Schedule slippages	Providing oversight and governance	Technical	Implementation of chosen system development methodology	Organizational alignment and structure

TIVOD officials identified multiple high-risk areas, including cybersecurity, information privacy, technical, and the risk of not implementing. Officials reported that the impact of not implementing TIVOD modernization would result in increasing risk to financial and other private information, leading to secondary and tertiary impacts to mission partners such as the Internal Revenue Service, Social Security Administration, and Department of Veterans Affairs.

TIVOD officials also anticipate facing multiple challenges based on previous experiences with other projects, such as obtaining adequate funding/budget, providing oversight and governance, and addressing technical issues. For example, officials stated that the Federal Student Aid office is not currently equipped to adequately support TIVOD's challenges related to flatlined or decreasing budgets, insufficient resources for vendor oversight, and insufficient data management options. Specifically, agency officials stated that Federal Student Aid's dispersed data and current options for data management are insufficient, creating significant risks during data migration and integration efforts.

COST AND BUDGET

Education has not determined cost savings associated with TIVOD modernization.	Education has not determined the total anticipated life cycle costs associated with TIVOD modernization.	Education has not identified key performance indicators or parameters associated with TIVOD modernization.

Education's Next Generation Program Office is responsible for both preparing TIVOD modernization's budget and providing the funding for the acquisition. However, Education has not yet determined estimated expenditures by fiscal year. Further, Education has not yet determined cost savings associated with the implementation of TIVOD Modernization.

PRIOR AND ONGOING WORK

We previously reported and testified on Education's federal student aid systems. Examples include:

- GAO. *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.
- GAO. *Department of Education: Federal Student Aid System Modernization Project Should Better Estimate Cost and Schedule.* GAO-23-106376. Washington, D.C.: June 21, 2023.
- GAO. *Information Technology: Education Needs to Address Student Aid Modernization Weaknesses.* GAO-23-105333. Washington, D.C.: Oct. 20, 2022.

We also have ongoing work looking at a related system, the Free Application for Federal Student Assistance Processing System.

DEPARTMENT OF HEALTH AND HUMAN SERVICES | Indian Health Service Electronic Health Records Modernization

Sources: HHS (logo); Gefo/stock.adobe.com (photo). | GAO-25-106908

From 2018 to 2019, the Indian Health Service (IHS)—an operating division of Health and Human Services (HHS)—engaged in comprehensive research and analysis of the current state of the IHS Health IT infrastructure and options for modernization. In doing so, IHS identified multiple shortcomings, such as outdated technology and an unsustainable support model. The IHS Electronic Health Record (EHR) modernization effort is intended to implement a new EHR solution and provide technology and process tools that will allow healthcare providers and administrators to deliver required services to the communities and populations they serve.

KEY INFORMATION

IHS EHR Modernization will store and use personally identifiable information.	Related key GAO high-risk area: Improving Federal Management of Programs That Serve Tribes and Their Members. (GAO-23-106203)	IHS EHR Modernization is expected to replace the Resource and Patient Management System, which has been in use for more than 40 years.	IHS EHR Modernization was started to address legislative requirements, audit findings from GAO and HHS Office of Inspector General, presidential directives, and HHS's determination that legacy systems were not supporting high-quality patient care.

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Replacement of legacy system

Scope of acquisition: Agency wide

System users: Approximately 48,000 users

Unique investment identifier: 09-000452168

Total anticipated life cycle costs: $6.204 billion over 10 years

Development Approach: Various incremental development approaches using commercial off-the-shelf solutions

Project workforce: 33 full-time equivalent government employees at IHS headquarters, with a need for 66 additional full-time equivalents identified. Additionally, nearly 500 contractor staff are supporting the modernization effort on behalf of IHS

Federal IT Dashboard risk rating: Moderately low, as of January 2025

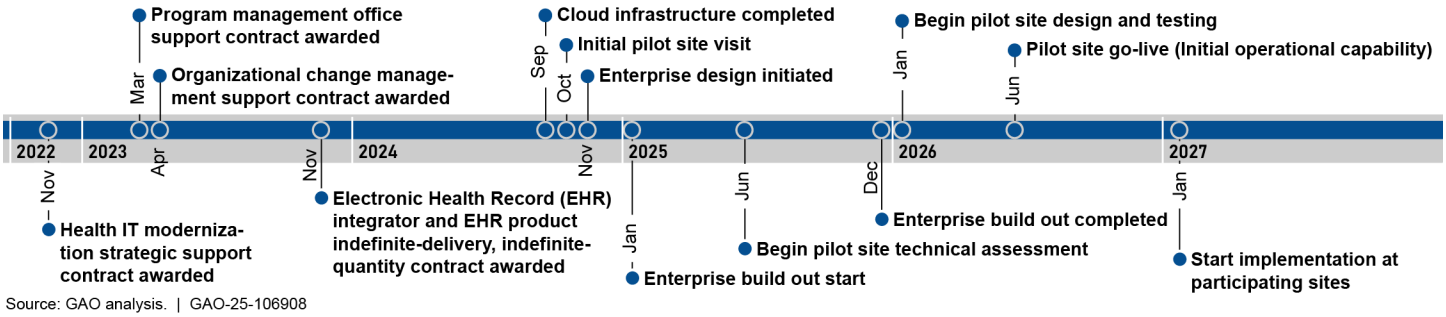
OVERVIEW

IHS EHR Modernization is critical to the mission of IHS, as the EHR system is the core infrastructure for both patient care delivery and revenue recovery at IHS facilities. IHS and HHS identified the following shortcomings with the current state of IHS Health IT infrastructure: outdated technology, unsustainable support model, limited healthcare data and information interoperability, and inconsistent clinical and business practices. Moreover, the current system—the Resource and Patient Management System—has very limited capability to support critical patient care services, such as surgery, intensive care, and labor and delivery, among others. The lack of modern digital tools creates a significant risk to quality of care, care coordination, patient safety, and the ability of the IHS to understand and report on the success of its mission.

IHS EHR is intended to provide an enterprise approach to health IT and is planned fill numerous technology gaps currently unsupported by the Resource and Patient Management System. Expected benefits include, for example, minimizing the technical support burden for facilities, increasing the focus on system optimization for end-users, and promoting standardization and best practices.

CURRENT STATUS AND TIMELINE

IHS EHR Modernization uses Agile, in addition to other continuous development lifecycles, and is undergoing project initiation and defining initial requirements. As of October 2024, IHS EHR Modernization officials reported that the acquisition planned to conduct iterative design workshops, end to end testing, data validation, security authorizations, and related activities in fiscal year 2025 through 2026, with a plan to implement the new EHR at selected pilot sites in mid-2026. Subsequent rollout of the solution to the remainder of IHS, as well as to tribal and urban Indian organization partners, is planned to take place over a number of years beginning in fiscal year 2027. IHS had not yet determined the initial operational capability or full operational capability dates.



Source: GAO analysis. | GAO-25-106908

AGENCY IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Moderate risk						High risk
Organizational risk	Cybersecurity risk	Information privacy risk	Technical risk	Cost/budget risk	Schedule risk	Risk of not implementing

CHALLENGES IDENTIFIED

Not a challenge			Identified by the agency as a challenge				
Cost constraints	Providing oversight and governance	Implementation of chosen system development methodology	Obtaining adequate funding/budget	Workforce issues	Schedule slippages	Technical	Organizational alignment and structure

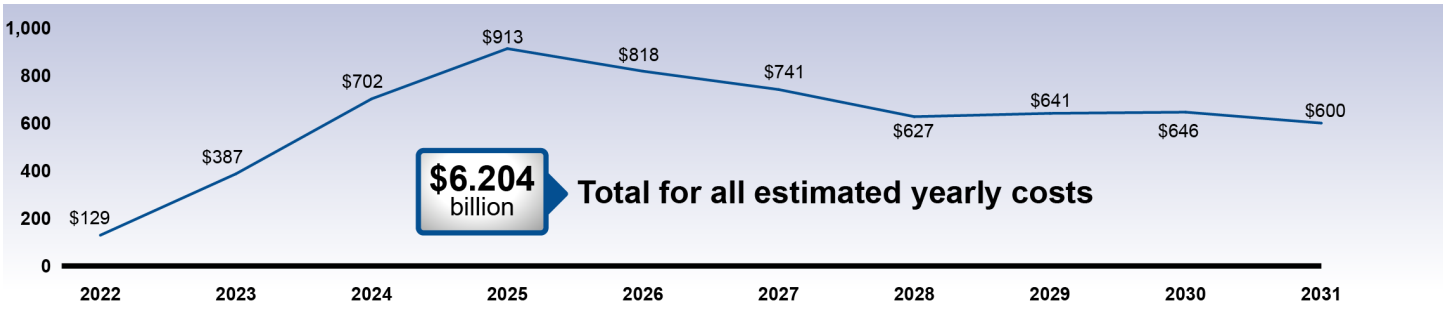
HHS identified multiple risks, ranging from moderate to high, faced by IHS EHR Modernization. For example, HHS officials stated that the current record keeping system is increasingly difficult and expensive to maintain, as it is built on outdated technology that uses support resources that become scarcer every year. IHS EHR officials also reported facing multiple challenges. For example, IHS EHR officials stated that funding to begin work was received, but funding challenges have resulted in longer schedules for performing critical task order work. Additionally, officials reported that the implementation of a centralized and standardized IHS EHR system requires a strategy of constant communication to encourage understanding and acceptance of the new system.

COST AND BUDGET

HHS has not anticipated cost savings associated with IHS EHR Modernization, but officials stated that this acquisition was determined to be the most cost-effective path forward to meet increasing healthcare technology demands.	IHS EHR Modernization obligations equaled 2.09% of HHS's total fiscal year 2024 IT budget.	Total anticipated life cycle costs: $6.204 billion over 10 years.	IHS EHR Modernization officials stated that by establishing a centralized operations center, duplication of work and hardware costs are expected to be reduced, improving the efficiency of IT support services.

The IHS Office of Information Technology, Division of Health IT Modernization and Operations, is responsible for preparing the budget for IHS EHR Modernization. IHS EHR Modernization is funded by congressional appropriations. IHS officials stated that an enterprise approach leveraging commercially available systems is the most cost-effective path forward to meet the needs of the agency but have not yet determined what the cost savings produced by IHS EHR Modernization will be.

Estimated expenditures by fiscal year according to agency officials (in millions)



Source: GAO analysis of survey results. | GAO-25-106908

PRIOR WORK

We previously issued two reports related to the IHS EHR Modernization:

- GAO. *Indian Health Service: Actions Needed to Improve Use of Data on Adverse Events.* GAO-23-105722. Washington D.C.: July 10, 2023.
- GAO. *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*. GAO-19-471. Washington D.C.: June 11, 2019.

DEPARTMENT OF HOMELAND SECURITY | Homeland Advanced Recognition Technology

Sources: DHS (logo); Pakin/stock.adobe.com (photo). | GAO-25-106908

The purpose of the Homeland Advanced Recognition Technology (HART) is to provide core biometric identity services to support the Department Homeland Security's (DHS) missions. HART was initiated in September 2017 to replace the Automated Biometric Identification System (IDENT) due to system performance limitations and rising sustainment costs.

KEY INFORMATION

HART will use and store personally identifiable information.	Related key GAO high-risk area: Improving IT Acquisitions and Management. (GAO-25-107852)	HART was rebaselined in May 2019, April 2022, and September 2023 attributed to a mix of cost and schedule breaches, caused primarily by technical issues.	DHS officials stated that multimodal biometric services provided by HART will increase identity surety and assist in overcoming field operational challenges when fingerprints prove insufficient.

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Replacement of legacy system

Scope of acquisition: Agency-wide

System users: Over 45 U.S. and international organizations

Unique investment identifier: 024-000005253

Total anticipated life cycle costs: $2.245 billion over 23 years, as of July 2024

Development approach: Agile software development using contractor developed, commercial off-the-shelf, and open-source software

Project workforce: 26 government full-time equivalent employed and approximately 221 full-time equivalent contractor personnel for HART specifically, and 18 full-time equivalent contractor personnel shared between mission systems, including HART

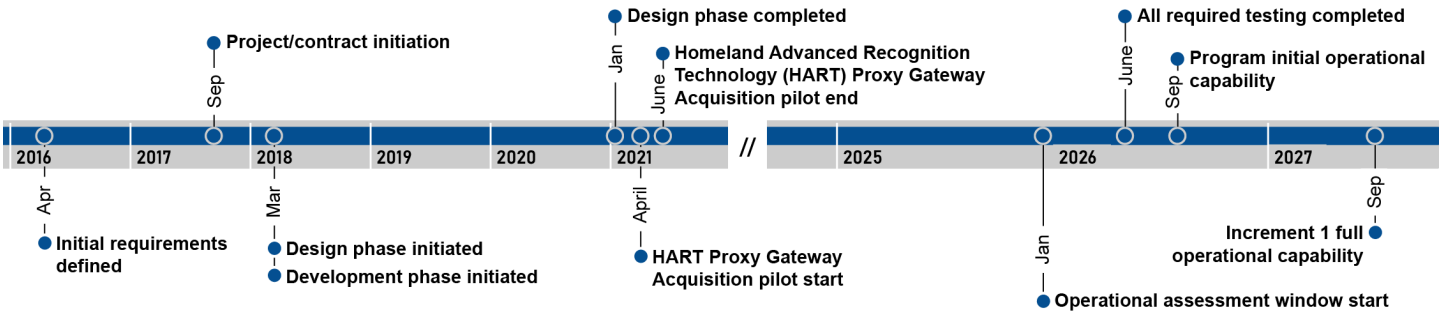
Federal IT Dashboard risk rating: Medium, as of December 2024

OVERVIEW

HART's mission is to provide a central, DHS-wide repository to compare, store, share biometric and associated biographic information. HART is expected to improve efficiencies by providing multimodal biometric services, improving detection and matching biometric data to information that may justify further investigation, and delivering capabilities and services more rapidly. According to agency officials, HART data and analysis is intended to secure and protect the United States against terrorism; enable data integration and analysis; support and strengthen responsive immigration processing and law enforcement; minimize disruptions to trade and travel; and support a smarter, stronger border by enhancing DHS's security infrastructure through support of new technologies.

CURRENT STATUS AND TIMELINE

HART is using Agile software development and is undergoing development, testing, and maintenance efforts concurrently. According to agency officials, HART is currently carrying out maintenance of the HART Proxy Gateway, which is a subsystem of HART. This subsystem ingests customer requests and returns responses from IDENT as the current system of record. Prior to HART reaching initial operational capability, it also enables the parallel operation and testing of HART. Additionally, agency officials stated that the program is conducting development, integration, and testing of increment 1—the core operating infrastructure. Future capabilities are expected be addressed after HART is fielded and IDENT is decommissioned.



Source: GAO analysis. | GAO-25-106908

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk			Moderate risk	High risk		
Organizational risk	Cybersecurity risk	Information security risk	Technical risk	Cost/budget risk	Schedule risk	Risk of not implementing

CHALLENGES IDENTIFIED

Not a challenge				Identified by the agency as a challenge			
Workforce issues	Providing oversight and governance	Implementation of chosen system development methodology	Organizational alignment and structure	Obtaining adequate funding/budget	Cost constraints	Schedule slippages	Technical

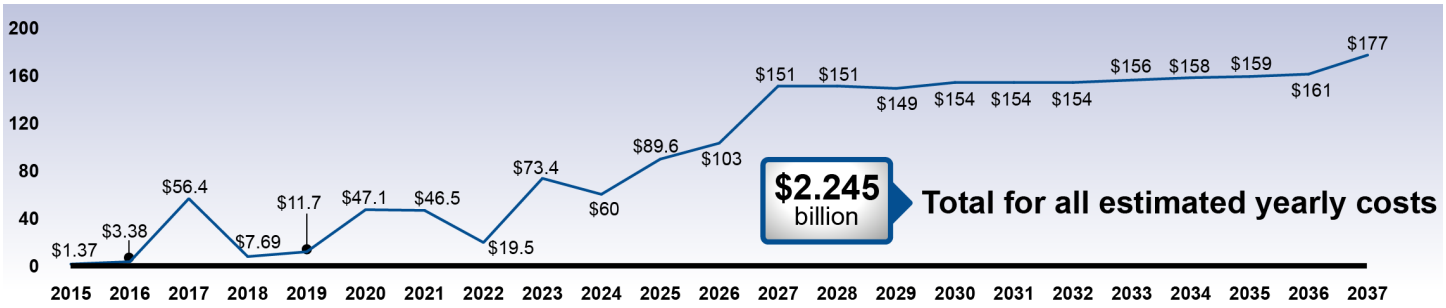
DHS identified several program risks in its effort to replace IDENT with HART, such as cost and budget risks, schedule risks, and the risk of not implementing. For example, DHS officials stated that the early termination of HART will significantly hamper immigration, credentialing, and law enforcement missions, among other impacts. DHS officials identified several challenges faced by HART, such as obtaining adequate funding, cost constraints, schedule slippages, and technical challenges. Officials stated that delays in replacing IDENT with HART has resulted in DHS needing to fund operations and maintenance for both systems, despite receiving funding based on the lower cost of operating HART alone.

COST AND BUDGET

DHS anticipates cost savings after implementing HART and decommissioning the Automated Biometric Identification System.	HART obligations equaled 0.8% of DHS's total fiscal year 2024 IT budget.	Total anticipated life cycle costs: $2.245 billion over 23 years	DHS anticipates quantitative benefits with HART, such as the reduced cost of infrastructure and increased availability of multimodal biometric services.

Within DHS, the Office of Biometric Identity Management is responsible for both preparing the budget and funding HART. HART has been rebaselined multiple times for either cost or schedule breaches. DHS officials anticipate that HART will result in cost savings after implementation is completed and IDENT is decommissioned. Actual savings are not expected to be realized until HART has been operating for a full year.

Actual and estimated expenditures by fiscal year according to agency officials (in millions)



Source: GAO analysis of survey results. | GAO-25-106908

Note: Yearly expenditures may not add up to total due to rounding.

PRIOR AND ONGOING WORK

We have previously issued several reports related to DHS's HART program. Examples include:

- GAO. *DHS Annual Assessment: Most Programs Are Meeting Current Goals, but Some Continue to Face Cost and Schedule Challenges.* GAO-24-106573. Washington, D.C.: Feb. 22, 2024.
- GAO. *Biometric Identity System: DHS Needs to Address Significant Shortcomings in Program Management and Privacy.* GAO-23-105959. Washington, D.C.: Sept. 12, 2023.
- GAO. *DHS Annual Assessment: Major Acquisition Programs Are Generally Meeting Goals, but Cybersecurity Policy Needs Clarification.* GAO-23-106701. Washington, D.C.: Apr. 20, 2023.

As of February 2025, we had nine open IT and cybersecurity related recommendations to DHS pertaining to HART. For example, we recommended that the Secretary of DHS should direct the Office of Biometric Identity Management Director to:

- revise the schedule estimate for the HART program that incorporates the best practices called for in the GAO *Schedule Assessment Guide*. (GAO-23-105959)
- update the cost estimate for the HART program to account for all costs and incorporate the best practices called for in the GAO *Cost Estimating and Assessment Guide*. (GAO-23-105959)

We have ongoing work looking at DHS's progress in implementing our previous recommendations on the HART program and contractor implementation of privacy controls within HART, among other areas.

DEPARTMENT OF HOMELAND SECURITY | Non-Intrusive Inspection Integration

Sources: DHS (logo); cat027/stock.adobe.com (photo). | GAO-25-106908

The U.S. Customs and Border Protection (CBP), a component of the Department of Homeland Security, has a mission to protect the public by preventing the entrance of dangerous contraband at points of entry throughout the country. The Non-Intrusive Inspection (NII) Integration Program is intended to support this mission by helping CBP expand detection capabilities, lower costs, and enhance efficiency with the addition of new technology. NII Integration is also expected to enhance the system architecture for the NII Program. The acquisition's contract initiation occurred in October 2022.

KEY INFORMATION

NII Integration will use and store personally identifiable information.	Related key GAO high-risk area: Strengthening Department of Homeland Security IT and Financial Management. (GAO-23-106203)	The Office of Field Operations within CBP is responsible for oversight of NII Integration.	NII Integration is intended to give CBP personnel access to artificial intelligence technology which is expected to increase the efficiency of detection at ports of entry across the country.

ACQUISITION BACKGROUND

Acquisition designation: Major acquisition

Type of acquisition: New system with new capabilities

Scope of acquisition: Component/bureau-specific within CBP

System users: Officials anticipate that approximately 26,000 CBP officers and 19,000 Border Patrol agents will utilize this acquisition in the field

Unique investment identifier: 024-000005119

Total anticipated life cycle costs: $5.701 billion over 19 years[56]

Development approach: Agile software development using contractor-developed and commercial off-the-shelf solutions

Project workforce: Approximately 30 government full-time equivalents and approximately 58 contract personnel

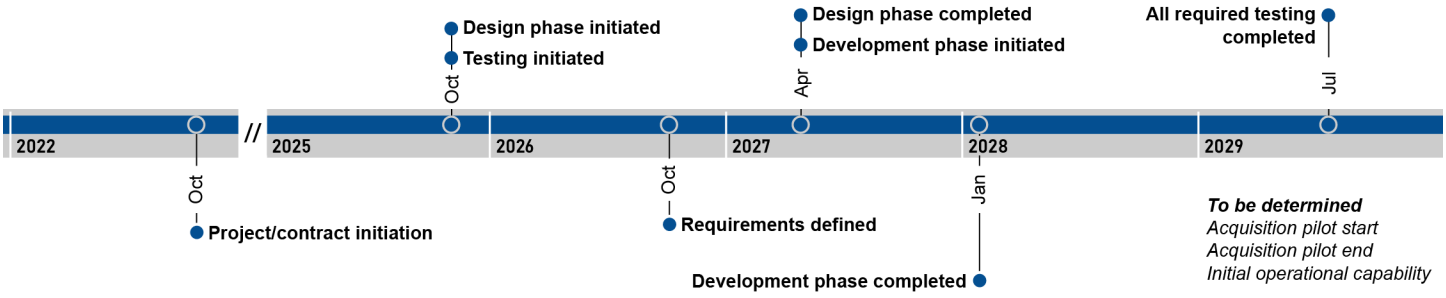
Federal IT Dashboard risk rating: Medium, as of December 2024

OVERVIEW

CBP is developing NII Integration to assist the agency in its mission of ensuring the safety and security of the American people by enhancing CBP's ability to scan for illegal contraband at domestic land, sea, and airports of entry. The primary objective of the acquisition is to improve and transform the existing standalone architecture of the NII, which has limited capabilities. The new system is expected to allow agency officials to increase the volume of image scans that CBP personnel can process to monitor the presence of illegal contraband by using artificial intelligence technology and an improved infrastructure to support the new capabilities. NII Integration scanning units are intended to examine passengers, as well as containers, railcars, and other items to prohibit potential threats or contraband from entering the United States. Agency officials stated that all required testing for NII Integration is planned to be completed by the end of 2029 but have not yet determined full operational capability date.

CURRENT STATUS AND TIMELINE

Agency officials reported that CBP is still in the process of defining the requirements for NII Integration after the contract initiation occurred in October 2022. The officials added that NII Integration will be following an Agile software development methodology to enable continuous development of contractor-developed and commercial off-the-shelf solutions. As a result, agency officials stated that the program is working to obtain agency approval to solidify a functional design for NII Integration and initiate the design phase in early 2025, as well as continuing to define the initial requirements. CBP had not yet determined the initial operational capability or full operational capability dates.



Source: GAO analysis. | GAO-25-106908

[56]The Department of Homeland Security indicated that this figure is preliminary because the program had not yet been baselined.

AGENCY IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk			Moderate risk				
Information privacy risk	Organizational risk	Cybersecurity risk	Schedule risk	Information privacy risk	Cost/budget risk	Technical risk	Risk of not implementing

CHALLENGES IDENTIFIED

Not a challenge			Identified by the agency as a challenge				
Implementation of chosen system development methodology	Organizational alignment and structure	Providing oversight and governance	Schedule Slippages	Cost constraints	Technical	Obtaining adequate funding/budget	Workforce issues

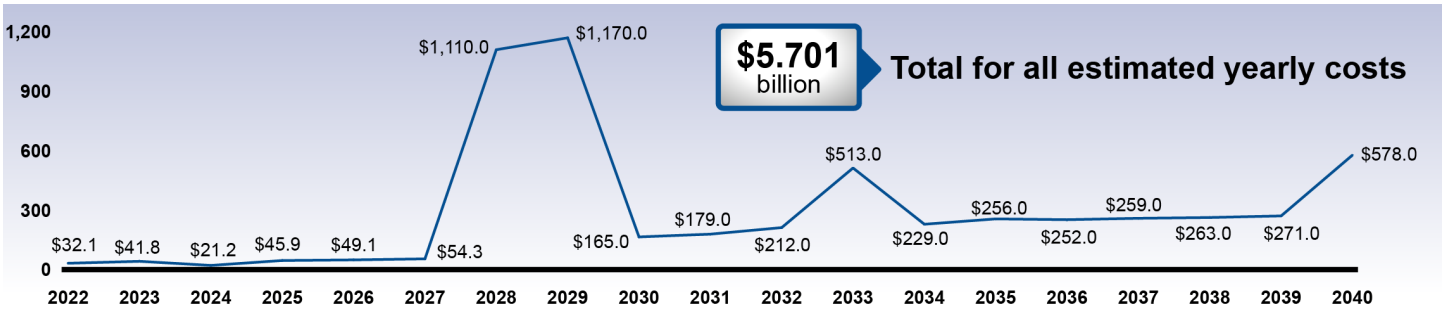
Agency officials reported a variety of risks and challenges which impact the development of NII Integration. More specifically, schedule risk, information privacy risk, cost/budget risk, technical risk, and risk of not implementing were designated as having a moderate risk. Furthermore, officials identified challenges such as schedule slippages, cost constraints, technical, obtaining adequate funding/budget, and workforce issues. Officials cited examples to support these designations, such as difficulties working with new technologies to train the artificial intelligence algorithms used for NII Integration's image processing capabilities and adapting to internal leadership changes. Officials added that cost and budget will remain a top risk for the acquisition as NII Integration does not have its own funding profile and is currently using funds budgeted for the previous legacy system. Additional funding is not projected to be requested until 2025.

COST AND BUDGET

Agency officials are unsure if there will be cost savings after NII Integration is deployed.	NII Integration obligations equaled 5.25% of DHS' total fiscal year 2024 IT budget.	Total anticipated life cycle costs: $5.701 billion over 19 years.	DHS anticipates that NII Integration will increase the speed and efficiency with which CBP personnel conduct contraband detection.

Agency officials stated that CBP's Office of Field Operations is responsible for both funding the acquisition and providing oversight. NII Integration has not required rebaselining at any point during development as CBP is still working to create a formal baseline. Agency officials stated that current funding is focused on meeting the increased infrastructure costs related to the installation of NII Integration technology in the field. Officials added that they are unsure if there will be cost savings after the acquisition is deployed.

Actual and estimated expenditures by fiscal year according to agency officials (in millions)



Source: GAO analysis of survey results. | GAO-25-106908

Note: The Department of Homeland Security indicated that the total life cycle cost estimate is preliminary because the program had not yet been baselined.

PRIOR WORK

We have previously issued several reports on DHS's NII Integration. Examples include:

- GAO. *DHS Annual Assessment: Most Programs Are Meeting Current Goals, but Some Continue to Face Cost and Schedule Challenges.* GAO-24-106573. Washington, D.C.: Feb. 22, 2024.
- GAO. *DHS Annual Assessment: Major Acquisition Programs Are Generally Meeting Goals, but Cybersecurity Policy Needs Clarification.* GAO-23-106701. Washington, D.C.: Apr. 20, 2023.
- GAO. *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*. GAO-23-106203. Washington, D.C.: Apr. 20, 2023.

DEPARTMENT OF JUSTICE | SENTRY Modernization – Centralized Inmate Case Logistics Operations and Planning System

The SENTRY Modernization - Centralized Inmate Case Logistics Operations and Planning System (CICLOPS) will become the primary case management system for individuals in Federal Bureau of Prisons' (FBOP) custody. The contract for this acquisition was awarded in 2021 and is intended to modernize an existing legacy system used to monitor inmate data housed in FBOP facilities. CICLOPS is projected to attain initial operational capability in July 2025 and full operational capability by December 2026.

Sources: Department of Justice (logo); blackboard/stock.adobe.com (photo). | GAO-25-106908

KEY INFORMATION

CICLOPS will use and store personally identifiable information.	Related key GAO high-risk area: Strengthening Management of the Federal Prison System. (GAO-23-106203)	The FBOP's Information Technology and Data Division (principally, System Development Branch) is responsible for oversight of the acquisition.	CICLOPS is also expected to modernize the case management of inmates from other jurisdictions (e.g., the military and Washington, D.C. inmates) housed in FBOP facilities.

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Modernization of legacy system

Scope of acquisition: Component/bureau-specific to FBOP

System users: Over 38,000 users within FBOP

Unique investment identifier: 011-000002705

Total anticipated life cycle costs: $68.64 million over 10 years

Development Approach: Agile software development using multiple approaches, including customized development by agency personnel and contractor development.

Project workforce: 6 government full-time equivalents and 34 contractor personnel.

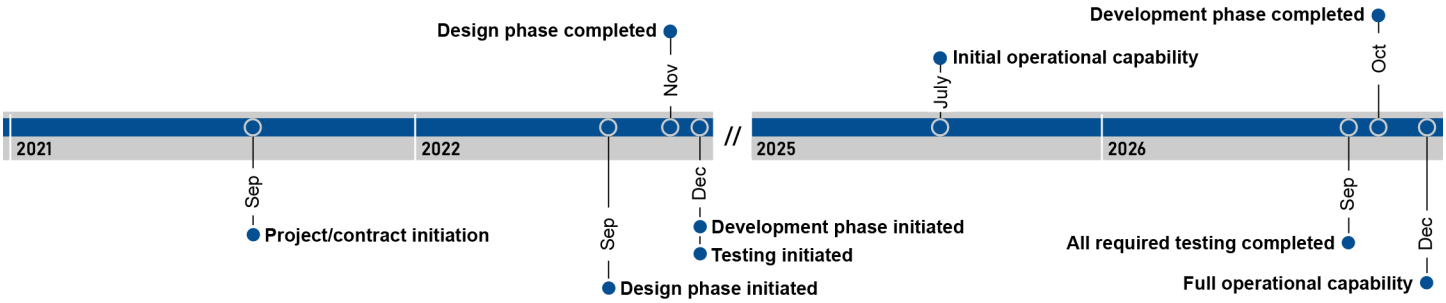
Federal IT Dashboard risk rating: Medium, as of September 2024

OVERVIEW

The Department of Justice's FBOP is responsible for the collection, dissemination, and governance of various data associated with the inmates housed in its facilities to manage their care and supervision. To carry out this responsibility, FBOP is modernizing its primary mission support and case management system with the development of CICLOPS. CICLOPS is expected to use various applications to process, in real-time, sensitive but unclassified inmate information. The new application environment is intended to enable improved data storage and analysis, and FBOP officials stated that the acquisition is expected to support the rapid development of additional applications which depend on data from CICLOPS. Ultimately, CICLOPS is intended to provide the over 38,000 personnel at FBOP and federal law enforcement agencies with the necessary tools to monitor the information of FBOP inmates.

CURRENT STATUS AND TIMELINE

FBOP officials stated that CICLOPS is using continuous development under an Agile development framework and completed the design phase in November 2022. The acquisition is currently in both the development and maintenance phases. This involves the maintenance of the current SENTRY legacy system and development efforts for the SENTRY CICLOPS modernization. Officials also reported that initial operational capability is expected be deployed beginning in July 2025 and all required testing is expected to be completed by September 2026. The CICLOPS modernization is projected for full operational capability by the end of December 2026.



Source: GAO analysis. | GAO-25-106908

AGENCY IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk		Moderate risk		High risk		
Cost/budget risk	Schedule risk	Organizational risk	Technical risk	Cybersecurity risk	Information privacy risk	Risk of not implementing

CHALLENGES IDENTIFIED

Not a challenge							
Implementation of chosen system development methodology	Organizational alignment and structure	Cost constraints	Schedule slippages	Technical	Providing oversight and governance	Obtaining adequate funding/budget	Workforce issues

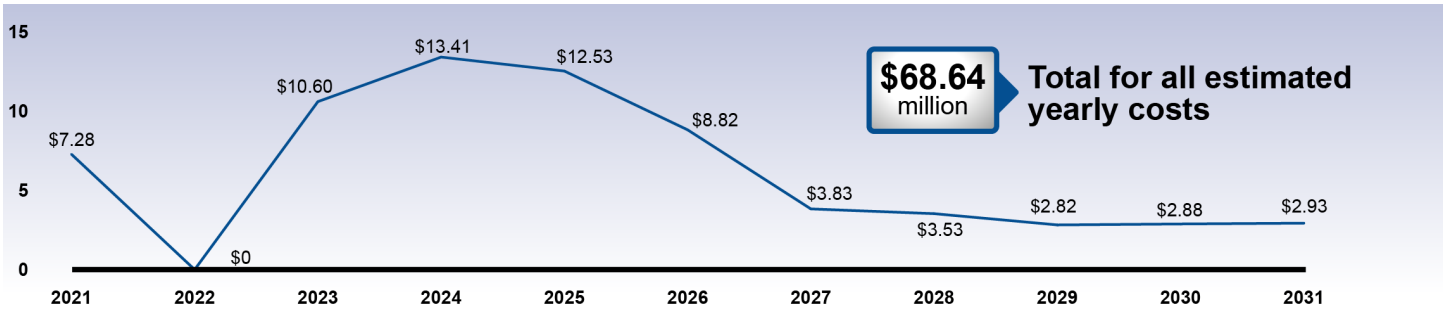
FBOP officials identified numerous risk factors associated with the CICLOPS acquisition. Cybersecurity and information privacy risks represent two of the three high-risk areas identified by agency officials. According to FBOP officials, maintaining security standards will be vital as the acquisition will both use and store personally identifiable information. The risk of not implementing was the final high-risk area identified by the agency. Officials reported that implementation of the system is vital as it will allow FBOP to migrate from a mainframe computer. Further, officials noted that it will allow FBOP to take advantage of cloud services to improve scaling, introduce new security frameworks, and improve cost management. Officials also classified organizational and technical risks as posing a moderate risk to the acquisition.

COST AND BUDGET

FBOP does not anticipate any measurable cost savings with CICLOPS.	CICLOP's obligations equaled 0.38% of Justice's total fiscal year 2024 IT budget.	Total anticipated life cycle costs: $68.64 million over 10 years	Justice anticipates this acquisition will increase the availability of resources to maintain the modernized environment, scalability, and cloud compatibility once implemented.

FBOP officials reported that the IT Planning and Development Branch is responsible for funding the acquisition. FBOP's Information Technology and Data Division, and in particular, the System Development Branch, is responsible for oversight of the acquisition. FBOP officials reported that the acquisition has not required re-baselining at any point during its development. Officials stated that no cost savings are expected upon deployment; however, the acquisition is expected to yield benefits long-term as operational costs associated with operation of the mainframe should be offset once cloud optimization can be leveraged. In addition, system users, FBOP customers, and the public are expected to benefit from the use of an updated application environment and related services. Lastly, FBOP officials expect improved data storage, data analysis, and cloud automation services from the acquisition.

Actual and estimated expenditures by fiscal year according to agency officials (in millions)



Source: GAO analysis of survey results. | GAO-25-106908

PRIOR WORK

We have previously issued two reports related to FBOP's CICLOPS. Examples include:

- GAO. *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*. GAO-23-106203. Washington, D.C.: Apr. 20, 2023.
- GAO. *Federal Prisons: Bureau of Prisons Should Improve Efforts to Implement its Risk and Needs Assessment System.* GAO-23-105139. Washington, D.C.: Mar. 20, 2023.

DEPARTMENT OF STATE | Consular Systems Modernization

Sources: Department of State (logo); Rawpixel.com/stock.adobe.com (photo). | GAO-25-106908

The Department of State's Consular Systems Modernization (CSM) acquisition supports the department's ConsularOne initiative. This initiative is intended to modernize and consolidate approximately 90 discrete legacy applications that help analysts provide consular services—including visa and passport application, visa adjudication and issuance, and other consular services—into a common technology framework. One of the goals of this acquisition is to modernize State's tools and technologies by providing online business service capabilities, such as passports, visas, repatriation loans, and travel alerts, through the ConsularOne initiative. Through this acquisition, the department seeks to avoid increased costs for its continued investment in legacy systems.

KEY INFORMATION

CSM will use and store personally identifiable information.	State's Office of the Procurement Executive, Office of Acquisitions Management, and the Bureau of Consular Affairs' Consular Systems and Technology Office are responsible for the oversight of CSM.	The CSM investment was rebaselined in 2018 due to new technologies being used.	State anticipates that CSM will be used by millions of U.S citizens and international travelers.

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Modernization of legacy system.

Scope of acquisition: Component/bureau specific for the Bureau of Consular Affairs

System users: 8,000 internal users and approximately 15,000,000 external users (e.g., the public and non-Department of State government employees and contractors)

Unique investment identifier: 014-000000474

Total anticipated life cycle costs: Approximately $385 million over 8 years

Development approach: Agile development using commercial off-the-shelf solutions.

Project workforce: 12 government full-time equivalents and approximately 200 contractor personnel.

Federal IT Dashboard risk rating: Moderately high, as of January 2025

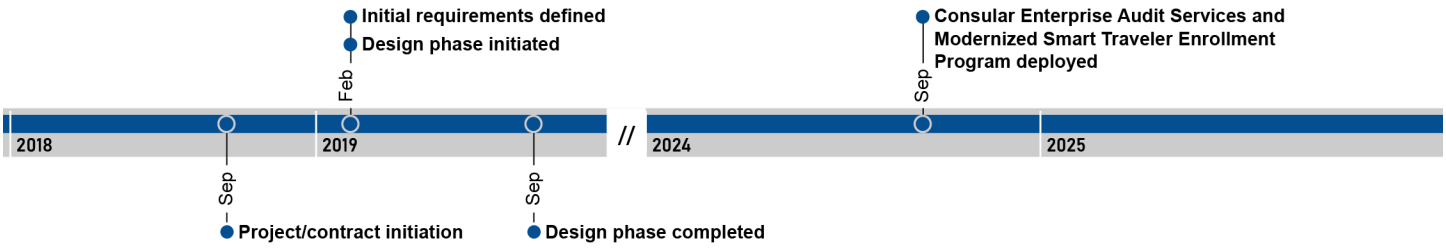
OVERVIEW

State is charged with protecting the lives and interests of U.S. citizens overseas. To help achieve this task, the department provides consular services through the Bureau of Consular Affairs. For example, the Bureau of Consular Affairs is responsible for the adjudication of visa and passport applications and facilitating legitimate travel to the U.S.

To further its mission, State is undertaking efforts to modernize its consular service legacy systems through the CSM acquisition. CSM is the contract vehicle that provides engineering and operations resources to support the bureau's ConsularOne initiative. This initiative is expected to provide a paperless processing mechanism, improved self-service options, integrated fraud detection and prevention, enhanced financial and management information data, and a standardized user interface, among other benefits. As part of CSM, ConsularOne is to provide self-service capabilities for customers through a user-friendly website and facilitate a digital paperless workflow through an online application process, among other things.

CURRENT STATUS AND TIMELINE

CSM is under continuous development and has already progressed through the initiation stage. Multiple projects under the CSM program are running concurrently and are in different lifecycle phases such as design, development, testing, piloting, implementation, and maintenance. Agency personnel reported that the next steps for CSM are to release enhancements for already deployed services. Notable enhancements, such as the Consular Enterprise Audit Services and Modernized Smart Traveler Enrollment Program, were deployed in September 2024 and agency personnel expect to perform continuous development on these enhancements until they are decommissioned at a later date. In January 2025, State noted that the Office of Consular Systems and Technology changed its CSM approach from the all-in-one ConsularOne initiative to implementing a series of separate systems to replace legacy systems. The department added that this is intended to enable the faster delivery of new and updated systems.



Source: GAO analysis. | GAO-25-106908

AGENCY IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Moderate risk				High risk		
Technical risk	Organizational risk	Risk of not implementing	Schedule risk	Information privacy risk	Cost/budget risk	Cybersecurity risk

CHALLENGES IDENTIFIED

Not a challenge			Identified by the agency as a challenge				
Implementation of chosen system development methodology	Oversight	Cost constraints	Organizational alignment and structure	Technical issues	Schedule slippages	Obtaining adequate funding/budget	Workforce issues

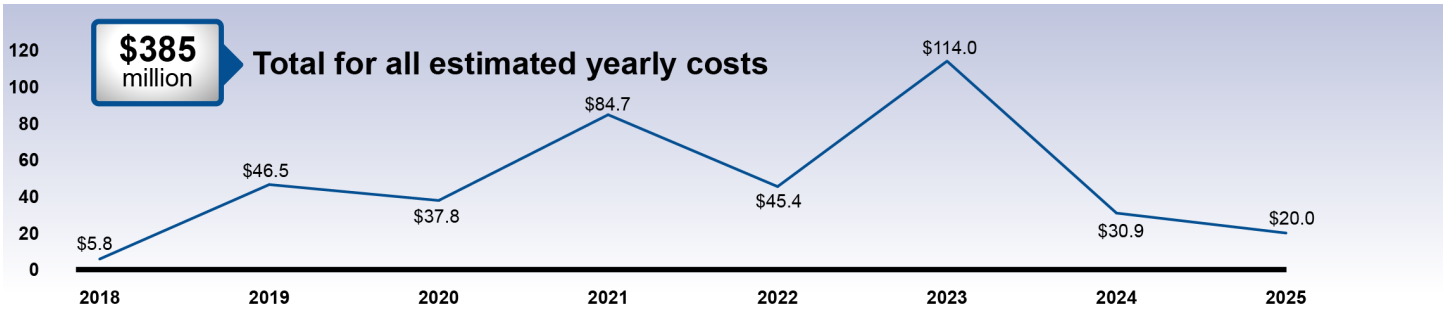
Personnel from State identified various challenges and risk factors associated with the CSM acquisition, ranging from issues with internal IT infrastructure to funding and staffing. For example, officials cited workforce issues such as a chronic staffing shortage of government full-time equivalents and schedule slippages as a result of the complicated technical infrastructure required for new technologies used in the modernization effort. Challenges associated with obtaining adequate funding for the acquisition arise from the fact that the Bureau of Consular Affairs relies on funding primarily from visa and passport fees. Restrictions put in place during the COVID-19 Pandemic drastically reduced the agency's available funding due to a lack of visa and passport demand. Personnel also described information privacy and cybersecurity issues as 'high risk' as the agency works to meet security requirements.

COST AND BUDGET

State does not expect that there will be cost savings with this acquisition.	CSM's obligations equaled approximately 2.25% of State's total fiscal year 2024 IT budget.	Total anticipated life cycle costs: Approximately $385 million over 8 years.	State anticipates that CSM will lower the total operational cost of ownership and complexity compared to the existing environment.

The Chiefs of both the Bureau of Consular Affairs' Office of System and Technology and the Service Strategy & Portfolio Management Division and the Chief of the New Service Design & Development Division are responsible for preparing the budget for the acquisition. The Chief Information Officer of the Bureau of Consular Affairs is responsible for funding the acquisition. State personnel reported that the acquisition was rebaselined in 2018 and has not required rebaselining since. In 2020, State personnel stated that the total anticipated life cycle cost estimate for the acquisition was approximately $617.86 million over 11 years. However, this has since been reduced by about $232 million due to a realignment of investments and development efforts, according to agency officials. Furthermore, State does not anticipate further spending on CSM past fiscal year 2025 and the timeline and cost estimates were reduced accordingly. Though the acquisition is not expected to generate direct cost savings when deployed, agency personnel stated that it is expected to lower the total operational cost of ownership for the system compared to the existing environment.

Actual and estimated expenditures by fiscal year according to agency officials (in millions)



Source: GAO analysis of survey results. | GAO-25-106908

PRIOR WORK

We have previously issued a report related to State's CSM acquisition:

- GAO. *Information Technology: Key Attributes of Essential Federal Mission Critical Acquisitions*. GAO-20-249SP. Washington, D.C.: Sept. 8, 2020.

DEPARTMENT OF TRANSPORTATION | Automatic Dependent Surveillance Broadcast

Sources: Transportation (logo); Old Man Stocker/stock.adobe.com (photo). | GAO-25-106908

The Automatic Dependent Surveillance Broadcast (ADS-B) acquisition is a modernized surveillance technology that provides improved air traffic information for pilots and air traffic controllers. The acquisition is a key component of the Federal Aviation Administration's (FAA) modernization of the nation's air transportation system, known as the Next Generation Air Transportation System (NextGen). ADS-B aims to increase efficiency and safety by improving the condition of America's aviation infrastructure and reducing aviation-related fatalities. FAA has been developing additional ADS-B capabilities since it was deployed in 2014. Most recently, this is part of the ADS-B Baseline Services Future Segments program and the Enhancement program.

KEY INFORMATION

ADS-B will use and store personally identifiable information.	Transportation officials stated that the FAA's Offices of Air Traffic Organization and Acquisition and Business Services are responsible for providing oversight for ADS-B.	ADS-B's baseline was changed in 2011 due to an increase in scope. ADS-B received a new baseline in 2019 to continue services through fiscal year 2020-2025.	Air Traffic Controllers rely on ADS-B as a critical input for tracking and separating air traffic in the National Airspace System. Pilots can use ADS-B surveillance information to enhance their situational awareness of the surrounding airspace.

ACQUISITION BACKGROUND

Acquisition designation: Major acquisition

Type of acquisition: New system with new capabilities

Scope of acquisition: Component/bureau specific for FAA

System users: Approximately 7,000 air transport aircraft staff and 130,000 general aviation and air taxi users. This number is expected to increase to more than 8,000 and 180,000 respective users by 2035

Unique investment identifier: 021-142305975

Total anticipated life cycle costs: Approximately $3.55 billion over 19 years

Development approach: Customized development by agency personnel, contractor-developed, commercial-off-the-shelf, and open-source software development solutions with a mix of Agile and waterfall development methodologies

Project workforce: 10 government full time equivalents and approximately 92 contractor personnel in fiscal year 2024

Federal IT Dashboard risk rating: Moderately low, as of January 2025

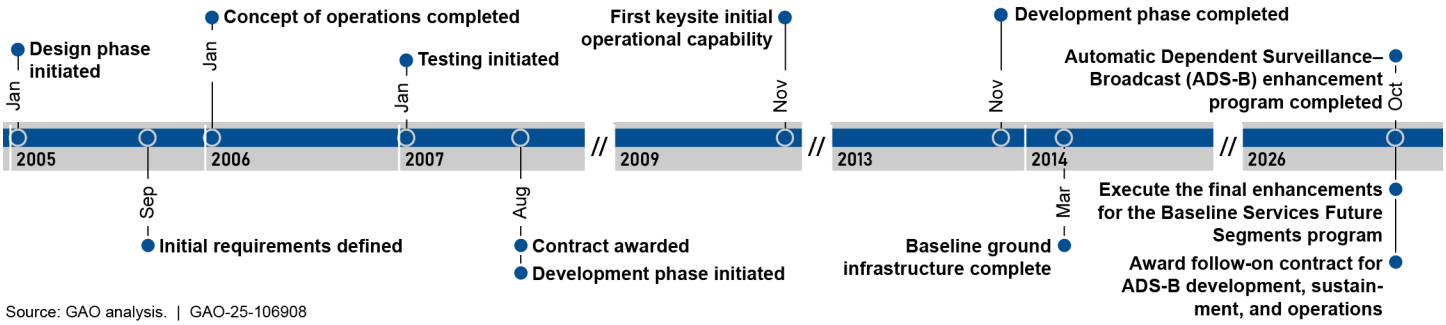
OVERVIEW

Transportation's mission includes ensuring the nation has a safe, efficient, and modern transportation system that improves the quality of life for all American people and communities. As part of this mission, the FAA—a component agency of Transportation—is leading the development of NextGen. NextGen is a complex, long-term initiative that is expected to transition the current ground-based radar air-traffic control system to a system based on satellite navigation, automated position reporting, and digital communications.

ADS-B—a program under one of six NextGen-related program areas—is expected to contribute to FAA's efforts to reduce congestion and provide increased capacity in the National Airspace System, among other benefits. ADS-B is intended to significantly increase efficiency and enhance safety by broadcasting an aircraft's position based on precise signals from the Global Navigation Satellite System—effectively tracking and managing air traffic. Aircraft equipped with ADS-B can receive and process surveillance information using the aircraft's multifunction display. ADS-B equipment also allows air traffic controllers and pilots to locate and identify ground vehicles when they are on runways or taxiways.

CURRENT STATUS AND TIMELINE

ADS-B is in continuous development and is currently performing activities for design, development, testing, implementation, and maintenance. Additional capabilities are being developed during these stages such as enhancements for the Baseline Services Future Segments program and other key acquisition milestones. Within the next two years, the ADS-B team expects to execute the final enhancements for the Baseline Services Future Segments program and other enhancements as well as the awarding of a follow-on contract for ADS-B development, sustainment, and operations by the end of fiscal year 2025.



Source: GAO analysis. | GAO-25-106908

AGENCY IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk	Moderate risk					High risk
Organizational risk	Cybersecurity risk	Technical risk	Information privacy risk	Cost/budget risk	Schedule risk	Risk of not implementing

CHALLENGES IDENTIFIED

Not a challenge				Identified by the agency as a challenge			
Workforce issues	Organizational alignment and structure	Cost constraints	Providing oversight and governance	Obtaining adequate funding/budget	Schedule slippages	Implementation of chosen system development methodology	Technical

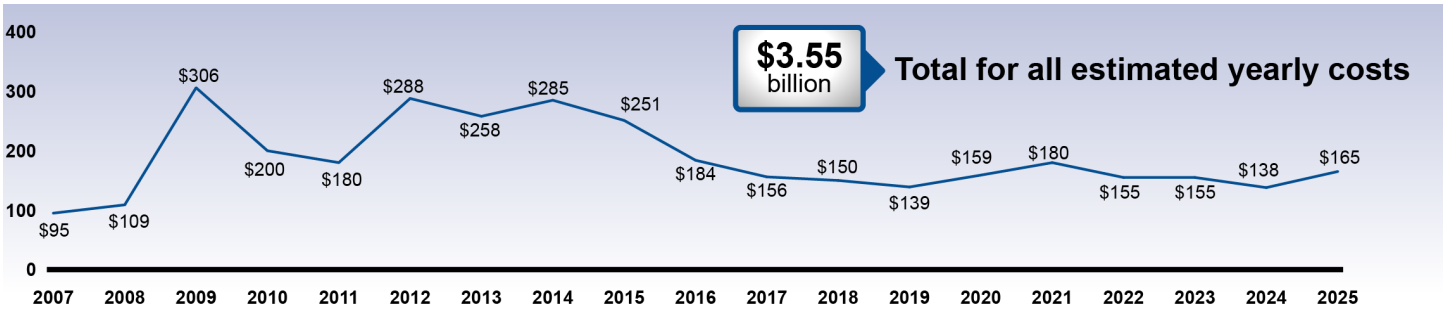
FAA officials reported cybersecurity, technical, information privacy, cost/budget, and schedule as moderate risk factors. The risk of not implementing was identified as a high-risk area since termination of the acquisition would halt work on the FAA's preferred source of information used for surveillance and separation services and severely impact the National Airspace System's operations. Furthermore, obtaining adequate funding/budget, schedule slippages, implementation of chosen system development methodology, and technical issues were identified as challenges. For example, FAA officials noted that insufficient funding in future years could require reductions in the scope of future ADS-B development activities, such as cybersecurity enhancements. Additionally, officials stated that insufficient funding for recurring subscription fees could result in interruptions to ADS-B surveillance capabilities and impacts to air traffic control operations. Further, officials described schedule slippages as a result of delays that impacted contractor performance and technical issues as a result of an insufficient number of users to conduct testing and required conversion from legacy to alternative telecommunication services. Lastly, officials identified challenges with implementing the system development methodology as a result of the use of a service-based contract which requires higher levels of oversight.

COST AND BUDGET

FAA anticipates over $400 million in cost avoidances with ADS-B.	ADS-B obligations equaled 3.63% of Transportation's total fiscal year 2024 IT budget.	Total anticipated life cycle costs: approximately $3.55 billion over 19 years	FAA officials stated that ADS-B implementation activities have already saved an estimated $29 million in cost avoidances.

ADS-B baseline was changed in 2011 due to an increase in scope. ADS-B received a new baseline in 2019 to continue services through fiscal years 2020-2025. FAA officials reported approximately $29 million in cost avoidances from removing legacy airport surveillance radars as part of its Automatic Dependent Surveillance Broadcast acquisition. In addition, the officials anticipated cost avoidances of over $400 million by fiscal year 2035 if remaining candidate radars are removed.

Actual and estimated expenditures by fiscal year according to agency officials (in millions)



Source: GAO analysis of survey results. | GAO-25-106908

PRIOR AND ONGOING WORK

We have previously issued several reports related to Transportation's ADS-B. For example:

- GAO. *Air Traffic Control: FAA Actions Are Urgently Needed to Modernize Aging Systems.* GAO-24-107001. Washington, D.C.: Sept. 23, 2024.
- GAO. *Air Traffic Control Modernization: Program Management Improvements Could Help FAA Address NextGen Delays and Challenges.* GAO-24-105254. Washington, D.C.: Nov. 9, 2023.
- GAO. Information Technology: *Key Attributes of Essential Federal Mission-Critical Acquisitions.* GAO-20-249SP. Washington, D.C.: Sept. 8, 2020.

We also have ongoing work reviewing, among other things, the extent to which FAA and aircraft operators have realized anticipated benefits of ADS-B to manage air traffic.

DEPARTMENT OF TRANSPORTATION | Voice Communications Systems

Sources: Transportation (logo); Gorodenkoff/stock.adobe.com (photo). | GAO-25-106908

The Federal Aviation Administration's (FAA) Voice Communications System (VCS) program is intended to provide safety mission critical air-to-ground and ground-to-ground communications between air traffic controllers, pilots, and other ground personnel. These personnel are responsible for separating, managing, and directing air traffic in the National Airspace System. Executed in a two-phased, four-procurement approach, VCS is intended to replace aging analog voice switching infrastructure at all Air Route Traffic Control Centers as well as some Airport Traffic Control Towers and Terminal Radar Approach Control facilities with a modern and supportable voice over internet protocol enabled system.

KEY INFORMATION

The VCS acquisition program will neither use nor store personally identifiable information.	FAA's Air Traffic Organization Program Management Office is responsible for oversight of VCS.	FAA intends to replace the legacy radio control equipment under the VCS program beginning in 2026 at key sites and finishing in 2035.	FAA terminated the National Airspace System Voice System program, a previous attempt to update aging voice switches, in 2018.

ACQUISITION BACKGROUND

Acquisition designation: Major acquisition

Type of acquisition: Combination of new systems and replacement of legacy systems

Scope of acquisition: FAA

System users: Air traffic control and technical operations professionals, and potentially DOD personnel

Unique investment identifier: 021-996986521

Total anticipated life cycle costs: $2.962 billion over 22 years

Development Approach: Anticipated Agile development using contractor developed, commercial off-the-shelf, and open-source software solutions[57]

Project workforce: Approximately 28 government full-time equivalents and 103 contractor full-time equivalents.

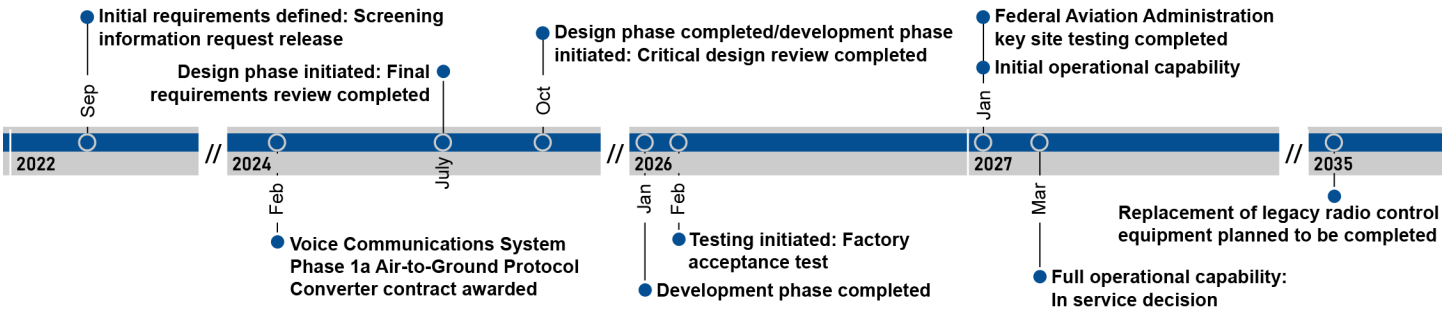
Federal IT Dashboard risk rating: Moderately low, as of January 2025

OVERVIEW

FAA's mission is to provide the world's safest, most efficient aerospace system. As part of its effort to modernize the National Airspace System, the FAA has planned for more than a decade to update the agency's voice communications systems—some more than 30 years old—with a voice over internet protocol solution. These voice communication systems are relied upon by air traffic controllers, pilots, and other ground personnel. FAA initiated the VCS acquisition program to address mission needs and performance gaps unfulfilled by the National Airspace System Voice System program, a previous initiative to update FAA's aging voice switches. According to FAA officials, this includes providing FAA a flexible, network-based voice communication enterprise, addressing radio control equipment obsolescence and end of life issues. It also includes replacing increasingly expensive to maintain legacy voice switches at Air Route Traffic Control Centers, Airport Traffic Control Towers, and Terminal Radar Approach Control. VCS intends to promote sustained operational availability with the latest technology to ensure continued safety-critical communications between air traffic controllers and pilots.

CURRENT STATUS AND TIMELINE

FAA officials stated that, in February 2024, the agency awarded the contract for VCS Phase 1a Air-to-Ground Protocol Converter system. Phase 1a is expected to provide air-to-ground internet protocol to analog interfaces and replace the aging radio control equipment. By summer of 2027, FAA expects Phase 1a procurement to begin deployment. The Phase 1b Ground-to-Ground Protocol Converter system is expected to focus on ground-to-ground internet protocol to analog interfaces. Both phases 1a and 1b are intended to allow a gradual transition of endpoint devices, such as voice switches and radios, from analog to internet protocol technology. Phase 2 is intended to deliver new internet protocol-based voice switch systems to select terminal facilities and all en route facilities. FAA expects Phase 2 contract award in 2027.



Source: GAO analysis. | GAO-25-106908

Note: This figure reflects VCS status as of February 2025.

[57]According to FAA officials, vendors will likely use an Agile development process, however, the system will not be provided to FAA until after test and evaluation.

AGENCY IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk		Moderate risk			High risk	
Organizational risk	Information privacy risk	Technical risk	Cost/budget risk	Schedule risk	Cybersecurity risk	Risk of not implementing

CHALLENGES IDENTIFIED

Not a challenge							
Obtaining adequate funding/budget	Workforce issues	Cost constraints	Schedule slippages	Providing oversight and governance	Technical	Implementation of chosen system development methodology	Organizational alignment and structure

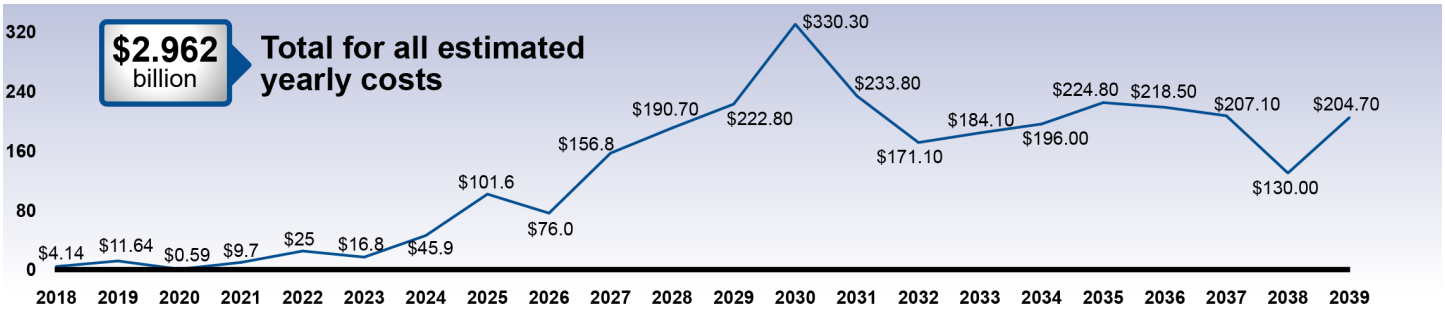
VCS acquisition program officials reported multiple risks associated with the program, including those related to design incompatibility as well as the impacts of other FAA acquisitions on the VCS schedule. For example, if Air Route Traffic Control Centers' console space limitations are not resolved before VCS issues a related contract in approximately the fourth quarter of fiscal year 2026, then potential offerers will be required to make hardware and software design changes to their commercial off-the-shelf products to compete. Furthermore, agency officials reported that the transition from the legacy voice switches to the internet protocol voice switches will not be possible with the current operator console configuration. Further, FAA officials noted a safety risk of not implementing VCS; specifically, that sustaining legacy voice communication systems is becoming increasingly challenging, thus, raising the risk of system outages. Officials added that the Phase 1a Air-to-Ground Protocol Converter vendor is focusing on early testing and software auditing with the intention of reducing potential cost and schedule risks to the program.

COST AND BUDGET

FAA does not expect that there will be cost savings associated with this acquisition.	VCS obligations equaled 1.18% of Transportation's total fiscal year 2024 IT budget.	Total anticipated life cycle costs: $2.962 billion over 22 years.	Transportation anticipates benefits associated with VCS Phase 1a, including simplifying the planned replacement of Voice over Internet Protocol switches in VCS Phase 2.

FAA officials stated that the agency's Office of Budget and Programs is responsible for preparing the budget for and funding the VCS acquisition program. FAA's Fiscal Year 2025 budget request included $18 million for VCS Phase 1a contract management, systems engineering, training development, systems development, and integrated logistics support; $43.9 million for the procurement and installation of equipment as part of Phase 1a deployment; and $10 million to award a new contract for Phase 1b. The VCS program's initial Phase 1a contract does not have operations and maintenance costs, according to FAA officials, and operations and maintenance costs for future VCS program phases have not yet been reported.

Actual and estimated expenditures by fiscal year according to agency officials (in millions)



Source: GAO analysis of survey results. | GAO-25-106908

PRIOR AND ONGOING WORK

We have previously released two reports related to FAA's air traffic control systems:

- GAO. *Air Traffic Control: FAA Actions Are Urgently Needed to Modernize Aging Systems.* GAO-24-107001. Washington, D.C.: Sept. 23, 2024.
- GAO. *Air Traffic Control Modernization: Program Management Improvements Could Help FAA Address NextGen Delays and Challenges*. GAO-24-105254. Washington, D.C.: Nov. 9, 2023.

As of February 2025, we had 10 open IT-related recommendations to FAA pertaining to its air traffic control systems. For example, we recommended that the FAA Administrator should:

- report to Congress on how it is mitigating risks of all unsustainable and critical systems that are identified in the annual operational risk assessments. (GAO-24-107001)
- develop an updated life-cycle cost estimate for NextGen, measure FAA's performance against it, and create a schedule for updating the life-cycle cost estimate regularly. (GAO-24-105254)

We also have ongoing work related to FAA's efforts to secure avionics against cyber-based threats.

DEPARTMENT OF THE TREASURY | Business Master File Modernization

Sources: Treasury (logo); M+Isolation+Photo/stock.adobe.com (photo). | GAO-25-106908

The Business Master File (BMF) Modernization acquisition is designed to modernize existing legacy systems at the Department of the Treasury's Internal Revenue Service (IRS) for the current Business Master File Tax Processing system, which supports tax processing for businesses and exempt organizations alike. The project was initiated in March 2024. Agency officials stated that the goal of the modernization effort is to enhance the taxpayer experience by upgrading the IRS' infrastructure to support enhanced customer support and tax processing services. To do so, the agency is upgrading outdated IT infrastructure and legacy systems to support the modernization effort. IRS has reported that the system is projected to reach full operational capability in fiscal year 2029.

KEY INFORMATION

BMF Modernization will use but not store personally identifiable information.	Related key GAO high-risk area: Improving IT Acquisitions and Management. (GAO-25-107852)	The IRS' Office of Chief Procurement Officer and Office of Chief Information Officer are responsible for providing oversight for the acquisition.	The BMF Modernization will support objectives in the IRS' Inflation Reduction Act Strategic Operating Plan.

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Modernization of legacy system

Scope of acquisition: Agency-wide across the Department of the Treasury and the IRS

System users: Supports tax processing for corporations and other businesses

Unique investment identifier: BMF is a subcomponent of the Tax Account Management investment (015-000200465)

Total anticipated life cycle costs: $561 million over 5 years

Development approach: Agile software development with contractor-developed solutions

Project workforce: Approximately 30 government full-time equivalents and 300 contractor personnel

Federal IT Dashboard risk rating: BMF does not have a CIO risk rating. However, the Tax Account Management investment has a rating of low, as of January 2025

OVERVIEW

The goal of Treasury and the IRS is to provide America's taxpayers with top quality service by helping them understand and meet their tax responsibilities while enforcing the law. Both Treasury and the IRS are working together to reach this goal by developing new technology to modernize the taxpayer experience. The BMF Modernization is intended support enhanced features for customer service and tax processing for business tax processing such as real-time digital taxpayer interactions, agile responses to legislative changes, rapid access to customer data, and fraud detection services. Agency officials have reported that the system will use but not store personally identifiable information. As a result, the BMF Modernization is expected to include improved security and privacy capabilities to address future threats to sensitive taxpayer information.

CURRENT STATUS AND TIMELINE

Agency officials reported that BMF Modernization is being developed with an Agile methodology and there are multiple work streams from three different vendors working concurrently. The contract was initiated in March 2024 and the design phase was initiated in April 2024. Furthermore, the acquisition is currently in multiple stages such as initiation, defining initial requirements, design, development, and piloting. The projected next steps for the acquisition are to develop and deliver phase 1 into production which is expected to result in the completion of the overall architecture and design. Officials project that the acquisition will reach full operational capability in fiscal year 2029.

Source: GAO analysis. | GAO-25-106908

AGENCY IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk					Moderate risk	High risk
Organizational risk	Cybersecurity risk	Information privacy risk	Cost/budget risk	Schedule risk	Technical risk	Risk of not implementing

CHALLENGES IDENTIFIED

Not a challenge							Identified by the agency as a challenge
Implementation of chosen system development methodology	Providing oversight and governance	Obtaining adequate funding/budget	Schedule slippages	Workforce issues	Organizational alignment and structure	Cost constraints	Technical

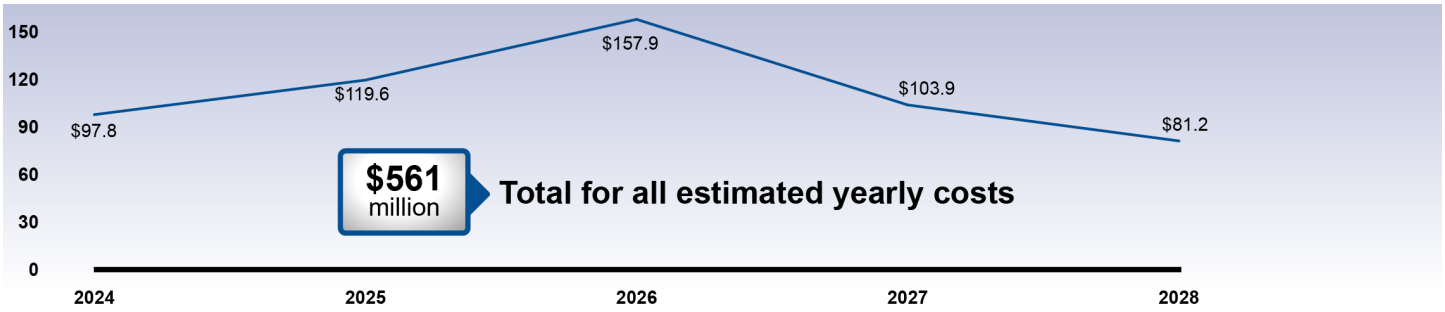
IRS officials cited the risk of not implementing as a high-risk factor and technical risk as a moderate risk factor. Additionally, the agency identified technical issues such as obtaining approval for commercial-off-the-shelf tools as a challenge to the acquisition's development. Officials reported that both the risk of not implementing and technical challenges were particularly important to consider during the development of the BMF Modernization as the IRS would have to rely on outdated systems, some of which were developed in the 1960s, if the modernization does not occur. Agency officials stated that they plan to employ various methods to mitigate these issues such as tracking key performance indicators and using performance-based metrics to monitor performance. Officials added that they also plan to work with contractors to ensure that defined performance standards are set and desired outcomes and requirements are discussed.

COST AND BUDGET

The IRS does not expect that there will be cost savings with this acquisition.	BMF is a subcomponent of the Tax Account Management investment. This investment's obligations equaled 6.25% of Treasury's total fiscal year 2024 IT budget.	Total anticipated life cycle costs: $561 million over 5 years.	IRS officials anticipate that the BMF Modernization will undergo rebaselining in late 2024.

The BMF Modernization Program Management Office is responsible for preparing this acquisition's budget. The IRS' Office of Chief Procurement Officer and Office of Chief Information Officer is responsible for providing oversight for the acquisition. The BMF Modernization is expected to undergo rebaselining in late 2024 as a result of collaboration with different vendors and a subsequent change in timelines. The agency does not expect cost savings once the acquisition is deployed. However, the agency expects to update the overall infrastructure and improve access to data for enhanced customer service, compliance, and fraud detection services.

Actual and estimated expenditures by fiscal year according to agency officials (in millions)



Source: GAO analysis of survey results. | GAO-25-106908

Note: Yearly expenditures may not add up to total due to rounding

PRIOR AND ONGOING WORK

We have previously issued several reports related to IRS's BMF. 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.
- GAO. *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*. GAO-23-106203. Washington, D.C.: Apr. 20, 2023.
- GAO. *Information Technology: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements.* GAO-23-104719. Washington, D.C.: Jan. 12, 2023.

From these reports, we have 12 open IT-related recommendations related to BMF Modernization. For example, we recommended that the Commissioner of the IRS should:

- Include information including a history of programs' cost and schedule goals and showing how the quarterly cost and schedule performance aligns with fiscal year and overall goals for the programs in its quarterly reports to Congress. (GAO-24-106566)
- Ensure that IRS establishes time frames for addressing the disposition of legacy systems for the Enterprise Case Management modernization initiative and follow through to document a complete modernization plan. (GAO-23-104719)

We also have ongoing work to evaluate IRS's progress in implementing its modernization program for fiscal year 2024, which includes BMF Modernization.

DEPARTMENT OF THE TREASURY | Individual Master File Modernization

Sources: Department of Treasury (logo); Miha Creative/stock.adobe.com (photo). | GAO-25-106908

The Internal Revenue Service's (IRS) Individual Master File (IMF) Modernization is intended modernize the technology environment that enables the IRS to process individual tax returns each year. The initiative aims to widen the scope of work that began with the Customer Account Data Engine (CADE) 2 program. CADE 2 was initially intended to replace the IMF, but the scope of CADE 2 was changed in 2019 to modernize the most complex parts of IMF. IMF Modernization is intended to streamline and simplify digital taxpayer interactions; make the IMF more agile to legislative changes; and enable faster access to data for enhanced customer service, compliance, and fraud detection services. IRS is aiming to retiring the IMF by the end of 2028.

KEY INFORMATION

The modernized IMF will both use and store personally identifiable information.	Related key GAO high-risk area: Improving IT Acquisitions and Management. (GAO-25-107852)	IMF Modernization efforts have rebaselined several times from 2016 to 2020 due to hiring freezes, competing staffing needs, and scope changes, among other issues.	IMF Modernization widens the aperture of the work started by the CADE 2 program initiated in 2009.

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Replacement of legacy system

Scope of acquisition: IRS, with information distribution to external agencies, such as the Social Security Administration

System users: Supports 200 million taxpayers per year

Unique investment identifier: IMF is a subcomponent of the Tax Account Management investment (015-000200465)

Total anticipated life cycle costs: $2.93 billion over 17 years

Development approach: Waterfall and Agile software development using multiple approaches, including contractor-developed, customized by agency personnel, commercial off-the-shelf, and open-source software solutions

Project workforce: Approximately 209 government full-time equivalents and 791 full-time equivalent contractor personnel

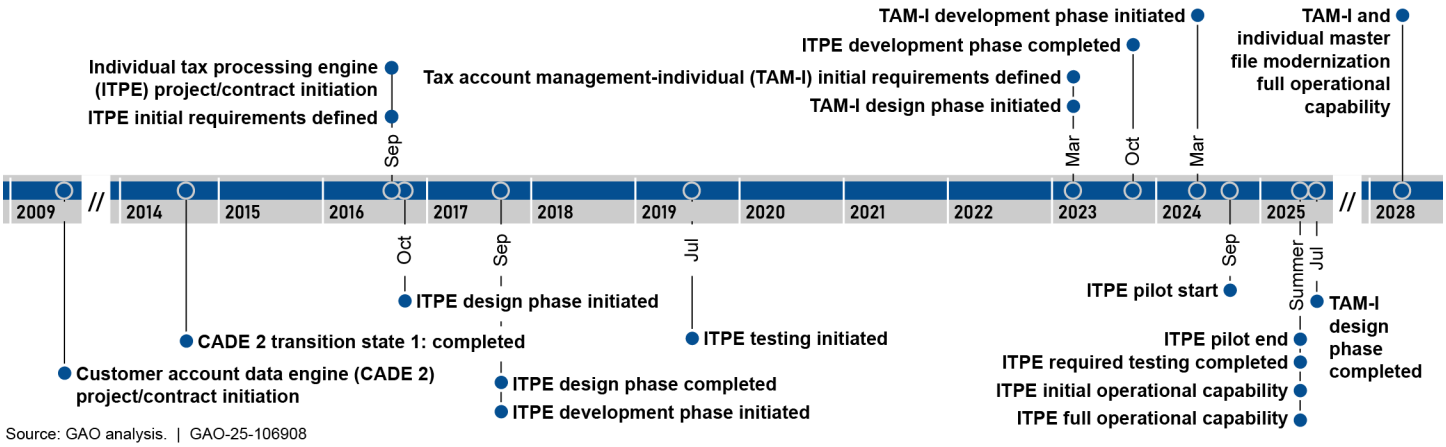
Federal IT Dashboard risk rating: IMF does not have a CIO risk rating. However, the Tax Account Management investment has a rating of low, as of January 2025

OVERVIEW

The IMF, which has been used since the 1960s, is IRS's key system for processing individual taxpayer account data. Over 250 IRS information system applications and processes depend on the downstream output from this data source. The agency established the IMF Modernization acquisition to address numerous mission-based and operational challenges of maintaining the legacy IMF, such as a shrinking number of subject matter experts knowledgeable in its programming language, and incomplete data retention due to architectural constraints. Further, the IMF Modernization creates a foundation for the retirement of the legacy IMF and provide a more flexible architecture for future enhancements to improve customer service, compliance, and the taxpayer experience, among other things.

CURRENT STATUS AND TIMELINE

Within the IMF Modernization initiative, the CADE 2 program is being implemented in three transition states to reduce risk and incrementally deliver the initiative. In 2014, the program completed the first transition state after migrating all IMF data to the CADE 2 relational database. The remaining two transition states include the Individual Tax Processing Engine (ITPE) and Tax Account Management-Individual projects (TAM-I). These transition states are expected to convert core IMF processing runs from Assembler Language Code to Java and modernize IRS's receipt, processing, and closure of the accounting cycle for individual taxpayer accounts. As of September 2024, according to IRS officials, the ITPE project was in the piloting phase.



Source: GAO analysis. | GAO-25-106908

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Moderate risk	High risk					
Cybersecurity risk	Organizational risk	Information privacy risk	Technical risk	Cost/budget risk	Schedule risk	Risk of not implementing

CHALLENGES IDENTIFIED

Not a challenge				Identified by the agency as a challenge			
Cost constraints	Providing oversight and governance	Implementation of chosen system development methodology	Organizational alignment and structure	Obtaining adequate funding/budget	Workforce issues	Schedule slippages	Technical

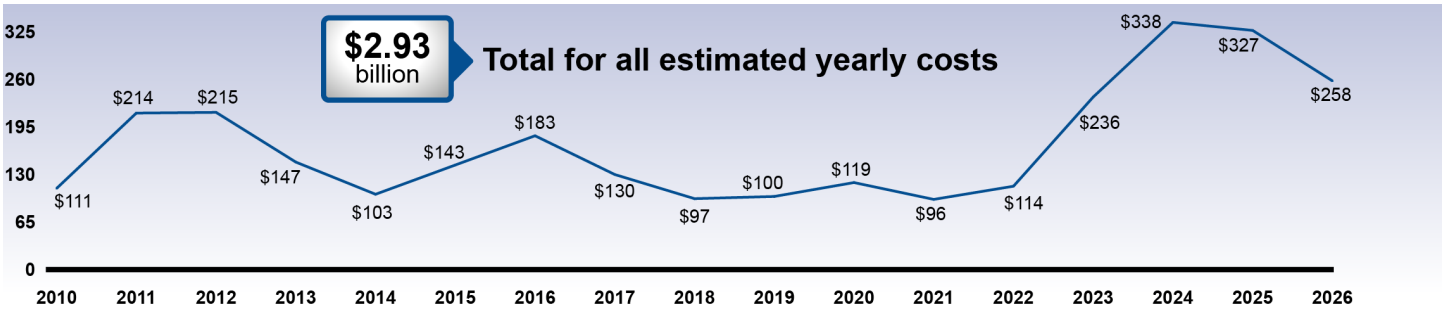
IRS officials noted several risks and challenges tied to IMF Modernization efforts. For example, IRS mentioned risks associated with securing contracts for required resources that are vital to delivering program goals. IRS also described workforce and technical challenges tied to the age of the IMF, including fewer developers being available to support its Assembler Language Code software and a complex ecosystem of approximately 2 million lines of code that are continuously updated for annual tax law changes and legislative mandates. According to IRS officials, as of May 2023, it had completed one hundred percent of the code conversion needed to retire IMF's legacy posting, settlement, and analysis code and was testing new code as part of CADE 2's Individual Tax Processing Engine program.

COST AND BUDGET

IRS officials stated that they did not know whether there would be cost savings associated with IMF Modernization.	IMF is a subcomponent of the Tax Account Management investment. This investment's obligations equaled 6.25% of the Treasury's total fiscal year 2024 IT budget.	Total anticipated life cycle costs: $2.93 billion over 17 years.	Performance measures for IMF Modernization include those related to refund timeliness and data validation.

The IMF Modernization Program Management Office is responsible for preparing this acquisition's budget. IRS's Transformation & Strategy Office, Office of the Chief Information Officer, and Financial Management Services division are tasked with allocating the funding for the effort. IRS officials cited obtaining adequate funding and budget as a challenge and noted that some IMF Modernization efforts were paused between May 2022 and November 2022 due to this challenge. Officials also noted that achievement of some of the effort's target milestones, such as fiscal year 2028 completion, are subject to shift based on factors that include funding and contract support.

Actual and estimated expenditures by fiscal year according to agency officials (in millions)



Source: GAO analysis of survey results. | GAO-25-106908

Note: Yearly expenditures may not add up to total due to rounding

PRIOR AND ONGOING WORK:

We have previously issued several reports related to IMF Modernization initiatives, including CADE 2. Examples include:

- GAO, *Information Technology: IRS Needs to Complete Planning and Improve Reporting for Its Modernization Programs*, GAO-24-106566, Washington, D.C.: Mar. 19, 2024.
- GAO, *Information Technology: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements*, GAO-23-104719, Washington, D.C.: Jan. 12, 2023.
- GAO, *Information Technology: Cost and Schedule Performance of Selected IRS Investments*, GAO-22-104387, Washington, D.C.: Oct. 19, 2021.
- GAO, *Information Technology: Key Attributes of Essential Federal Mission Critical Acquisitions*, GAO-20-249SP, Washington, D.C.: Sept. 8, 2020.

As of February 2025, we had 12 open recommendations to IRS related to IMF Modernization. For example, we recommended that the Commissioner of the IRS should include information including a history of programs' cost and schedule goals and showing how the quarterly cost and schedule performance aligns with fiscal year and overall goals for the programs in its quarterly reports to Congress. (GAO-24-106566)

We also have ongoing work to evaluate IRS's progress in implementing its modernization program for fiscal year 2024, which includes IMF Modernization.

DEPARTMENT OF VETERANS AFFAIRS | Electronic Health Record Modernization

Sources: VA (logo); C Malambo/peopleimages.com/stock.adobe.com (photo). | GAO-25-106908

The Department of Veterans Affairs' (VA) Electronic Health Record Modernization (EHRM) Integration Office aims to replace the more than 30-year-old Veterans Health Information Systems and Technology Architecture (VistA) Computerized Patient Record System with a commercial off-the-shelf EHR solution being deployed by the Department of Defense (DOD). The modernized system—known as the Federal EHR system—is intended to provide a single, accurate, lifetime health record for veterans to improve standardization of health care delivery, patient care quality, safety, and interoperability between VA and DOD as well as with the rest of the American health care system. Further, a goal of this effort is to provide a modern suite of technologies to empower VA staff and clinicians as they care for veterans.

KEY INFORMATION

The Federal EHR system will both use and store personally identifiable information.	Related key GAO high-risk area: Managing Risks and Improving VA Health Care. (GAO-23-106203)	VA's EHRM Integration Office began an EHRM program reset in April 2023 to, among other things, address issues experienced by clinicians and end users.	As of June 2024, agency personnel stated that the Federal EHR system is now in use at six VA medical centers, 25 associated clinics, and 104 remote service sites.

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Replacement of legacy system

Scope of acquisition: Agency-wide

System users: Approximately 400,000 VA employees serving more than 9 million veterans upon full deployment.

Unique investment identifier: 029-555555305

Total anticipated life cycle costs: $16.14 billion over 10 years. However, in 2022, the Institute for Defense Analyses independently determined that the 28-year life cycle costs for the program were $49.8 billion. As of February 2025, VA was not able to provide a time frame for when it would update the program life cycle cost estimate.

Development approach: Agile implementation of a commercial off-the-shelf solution with customized capability

Project workforce: 242 full-time equivalent government employees and over 800 contractor personnel

Federal IT Dashboard risk rating: Medium, as of February 2025

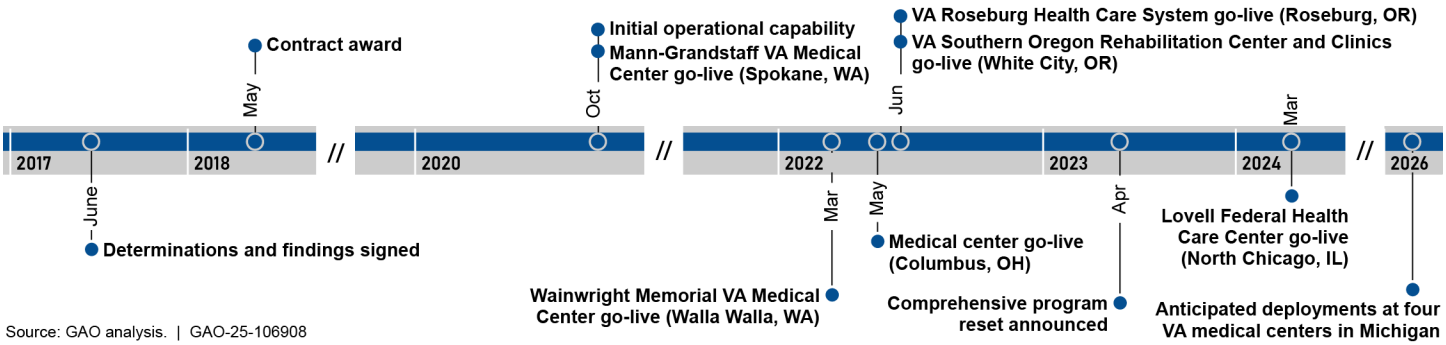
OVERVIEW

VA's mission is to care for those who have served in our nation's military and for their families, caregivers, and survivors. In service of this mission, the Veterans Health Administration operates one of the nation's largest and most complex medical organizations. The health care system features 1,380 facilities—including 170 VA medical centers—that serve over 9 million enrolled veterans.

In June 2017, VA initiated the EHRM program. The program is intended to replace the legacy VistA Computerized Patient Record System, which requires modernization to keep pace with advancements in health IT and cybersecurity, with the same Oracle Cerner EHR system DOD acquired (known as Military Health System GENESIS).

CURRENT STATUS AND TIMELINE

VA announced a program reset in April 2023 for EHRM. According to VA officials, it was intended to address issues experienced by clinicians and end users at live sites, position VA for successful future deployments, and prepare for implementation at the joint VA/DOD Lovell Federal Health Care Center in North Chicago, Illinois, in March 2024. In December 2024, VA announced that it was beginning early-stage planning for restarting deployments to four sites in Michigan in mid-2026. As of February 2025, VA did not have a deployment schedule for the other approximately 160 VA medical centers and associated clinics. The department noted that it is planning to develop additional deployment schedules after the restart of deployment activities in Michigan.



Source: GAO analysis. | GAO-25-106908

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Moderate risk			High risk			
Technical risk	Schedule risk	Risk of not implementing	Organizational risk	Cybersecurity risk	Information privacy risk	Cost/budget risk

CHALLENGES IDENTIFIED

Not a challenge						Identified by the agency as a challenge	
Obtaining adequate funding/budget	Cost constraints	Providing oversight and governance	Technical	Implementation of chosen system development methodology	Organizational alignment and structure	Workforce issues	Schedule Slippages

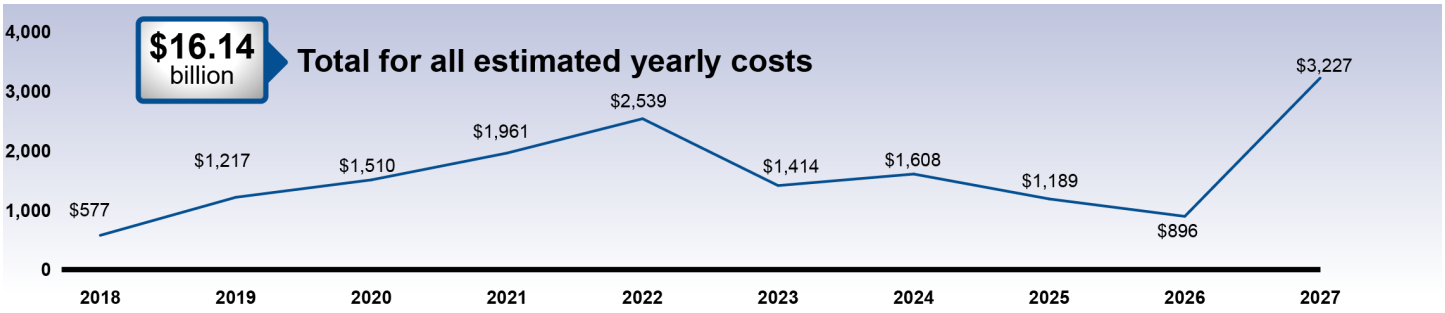
VA noted risks, issues, and challenges facing EHRM that ranged from cost and performance to clinical care quality. For example, schedule risks include testing workflows, the implementation of provisioning tools needed to reduce manual processes, and funding availability for training purposes. Technical risks include the inability to maintain acceptable system performance at EHRM sites. However, VA notes that the core federal EHR system has increasingly stabilized since the beginning of 2023, resulting in significant improvements to the user experience. Challenges cited by VA included workforce issues stemming from final approval of the EHRM Integration Office organizational chart as well as schedule slippages due to ongoing reset activities.

COST AND BUDGET

VA officials indicated that cost savings associated with EHRM would be analyzed after the program reset period.	Total anticipated life cycle costs: $16.14 billion over 10 years. However, VA plans to update this estimate, but did not have a time frame for completion.	VA anticipates its program restart assessment will rely on factors such as improved productivity at current EHRM sites.

The VA EHRM Integration Office and Office of Management are responsible for preparing the acquisition's budget, while the Office of the Deputy Secretary administers appropriated funds. VA officials stated that the EHRM lifecycle cost estimate was under review during the program reset and a revised version would be provided at its conclusion. VA requested $894 million for EHRM in fiscal year 2025—47 percent less than in the 2024 President's Budget—to support reset activities, sustainment of the six sites and 25 clinics currently using new Federal EHR system, and infrastructure readiness. VA did not know whether EHRM would realize cost savings upon full deployment, but the agency planned to analyze possible cost savings after the program reset.

Actual and estimated obligations by fiscal year according to agency officials (in millions)



Source: GAO analysis of survey results. | GAO-25-106908

Note: This total reflects VA's 2019 estimate. However, in 2022, the Institute for Defense Analyses independently determined that the 28-year life cycle costs for the program were $49.8 billion. As of February 2025, VA did not have a time frame for updating the program estimate. In addition, this graph only includes expenditures for VA EHRM appropriation; it does not include costs under the Veterans Health Administration or Office of Information and Technology appropriations. Actual expenditures through fiscal year 2024. Yearly expenditures may not add up to total due to rounding.

PRIOR AND ONGOING WORK

We have previously testified and issued several reports related to VA's EHRM. Examples include:

- GAO. *Electronic Health Record Modernization: VA Is Making Incremental Improvements but Much More Remains to Be Done*. GAO-25-108091. Washington, D.C.: Feb. 24, 2025.
- GAO. *Veterans Affairs: Action Needed to Address Continuing IT Management Challenges*. GAO-25-107963. Washington, D.C.: Dec. 12, 2024.
- GAO. *Electronic Health Records: VA Needs to Address Management Challenges with New System*. GAO-23-106731. Washington, D.C.: May 18, 2023.
- GAO. *Electronic Health Records: VA Needs to Address Data Management Challenges for New System*. GAO-22-103718. Washington, D.C.: Feb. 1, 2022.

As of February 2025, we had 14 open IT-related recommendations related to VA's EHRM. For example, we recommended that the Secretary of Veterans Affairs should ensure that VA documents a VA-specific change management strategy to formalize its approach to drive user adoption (GAO-23-106731).

We have ongoing work looking at the extent to which VA has made progress toward improving its new Federal EHR system at the initial deployment sites and the privacy of veterans' health information in systems that are part of the EHRM program, among other things.

ENVIRONMENTAL PROTECTION AGENCY | Integrated Compliance Information System Modernization

Sources: EPA (logo); Ratchapon/stock.adobe.com (photo). | GAO-25-106908

A crucial part of the Environmental Protection Agency's (EPA) mission is to protect human health and the environment through the development and enforcement of environmental regulations. The purpose of the Integrated Compliance Information System (ICIS) Modernization is to meet EPA's evolving enforcement and compliance business needs by integrating information into a single data system for use by EPA's Office of Enforcement and Compliance Assurance. This acquisition is expected to modernize the ICIS legacy system. The project/contract initiation for the acquisition occurred in September 2023 and the modernized system is projected to reach full operational capability in early 2029.

KEY INFORMATION

The new ICIS system will neither use nor store personally identifiable information.	Related key GAO high-risk areas: The U.S. Government's Environmental Liability and Transforming EPA's Process for Assessing and Controlling Toxic Chemicals. (GAO-23-106203)	EPA's Office of Enforcement and Compliance Assurance and Office of Mission Support are responsible for providing oversight for the acquisition's development.	ICIS Modernization is intended to track compliance with clean air and clean water regulations and permits.

ACQUISITION BACKGROUND

Acquisition designation: Major acquisition

Type of acquisition: Modernization of legacy system.

Scope of acquisition: Agency-wide.

System users: ICIS has approximately 3,000 active users and is expected to include the processing of data from roughly 100,000 users.

Unique investment identifier: 020-000015010

Total anticipated life cycle costs: $41.8 million over seven years

Development approach: Customized development by agency personnel, contractor-developed, commercial-off-the-shelf, and open-source solutions following Agile and waterfall methodologies.

Project workforce: Approximately two government full time equivalents and eight contractor personnel.

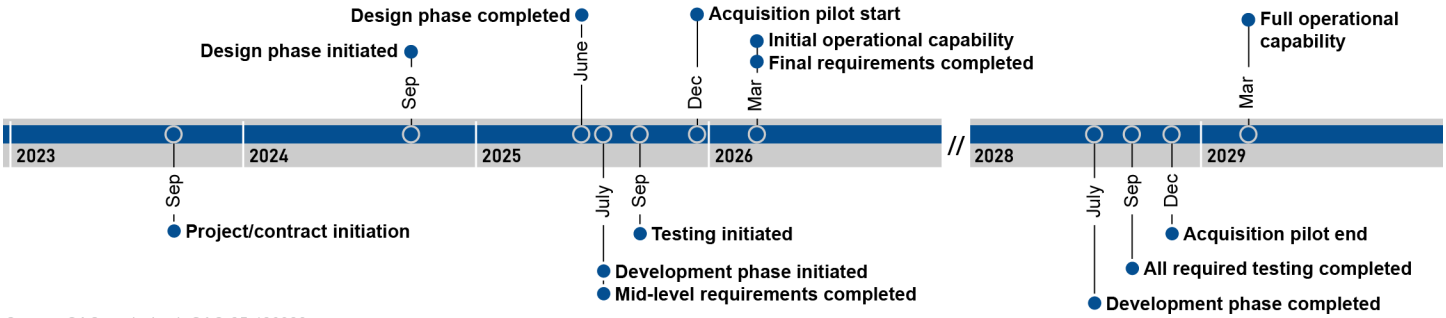
Federal IT Dashboard risk rating: Medium, as of January 2025

OVERVIEW

Agency officials stated that the ICIS Modernization is intended to help agency personnel fulfill EPA's mission by providing the agency and co-regulators more timely, complete, accurate, and nationally consistent set of regulatory, compliance, and enforcement data. Furthermore, EPA relies on its largest mission-critical data system, the ICIS legacy system, to track key compliance data related to permitting and the collection of detailed monitoring information. ICIS manages information for clean water permitting in addition to managing many other sources of environmental compliance information. The modernization of ICIS is expected to provide EPA, states, and local agencies with enhanced capabilities to make better decisions to protect public health and the environment. It is also expected to provide an improved ability to aggregate and analyze compliance and enforcement data. Additionally, the modernization is intended to allow the EPA to use updated technology to mitigate issues concerning the increasing costs of further development and maintenance for the current legacy system.

CURRENT STATUS AND TIMELINE

The ICIS Modernization is currently defining the initial requirements of the acquisiton's development. The code and user experience work follows an Agile methodology to better enable a dynamic development environment, while data storage and policy requirements follow a waterfall methodology so that these areas follow a more sequential progression. Agency officials stated that they anticipate that the agency will complete the high-level system design, analysis of alternatives, and the user requirements within the next year. The acquisition is currently projected to reach full operational capability in early 2029.



Source: GAO analysis. | GAO-25-106908

AGENCY IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

No risk	Moderate risk					High risk
Technical risk	Cybersecurity risk	Schedule risk	Organizational risk	Information privacy risk	Risk of not implementing	Cost/budget risk

CHALLENGES IDENTIFIED

Not a challenge		Identified by the agency as a challenge					
Implementation of chosen system development methodology	Technical	Cost constraints	Providing oversight and governance	Schedule slippages	Organizational alignment and structure	Obtaining adequate funding/budget	Workforce issues

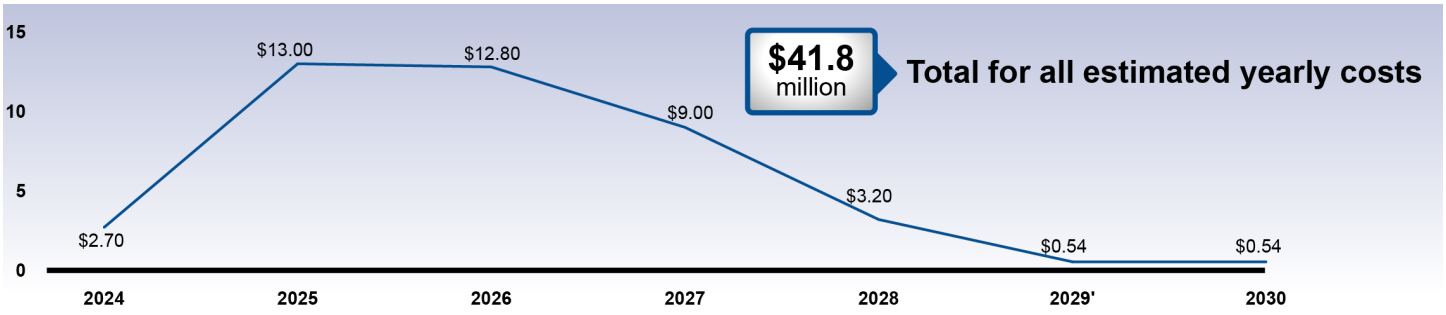
EPA officials reported cybersecurity risk, schedule risk, organizational risk, information privacy risk, and the risk of not implementing as posing a moderate risk to the acquisition's development, while cost/budget risk was designated as a high risk. In addition to these risks, officials cited workforce issues, obtaining adequate funding/budget, organizational alignment and structure, and providing oversight and governance as challenges for the acquisition's development. Officials cited specific examples of these challenges, such as receiving less funding than needed for the modernization, lack of full-time staff working on the system (due to many being temporary staff), schedule slippages due to internal factors (e.g., administrative delays in awarding contracts and onboarding contractors). Officials also cited external factors (e.g., rework needed to initial deliverables from contractors) and the limited history of successful cross-office IT projects at the agency as challenges.

COST AND BUDGET

EPA anticipates reduced costs and cost savings with the deployment of ICIS but has not yet determined the amount.	ICIS Modernization obligations equaled 8.78% of EPA's total fiscal year 2024 IT budget.	Total anticipated life cycle costs: $41.8 million over seven years.	EPA's Office of Enforcement and Compliance Assurance is responsible for preparing the budget for the acquisition's development.

EPA officials stated that a core team within the Office of Enforcement and Compliance Assurance is responsible for preparing the budget for the acquisition and often works with personnel from the Office of Mission Support. The Office of Enforcement and Compliance Assurance and the Office of Mission Support are also responsible for oversight of the acquisition's development. The agency anticipates that changing data collection forms and deploying business rules, such as data validation, will no longer require code changes and redeployments, which will both reduce costs and generate cost savings as a result of the acquisition. EPA officials anticipate a refined life cycle cost estimate as a result of an analysis of alternatives process in late fiscal year 2025 or early 2026.

Actual and estimated expenditures by fiscal year according to agency officials (in millions)



Source: GAO analysis of survey results. | GAO-25-106908

PRIOR WORK

We have previously issued reports related to EPA's ICIS Modernization. For example:

- GAO. *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*. GAO-23-106203. Washington, D.C.: Apr. 20, 2023.
- GAO. *Clean Water Act: EPA Needs to Better Assess and Disclose Quality of Compliance and Enforcement Data.* GAO-21-290. Washington, D.C.: July 12, 2021.
- GAO. *Environmental Protection: Additional Action Needed to Improve EPA Data on Informal Enforcement and Compliance Assistance Activities.* GAO-20-95. Washington, D.C.: Jan. 31, 2020.
- GAO. *Environmental Protection: Action Needed to Ensure EPA's Enforcement and Compliance Activities Support Its Strategic Goals.* GAO-21-82. Washington, D.C.: Dec. 9, 2020.

SMALL BUSINESS ADMINISTRATION | MySBA Platform

Sources: Small Business Association (logo); VAKSMANV/stock.adobe.com (photo). | GAO-25-106908

The Small Business Administration (SBA) is developing the MySBA Platform to help streamline access to SBA programs for small business owners and enable the agency to better serve its customers. The purpose of the acquisition is to implement new technologies, including customer relationship management capabilities, to serve as the foundation for all customer-facing SBA programs. Officials anticipate that these efforts will improve the customer experience while creating operational and cost efficiencies. The project/contract initiation for the MySBA Platform occurred in July 2023 and full operational capability was achieved in January 2025; however, development work is projected to continue through 2025 and 2026 as it expands across the agency.

KEY INFORMATION

The MySBA Platform will both use and store personally identifiable information.	Related key GAO high-risk area: Emergency Loans for Small Businesses. (GAO-23-106203)	The MySBA Platform is intended to centralize customer data sources across the agency to modernize how customer interactions are tracked.	Personnel from the Office of the Chief Information Officer and the Office of the Administrator are responsible for providing oversight for the MySBA Platform.

ACQUISITION BACKGROUND

Acquisition designation: Major acquisition

Type of acquisition: Modernization of legacy system

Scope of acquisition: Agency-wide

System users: The customer relationship management portion of the MySBA Platform is expected to be available to 650 agency personnel. The customer portal is expected to be available for all small businesses/disaster survivors who need to use the system to receive SBA support.

Unique investment identifier: 028-000008012

Total anticipated life cycle costs: $43 million over 5 years.

Development approach: Contractor-developed, commercial-off-the-shelf, and open-source software solutions following an Agile development methodology.

Project workforce: 13 government full-time equivalents and 36 contractor personnel.

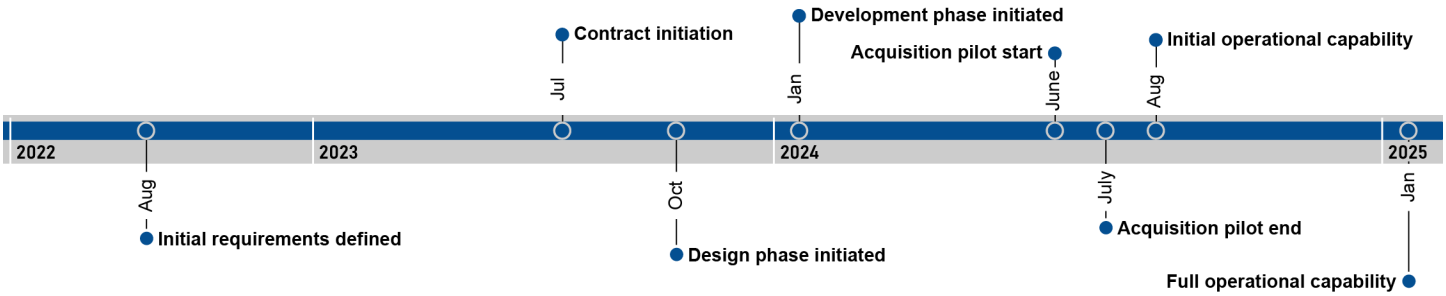
Federal IT Dashboard risk rating: Medium, as of August 2024

OVERVIEW

The MySBA Platform is intended to deliver an enterprise customer relationship management tool and customer portal with single sign-on technology, among other features. The acquisition is expected to further key areas of the agency's mission by offering a variety of enhanced features for customers and agency personnel alike. Among these are streamlining access to SBA programs for small business owners by giving them access to a dedicated MySBA portal, protected by single sign-on authentication, which contains all relevant business information and documents. Agency personnel are also expected to have access to improved customer relationship management functionality and can leverage a new shared services model for customer service and application processing to improve operational efficiency. Officials have reported that, if the MySBA Platform is not properly established due to a lack of engagement between SBA offices and personnel or inadequate resources, then the agency will fall short in its ability to meet its customer experience obligations.

CURRENT STATUS AND TIMELINE

Agency officials reported that the MySBA Platform is currenty in the development phase. Officials added that initial requirements were defined in August 2022 and project/contract initiation occurred in July 2023. The acquisition is in continous development and following an Agile methodology. Officials anticipate that the MySBA Platform will reach key development milestones, such as two releases of pilot versions, before the team moves to initial operational capability in August 2024. The MySBA Platform achieved full operational capability in January 2025, with continued development planned for 2025 and 2026, as the platform scales across the agency.



Source: GAO analysis. | GAO-25-106908

AGENCY IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Moderate risk				High risk		
Risk of not implementing	Organizational risk	Cost/budget risk	Schedule risk	Technical risk	Information privacy risk	Cybersecurity risk

CHALLENGES IDENTIFIED

Not a challenge					Identified by the agency as a challenge		
Implementation of chosen system development methodology	Providing oversight and governance	Cost constraints	Obtaining adequate funding/budget	Workforce issues	Organizational alignment and structure	Schedule slippages	Technical

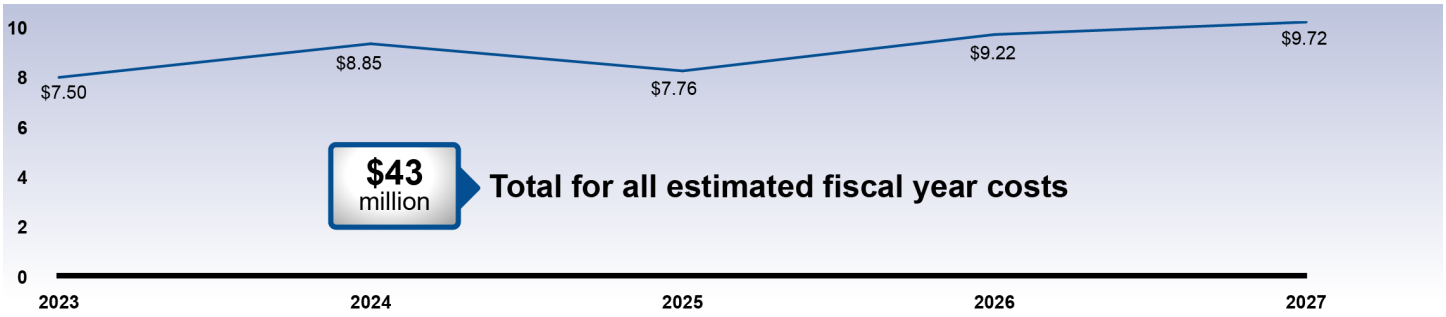
Agency personnel identified various risks and challenges that may impede the development of the acquisition. SBA officials specifically designated technical risk, information privacy risk, and cybersecurity risk as three high-risk areas. Furthermore, the risk of not implementing, organizational risk, cost/budget risk, and schedule risk are designated as moderate risks to the MySBA Platform's development. SBA personnel also identified the areas of organizational alignment and structure, schedule slippages, and technical requirements as three challenges the development faces. SBA officials added that these challenges stem from contract disputes which have led to schedule slippages, technical challenges, and risks due to issues with identifying a strategy to integrate data across the agency and maintaining organizational alignment since it is a cross-agency platform. SBA officials noted that they have established a project charter, leadership board, and staffing model to implement the acquisition while mitigating challenges related to organizational alignment and structure.

COST AND BUDGET

SBA anticipates cost savings after the full deployment of MySBA but has not yet determined the expected amount.	MySBA obligations equaled 2.93% of SBA's total fiscal year 2024 IT budget.	Total anticipated life cycle costs: $43 million over 5 years.	SBA anticipates quantifiable benefits with MySBA through streamlining processes, improving customer service, and unifying program data.

SBA officials stated that personnel from the Office of the Chief Information Officer, Office of the Administrator, and Office of the Chief Financial Officer are responsible for preparing MySBA's budget. The Office of the Chief Information Officer and the Office of the Administrator are responsible for providing oversight for the acquisition. MySBA has not required re-baselining at any point during its development. MySBA is expected to generate cost savings after the full implementation of its platform, though agency officials are still calculating exact savings figures associated with the acquisition.

Actual and estimated expenditures by fiscal year according to agency officials (in millions)



Source: GAO analysis of survey results. | GAO-25-106908

PRIOR WORK

We have previously issued reports related to SBA's MySBA Platform. For example:

- GAO. *Small Business Administration: Targeted Outreach About Disaster Assistance Could Benefit Rural Communities.* GAO-24-106755. Washington, D.C.: Feb. 22, 2024.
- GAO. *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*. GAO-23-106203. Washington, D.C.: Apr. 20, 2023.
- GAO. *IT Modernization: SBA Urgently Needs to Address Risks on Newly Deployed System*. GAO-25-106963. Washington, D.C.: Nov. 6, 2024.

As of February 2025, we had 14 open IT and cybersecurity recommendations related to SBA's efforts to modernize its IT systems. For example, we recommended that the Administrator of SBA should direct the Chief Information Officer to

- establish and implement policies and procedures to ensure that integrated master schedules are developed for IT modernization projects using leading practices described in GAO's *Schedule Assessment Guide*, and
- establish and implement policies and procedures to ensure that cost estimates for IT modernization projects are developed using leading practices described in GAO's *Cost Estimating and Assessment Guide*.

Agency Comments

We provided a draft of this report to the 11 agencies with IT acquisitions profiled in this report and OMB. In response, eight agencies (the Departments of Defense, Education, Health and Human Services, Homeland Security, Justice, State, Transportation, and Veterans Affairs) provided technical comments, which we incorporated as appropriate. Three agencies (the Department of the Treasury, the Environmental Protection Agency, and the Small Business Administration) stated that they did not have any comments on the report. OMB did not provide comments on the report.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of the Departments of Defense, Education, Health and Human Services, Homeland Security, State, Transportation, the Treasury, and Veterans Affairs; the U.S. Attorney General (Department of Justice); the Administrator of the Environmental Protection Agency; the Director of the Office of Management and Budget; the Administrator of the Small Business Administration; and other interested parties. This 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 in appendix III.

Sincerely,

Carol C. Harris, Director
Information Technology and Cybersecurity

Appendix I: Objective, Scope, and Methodology

The objective of this review was to identify essential mission-critical IT acquisitions across the federal government and their key attributes. To address the objective, we first developed a survey to distribute to each of the 24 federal agencies covered by the Chief Financial Officers Act of 1990.[1] In the survey, we asked agencies to identify their top three most important mission-critical acquisitions that had ongoing system development activities and had not yet been fully deployed.[2] We also asked agencies to answer specific questions about each identified acquisition. These questions related to, among other things, the acquisition's planned services and capabilities, the total anticipated lifecycle costs for the acquisition, potential risks, deployment timeline, types of acquisition end users, and anticipated impact on the agency and the nation (e.g., public health and safety). A copy of the questionnaire is reprinted in appendix II.

We then pretested the survey with two agencies: the Department of Homeland Security (DHS) and the Nuclear Regulatory Commission. In doing so, we interviewed and coordinated with officials in the offices of the Chief Information Officer (CIO) as well as acquisition oversight officials at these agencies to obtain their views as to whether our questions were clear and logical and to ensure that respondents could answer the questions without undue burden. We incorporated these agencies' feedback, as appropriate. We then administered the survey via

[1]The 24 federal agencies covered by the Chief Financial Officers Act of 1990, 31 U.S.C. § 901(b), 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.

[2]For this report, a mission-critical acquisition is one that furthers the specific mission of the agency and, as such, would be unique to that agency and that the damage to, or disruption of, this acquisition would cause the most impact on the organization, mission, or networks and systems. In addition, a mission-critical system is any telecommunication or information system that is defined as a national security system or that processes any information the loss, misuse, disclosure, or unauthorized access to or modification of would have a debilitating impact on the mission of the agency. See National Institute of Standards and Technology, Volume 1: *Guide for Mapping Types of Information and Information Systems to Security Categories,* Special Publication 800-60, Revision 1 (Gaithersburg, MD: August 2008).

email to each of the 24 agencies and received responses from 23.[3] The 23 agencies identified a total of 64 IT acquisitions.

To help ensure that we identified the most critical IT acquisitions for each agency, we also reviewed Federal IT Dashboard[4] data, assessed prior work that we and agencies' Inspectors General have issued, and consulted with our subject matter experts. We also asked each agency's Inspector General to provide us a list of what they believed were their agency's three to five most important mission-critical IT acquisitions. Fifteen of the 24 agencies' Inspectors General provided responses for a total of 54 IT acquisitions. These actions resulted in the selection of three additional acquisitions each from the Departments of Defense and the Department of Transportation and one each from the Department of the Treasury and DHS. With these additional selections, the total number of identified acquisitions we considered for our study was 72 from all 24 agencies.

To assess the criticality of each acquisition, we developed a set of criteria focused on several factors, including the acquisition's impact on the agency and the nation, cost and budget data, and risk factors. We developed these criteria based on our reviews of federal continuity planning guidance; agencies' Inspectors General reports; Federal IT Dashboard data (e.g., the agency's annual IT spending, acquisition-specific spending, and CIO risk ratings); and the 2021 President's Management Agenda. We also reviewed our April 2023 High-Risk Series report; our other relevant prior reports, including our September 2020 report on key attributes of essential federal mission-critical IT acquisitions; critical infrastructure sectors identified in the Presidential Policy Directive

[3]Although the Department of Defense did not provide a survey response designating its top three most important mission-critical acquisitions supported by IT within the audit time frame, we selected three as explained in the next paragraph.

[4]The Federal IT Dashboard is a public, government website previously operated by the Office of Management and Budget and currently by the General Services Administration at https://itdashboard.gov. It includes streamlined data to enable agencies and Congress to understand and manage federal IT portfolios and make better IT planning decisions and includes information on the performance of major IT investments.

21, Critical Infrastructure Security and Resilience; and federal agencies' survey responses.[5]

We then arranged the criteria into 14 categories: National Essential Functions, Agency Office of Inspector General, IT Dashboard/Chief Information Officer Risk Rating, President's Management Agenda, Government Accountability Office, Critical Infrastructure Sectors, Designation of Mission-Critical, Cost, Agency Oversight, OMB Oversight, Capabilities and Acquisition Type, Scope of End Users, Potential Risks to Agency and Nation, and Risk Factors. For each criterion within the 14 categories, we assigned a total point value ranging from zero to 16. We assigned point values based on the criticality of the criteria in terms of impact on the agency's mission. Our point values and criteria selection were informed by discussions with internal subject matter experts and methodologists. See table 6 for the selection criteria and their associated point values.

[5]U.S. Department of Homeland Security Federal Emergency Management Agency, *Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements* (Jan. 17, 2017); Office of Management and Budget, *The Biden-Harris Management Agenda Vision* (Washington, D.C.: November 2021); GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023); *Information Technology: Key Attributes of Essential Federal Mission-Critical Acquisitions*, GAO-20-249SP (Washington, D.C.: Sept. 8, 2020); and The White House, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013). National Security Memorandum 22 replaced Presidential Policy Directive 21 in April 2024, after we developed our criteria and analyzed each acquisition. See The White House, *National Security Memorandum 22: National Security Memorandum on Critical Infrastructure Security and Resilience* (Washington, D.C.: Apr. 30, 2024).

Table 7: GAO Selection Criteria Categories and Their Point Values

Criteria categories and attributes	Points	Point value description
National Essential Functions[a]		
Does the goal of the acquisition relate to maintaining and fostering effective relationships with foreign nations?	0 or 2	If yes, 2 points
Does the goal of the acquisition relate to protecting against threats to the homeland and bringing to justice perpetrators of crimes or attacks against the United States or its people, property, or interests?	0 or 2	If yes, 2 points
Does the goal of the acquisition relate to providing rapid and effective response to, and recovery from, the domestic consequences of an attack or other incident?	0 or 2	If yes, 2 points
Does the goal of the acquisition relate to protecting and stabilizing the nation's economy or ensuring public confidence in financial systems?	0 or 2	If yes, 2 points
Does the goal of the acquisition relate to providing for critical federal government services that address the national health, safety, and welfare needs of the United States?	0 or 2	If yes, 2 points
Agency Office of the Inspector General (OIG)		
Has the acquisition been audited by its agency OIG?	0 or 2	If yes, 2 points
Was the acquisition identified by the agency's OIG as a top mission-critical acquisition?	0 or 2	If yes, 2 points
IT Dashboard/Chief Information Officer (CIO) Risk Rating		
What was the acquisition's Federal IT Dashboard CIO risk rating?[b]	0 to 3	3 points if the risk rating was 'high', 2 points if the risk rating was 'medium', and 1 point if the risk rating was 'low', 0 points if the acquisition was not listed on the federal IT Dashboard
President's Management Agenda (PMA)[c]		
Does the acquisition address PMA Priority 1: Strengthening and Empowering the Federal Workforce?	0 or 2	If yes, 2 points
Does the acquisition address PMA Priority 2: Delivering Excellent, Equitable, and Secure Federal Services and Customer Experience?	0 or 2	If yes, 2 points
Does the acquisition address PMA Priority 3: Managing the Business of Government to Build Back Better?	0 or 2	If yes, 2 points
GAO		
Was the acquisition or its topic area included within GAO's High-Risk List?[d]	0 or 4	If yes, 4 points
Was the acquisition included in the scope of past and current GAO audits?	0 or 3	If yes, 3 points
Was the acquisition identified as an essential mission-critical IT acquisition across the federal government by GAO subject matter experts?	0 or 3	If yes, 3 points
Was the acquisition reported by the agency and/or selected by GAO as one of the most critical legacy systems in need of modernization?[e]	0 or 3	If yes, 3 points
Was the acquisition reported by the agency and/or profiled by GAO in our 2020 report as an essential mission-critical IT acquisition?[f]	0 or 3	If yes, 3 points

Critical Infrastructure Sectors[g]		
To which of the 16 critical infrastructure sectors does the acquisition relate?	0 to 16	1 point for each relevant critical infrastructure sector, up to 16 possible points
Designation of Mission-Critical[h]		
Does the acquisition meet the definition for "mission-critical" provided in the questionnaire?	1 to 3	Points based on professional judgment. 3 points if the definition was met, 2 points if partially met, 1 point if not met
Was the acquisition formally designated by the agency as "mission-critical"?	0 or 2	If yes, 2 points
Cost		
What is the acquisition's total life cycle cost?	1 to 3	3 points if the acquisition's total life cycle cost was greater than $100 million, 2 points if greater than $50 million and less than $100 million, 1 point if less than $50 million
What percentage of the agency's Fiscal Year (FY) 2023 IT budget was the acquisition allotted?	1 to 3	3 points of the acquisition was allotted 5 or more percent of the agency's FY 2023 IT budget, 2 points if greater than 1 percent and less than 5 percent, 1 point if less than 1 percent
Is the agency sharing the development costs and/or management of the acquisition with another federal agency?	0 or 1	If yes, 1 point
Agency Oversight		
Which offices within the agency is/are responsible for the acquisition's oversight?	1 to 3	3 points if 3 or more offices were responsible for the acquisition's oversight, 2 points if 2 offices were responsible, 1 point if 1 office was responsible
OMB Oversight		
Has the agency conducted a TechStat related to the acquisition or the investment that it supports?[i]	0 or 2	If yes, 2 points
What was GAO determination of the TechStat session's significance?	1 to 3	Points based on professional judgment. 3 points if very significant, 2 points if moderately significant, 1 point if not very significant
Has the agency met with OMB regarding oversight of the acquisition or the investment that it supports?	0 or 2	If yes, 2 points
How often did these agency meetings with OMB take place?	1 to 3	Acquisitions for which OMB meetings were held on a more frequent basis received more points
What was GAO's determination of the significance of the OMB meeting(s)?	1 to 3	Points based on professional judgment. 3 points if very significant, 2 points if moderately significant, 1 point if not very significant
Has OMB conducted a PortfolioStat for the acquisition or the investment that it supports?[j]	0 or 2	If yes, 2 points

What was GAO's determination of the PortfolioStat's significance?	1 to 3	Points based on professional judgment. 3 points if very significant, 2 points if moderately significant, 1 point if not very significant
Is the acquisition, or the investment that it supports, related to an entity that OMB has designated as a High Impact Service Provider?[k]	0 or 2	If yes, 2 points
Does the agency expect to identify any systems, information, or data resulting from the acquisition as a high value asset?[l]	0 or 3	If yes, 3 points
What was GAO's determination of the criticality of the high value asset?	0 to 3	Points based on professional judgment. 3 points if criticality was high; 2 points if criticality was medium; 1 point if criticality was low; 0 points if the agency did not expect to identify systems, information, or data resulting from the acquisition as a high value asset.
Capabilities and Acquisition Type		
Do the acquisition's services and capabilities address or impact infrastructure?	0 or 1	If yes, 1 point
Do the acquisition's services and capabilities address or impact the agency's IT architecture?	0 or 1	If yes, 1 point
Do the acquisition's services and capabilities address or impact the agency's mission?	0 or 1	If yes, 1 point
Do the acquisition's services and capabilities have national implications?	0 or 3	If yes, 3 points
Was the acquisition designated as a major acquisition?[m]	0 or 2	If yes, 2 points
What was the acquisition type?	1 to 3	3 points if the acquisition is a new system with new capabilities, 2 points if it is a replacement of a legacy system, 1 point if it is an enhancement or component to an existing system
Scope of End Users		
Will agency-wide end users use or be affected by the acquisition?	0 or 1	If yes, 1 point
Will component-specific end users use or be affected by the acquisition?	0 or 1	If yes, 1 point
Will the general public use or be affected by the acquisition?	0 or 2	If yes, 2 points
Will specific public users use or be affected by the acquisition?	0 or 1	If yes, 1 point
Will the military use or be affected by the acquisition?	0 or 1	If yes, 1 point
Will other agencies use or be affected by the acquisition?	0 or 1	If yes, 1 point
Will international end users use or be affected by the acquisition?	0 or 1	If yes, 1 point
Will other relevant end users use or be affected by the acquisition?	0 or 1	If yes, 1 point
Potential Risks to Agency and Nation		
Did the agency report that there would be an adverse impact on the agency and its mission if the acquisition were terminated before the work was completed?	0 or 2	If yes, 2 points

What was GAO's determination of the acquisition's level of potential impact on the agency and its mission?	0 to 3	Points based on professional judgment. 3 points if the impact was high, 2 points if the impact was medium, 1 point if the impact was low, 0 points if the agency did not report that there would be an adverse impact
Did the agency report that the acquisition would have an impact on the nation's public health and safety once deployed or placed in production?	0 or 3	If yes, 3 points
What was GAO's determination of the acquisition's level of potential impact on the nation's public health and safety?	0 to 3	Points based on professional judgment. 3 points if the impact was high, 2 points if the impact was medium, 1 point if the impact was low, 0 points if the agency did not report that there would be an impact
Risk Factors		
How did the agency rate the organizational risk associated with the acquisition?	0 to 6	6 points if very risky, 4 points if moderately risky, 2 points if low risk, 0 points if not risky or not applicable/no basis to judge
How did the agency rate the cybersecurity risk associated with the acquisition?	0 to 3	3 points if very risky, 2 points if moderately risky, 1 point if low risk, 0 points if not risky or not applicable/no basis to judge
How did the agency rate the information privacy risk associated with the acquisition?	0 to 3	3 points if very risky, 2 points if moderately risky, 1 point if low risk, 0 points if not risky or not applicable/no basis to judge
How did the agency rate the technical risk associated with the acquisition?	0 to 3	3 points if very risky, 2 points if moderately risky, 1 point if low risk, 0 points if not risky or not applicable/no basis to judge
How did the agency rate the cost/budget risk associated with the acquisition?	0 to 3	3 points if very risky, 2 points if moderately risky, 1 point if low risk, 0 points if not risky or not applicable/no basis to judge
How did the agency rate the schedule risk associated with the acquisition?	0 to 3	3 points if very risky, 2 points if moderately risky, 1 point if low risk, 0 points if not risky or not applicable/no basis to judge
How did the agency rate the risk of not implementing the acquisition?	0 to 6	6 points if very risky, 4 points if moderately risky, 2 points if low risk, 0 points if not risky or not applicable/no basis to judge
How did the agency rate an applicable other risk associated with the acquisition?	0 to 3	3 points if very risky; 2 points if moderately risky; 1 point if low risk, 0 points if not risky or no risk provided/not applicable/no basis to judge

Source: GAO analysis. | GAO-25-106908

[a]For the National Essential Functions used in these criteria, see U.S. Department of Homeland Security Federal Emergency Management Agency, Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements (Jan. 17, 2017).

[b]In June 2009, OMB deployed the Federal IT Dashboard, a public website with information on the performance of major federal investments to further improve the transparency into and oversight of federal agencies' IT investments.

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

[d]For GAO's High-Risk List, see 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).

[e]See GAO, Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems, GAO-19-471 (Washington, D.C., June 11, 2019). As part of the methodology for this report, agencies identified legacy systems that were most in need of modernization.

[f]See GAO, Information Technology: Key Attributes of Essential Federal Mission Critical Acquisitions, GAO-20-249SP (Washington, D.C.: Sept. 8, 2020). As part of the methodology for this report, we asked each agency to identify its five most important mission-critical IT acquisitions that had ongoing system development activities and had not yet been fully deployed.

[g]The White House, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (Washington, D.C.: Feb. 12, 2013). There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. These sectors include chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation, and water and wastewater systems.

[h]For this report, a mission-critical acquisition refers to an acquisition supported by IT that furthers the specific mission of the agency and as such would be unique to that agency. The damage or disruption to this acquisition would cause the most impact on the organization, mission, or to its networks and systems. In addition, also categorized as mission critical is any telecommunications or information system that is defined as a national security system or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.

[i]A TechStat is a face-to-face meeting to discuss whether to terminate or turn around IT investments that are in danger of failing or are not producing results.

[j]A PortfolioStat session is a face-to-face, evidence-based review of an agency's IT portfolio that includes data on commodity IT investments, potential duplications within the agency, investments that do not appear to be well aligned to agency missions or business functions, and other key considerations and data within an agency's IT portfolio. In addition, PortfolioStat is a tool that agencies use to assess the current maturity of their IT portfolio management process, make decisions on eliminating duplication, augment current CIO-led capital planning and investment control processes, and move to shared solutions in order to maximize the return on IT investments across the portfolio.

[k]As defined in OMB Circular A-11, Section 280, High-Impact Service Providers (HISPs) are those Federal entities designated by OMB that provide high-impact customer-facing services, either due to a large customer base or a high impact on those served by the program. A HISP interacts with the public to provide a transactional service or perform a regulatory function in which time, money, or information is used to receive a good, service, or authorization.

[l]High Value Assets are those assets, federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. HVAs may contain sensitive controls, instructions, data used in critical Federal operations, or unique collections of data (by size or content), or support an agency's mission essential functions, making them of specific value to criminal, politically motivated, or state sponsored actor for either direct exploitation or to cause a loss of confidence in the U.S. Government.

[m]As defined in OMB Circular A-11, Part 7, major acquisitions are capital assets that require special management attention because of their importance to the agency mission; high development, operating, or maintenance costs; high risk; high return; or their significant role in the administration of agency programs, finances, property, or other resources.

We then analyzed information regarding the acquisitions from agency-provided survey responses, the Federal IT Dashboard, and prior reports that we and the agencies' Inspectors General have issued. For each acquisition, we used this information to assign point values based on either the presence of the criteria within an acquisition or the criticality of the acquisition's impact, such as to the agency's mission or the nation.

To select a subset of 16 of the 72 acquisitions on which to gather additional data for potential profiling in our report, we first calculated the total point values associated with the criteria for each acquisition. In order to provide a larger representation of agencies' acquisitions across the federal government, we limited our selection to the two IT acquisitions with the highest point values per agency.[6] As a result of these activities and based on the highest point totals, we selected 16 IT acquisitions across 11 agencies that are key to achieving the various agencies' missions across the federal government.[7]

For each of the 16 selected acquisitions, we provided the relevant agencies with a second survey that inquired about the agency's basis for initiating the acquisition, dates of key milestones, cost and budget data, performance measures, and government and contract workforce. We also obtained and analyzed supporting documentation regarding acquisition implementation and strategy, cost and schedule, risks and issues, and related information. Additionally, we interviewed relevant agency officials, as necessary. We then summarized key attributes provided in agency responses and documentation into acquisition profiles that are included in this report. The profiles include IT acquisitions from 11 of the 24 agencies covered under the Chief Financial Officers Act of 1990.

[6]We also excluded acquisitions that did not have ongoing or planned system development activities at the time of our review or had sensitivity concerns.

[7]The 11 federal agencies from which we selected acquisitions are the Departments of Defense, Education, Health and Human Services, Homeland Security, Justice, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; and the Small Business Administration.

The profiles and the data presented in this report reflect key attributes of the selected federal IT acquisitions as of January 2025, unless otherwise noted.

We conducted this performance audit from June 2023 to March 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Copy of the Questionnaire That GAO Administered to the 24 Agencies Covered by the Chief Financial Officers Act

To obtain information on federal agencies' IT acquisitions, we administered a questionnaire to the 24 major agencies covered by the Chief Financial Officers Act of 1990, from December 2023 through May 2024.[1] The questionnaire is shown here and a more detailed discussion of our questionnaire methodology is discussed in appendix I.

[1]The 24 major federal agencies covered by the Chief Financial Officers Act 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.

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

GAO Survey: Nation's Top Mission-Critical Acquisitions Supported by Information Technology

Agency:
Date Sent:
Date Due:
GAO Engagement Code: 106908
GAO Point of Contact: <Select one>

Instructions

This is a fillable PDF form. Before starting to fill out this form, save the file to your computer now. Open it in Adobe Acrobat or Foxit, then re-save your answers periodically as you go.

- You can click on buttons or check boxes, and type into highlighted boxes throughout the form; the boxes will accommodate more text than is visible. A second click on a check box will remove the check mark.
- In addition to clicking or scrolling, you can use the Tab key to jump to the next answer space and use Shift + Tab to move backwards.

The Government Accountability Office (GAO) is conducting this survey in response to a Congressional request for information on the status of the top mission critical acquisitions supported by information technology (IT) across federal agencies. This is being sent to you and the other *Chief Financial Officers Act* agencies under engagement **106908**. We need your help in identifying the top three acquisitions that are supported by IT in your agency that are considered to be mission critical.

Please respond to the survey by the due date shown above. In case we have additional questions, please provide a point of contact(s) or person(s) responsible for filling out the survey section corresponding to each acquisition in the spaces provided in Sections B, C, and D. **Your response can be submitted via email to the GAO point of contact shown above. Please also copy the response to** <Select one>.

Key Terms

Mission Critical: An acquisition supported by IT that furthers the specific mission of the agency and as such would be unique to that agency. The damage or disruption to this acquisition would cause the most impact on the organization, mission, or to its networks and systems. In addition, also categorized as mission critical is any telecommunications or information system that is defined as a national security system or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.[1]

Acquisition: According to Federal Acquisition Regulation (FAR) 2.101(b)(2), an "acquisition" means the acquiring by contract with appropriated funds of supplies or services (including construction) by and for the use of the federal government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract.

[1]*National Institute of Standards and Technology,* Guide for Mapping Types of Information and Information Systems to Security Categories, Special Publication 800-60 Volume I Revision 1 (Gaithersburg, MD: August 2008).

1

Source: GAO. | GAO-25-106908

Information Technology: According to section 11101(6) of title 40, United States Code, the term "information technology"- (1) with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use- (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; (2) includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

Section A. Mission Critical Acquisitions Supported by IT

A1. What are your top 3 mission critical acquisitions supported by IT (include only those acquisitions that are not yet fully deployed)? Please enter each acquisition's name and unique investment identifier.[2] (Please complete Sections B, C, and D, one for each of the acquisitions listed below):

Mission critical acquisition	Name of mission critical acquisition	Unique investment identifier
Mission critical acquisition #1		
Mission critical acquisition #2		
Mission critical acquisition #3		

[2]A unique investment identifier is a persistent numeric code applied to an investment that allows the identification and tracking of an investment across multiple fiscal years of an agency's investment portfolio. The unique investment identifier is composed of a 3-digit agency code concatenated with a 9-digit unique investment number generated by the agency.

2

Source: GAO. | GAO-25-106908

Section B. Profile of Mission Critical Acquisition Number 1 of 3:
Name of Acquisition:

Background and Systems Development

Please provide your responses to the questions below for the first acquisition listed in Section A:

B1. Who is/are the point(s) of contact responsible for filling out this acquisitions profile?

a. Name:
b. Title:
c. Office/Team:
d. Telephone:
e. Email:

B2. How does this acquisition fit into the definition provided for "mission critical?"

a. Before this survey, was this acquisition formally designated as 'mission critical' by the agency?
- ◯ Yes
- ◯ No
- ◯ Other *(specify)*:
- ◯ Don't know

B3. What are the total anticipated lifecycle costs[3] for this acquisition?

B4. Is your agency sharing the development costs and/or management of this acquisition (e.g., interagency agreements, cost-sharing contracts, etc.) with another federal agency?
- ◯ Yes
- ◯ No
- ◯ Other *(specify)*:

a. If yes, please describe this relationship:

B5. When was the first contract for this acquisition awarded?

B6. When does your agency expect the work under this acquisition to be placed into deployment/production?

[3]For the purposes of this survey, life-cycle cost means the total cost to the agency of acquiring, operating, and supporting the asset being acquired.

3

Source: GAO. | GAO-25-106908

B7. What office(s) within your agency is/are responsible for the oversight of this acquisition?

B8. Has your agency conducted a TechStat[4] session related to this acquisition or the investment that it supports?

◯ Yes ◯ No ◯ Don't know ◯ Not applicable

a. If yes, please describe the nature and purpose of this session:

B9. Has your agency met with officials from the Office of Management and Budget (OMB) regarding oversight of this acquisition or the investment that it supports?

◯ Yes ◯ No

a. If yes, how often did these meetings take place and with whom?

b. If yes, please describe the nature and purpose of these meetings:

B10. Has OMB conducted a PortfolioStat[5] for this acquisition or the investment that it supports?

◯ Yes ◯ No ◯ Don't know ◯ Not applicable

a. If yes, please describe the nature and purpose of this session:

B11. Is this acquisition, or the investment that it supports, related to an entity that OMB has designated as a "High-Impact Service Provider?"[6]

◯ Yes ◯ No ◯ Don't know

B12. Does your agency expect to identify any systems, information, or data resulting from this acquisition as a high value asset?[7]

◯ Yes ◯ No ◯ Don't know

[4]A TechStat is a face-to-face meeting to discuss whether to terminate or turn around IT investments that are in danger of failing or are not producing results.

[5]A PortfolioStat session is a face-to-face, evidence-based review of an agency's IT portfolio that includes data on commodity IT investments, potential duplications within the agency, investments that do not appear to be well aligned to agency missions or business functions, and other key considerations and data within an agency's IT portfolio. In addition, PortfolioStat is a tool that agencies use to assess the current maturity of their IT portfolio management process, make decisions on eliminating duplication, augment current CIO-led capital planning and investment control processes, and move to shared solutions in order to maximize the return on IT investments across the portfolio.

[6]As defined in OMB Circular A-11, Section 280, High-Impact Service Providers (HISPs) are those Federal entities designated by OMB that provide high-impact customer-facing services, either due to a large customer base or a high impact on those served by the program. A HISP interacts with the public to provide a transactional service or perform a regulatory function in which time, money, or information is used to receive a good, service, or authorization. See also http://www.performance.gov/cx/HISPs for more information.

[7]"High Value Assets" (HVA) are those assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. HVAs may contain sensitive controls, instructions, data used in critical Federal operations, or unique collections of data (by size or content), or support an agency's mission essential functions, making them of specific value to criminal, politically motivated, or state sponsored actor for either direct exploitation or to cause a loss of confidence in the U.S. Government.

Source: GAO. | GAO-25-106908

B13. What services and capabilities are to be provided by this acquisition?

B14. What type of end users will be affected by the asset under this acquisition? *(select all that apply)*:

- ☐ Agency-wide
- ☐ Component-specific
- ☐ General Public
- ☐ Specific Public Users
- ☐ Military
- ☐ Other Agencies
- ☐ International
- ☐ None
- ☐ Other *(specify)*:

B15. Is this acquisition designated as:

- ◯ a Major acquisition?[8]
- ◯ a Non-Major acquisition?
- ◯ Other *(specify)*:

Please describe how your agency defines the acquisition type selected above:

B16. Is this acquisition:

- ◯ a new system with new capabilities?
- ◯ a replacement of a legacy system?
- ◯ an enhancement or component to an existing system?
- ◯ Other *(specify)*:

Potential Risks

Questions in this section are intended to collect information for each mission critical acquisition identified in section A regarding the agency's perceived and potential risk for the attributes listed below. Please provide your responses to the following questions:

B17. What impact would this acquisition have on your agency and its mission if it were terminated before the work was completed?

B18. What impact, if any, will this acquisition have on the nation's public health and safety once deployed/placed in production?

[8]As defined in OMB Circular A–11, Part 7, major acquisitions are capital assets that require special management attention because of their importance to the agency mission; high development, operating, or maintenance costs; high risk; high return; or their significant role in the administration of agency programs, finances, property, or other resources.

Source: GAO. | GAO-25-106908

B19. In your opinion, how would you rate the following risk factors for this acquisition? (Descriptions of the risk factors are included after the survey questions.)

	Very risky ▼	Moderately risky ▼	Low risk ▼	Not risky ▼	Not applicable/ No basis to judge ▼
Organizational risk	○	○	○	○	○
Cybersecurity risk	○	○	○	○	○
Information privacy risk	○	○	○	○	○
Technical risk	○	○	○	○	○
Cost/budget risk	○	○	○	○	○
Schedule risk	○	○	○	○	○
Risk of not implementing this acquisition	○	○	○	○	○
Other *(specify)*:	○	○	○	○	○

Risk Factors

Organizational Risk: Evaluates the impact of acquisition on the organization. Also, assesses the risk that the proposed system will fail due to organizational disruption.

- Low Risk: Acquisition has little impact on the organization or the project is mitigating this risk through training and/or investment in a business process redesign effort which builds commitment to the acquisition.
- Very Risky: Implementation requires significant organizational change, process redesign and/or people's jobs to be done differently and the project is not proactively seeking to mitigate this risk.

Cybersecurity Risk: A level of security should be established for all information systems that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in these information systems. Identifying and assessing security risks are essential steps in determining what controls are required to mitigate the risks.

- Low Risk: A threat event could be expected to have a limited adverse effect on organizational security operations, operational assets, individuals, other organizations, or the Nation.
- Very Risky: A threat event could be expected to have severe or catastrophic adverse effect on organizational security operations, operational assets, individuals, other organizations, or the Nation.

Information Privacy Risk: Information privacy risks include, but are not limited to, disclosure to unknown third parties for unspecified uses, tracking, identity theft, threats to physical safety, and surveillance. Agencies should determine the risks and effects of collecting, maintaining, and disseminating information in an identifiable form in an electronic information system.

- Low Risk: A threat event could be expected to have a limited adverse effect on organizational privacy operations, operational assets, individuals, other organizations, or the Nation.
- Very Risky: A threat event could be expected to have severe or catastrophic adverse effect on organizational privacy operations, operational assets, individuals, other organizations, or the Nation.

Technical Risk: Evaluates the risk to complete the acquisition from a technical point of view.

- Low Risk: Hardware and software conform to organization's technical architecture and there is successful experience in using this technology in the organization. Hardware, software, and support are commercially available and do not have to be developed for use in the organization.

6

Source: GAO. | GAO-25-106908

- Very Risky: Hardware and/or software solution does not conform to organization's technical architecture and/or there is little or no experience with this technology in the organization. Hardware, software, or support is not now available commercially and requires development specifically for the organization.

Cost/Budget Risk: Evaluates the sensitivity or quality of the cost estimates.

- Low Risk: Cost estimates are well supported. Little software development required or a software cost estimating technique has been used to produce a reasonably reliable cost estimate.
- Very Risky: Acquisition is complex and cost estimates appear to require or have required additional refinement. Software development is required and represents more than 50% of the predicated cost.

Schedule Risk: Evaluates the probability this acquisition will remain on schedule.

- Low Risk: Acquisition is not likely to slip; acquisition strategy should result in timely contract award such that funds scan be obligated as planned. Adequate staff is available and has requisite experience to execute the acquisition; acquisition is not complex. Acquisition's schedule has not been accelerated to meet deadlines.
- Very Risky: Acquisition is likely to slip; acquisition strategy indicates contract may not be awarded in time to meet schedule or obligate budget year dollars. Acquisition's staff is limited in size and/or experience and is complex. An accelerated schedule was imposed rather than developed from project planning.

Risk of Not Implementing this Acquisition: Assess the risk to the organization of not proceeding with this acquisition.

- Low Risk: If this acquisition is not deployed the effects of this acquisition can still be attained.
- Very Risky: This acquisition is important to provide future opportunities for cost savings and/or much improved customer service. If this acquisition is not deployed or is delayed for a year the organization will probably fail to meet customer demands in the near future.

7

Source: GAO. | GAO-25-106908

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Carol C. Harris, (202) 512-4456 or harriscc@gao.gov

Staff Acknowledgments

In addition to the contact name above, the following staff made key contributions to this report: Jon Ticehurst (Assistant Director), Neha Bhatt (Analyst in Charge), Chris Businsky, Andrew Erickson, Rebecca Eyler, Jonnie Genova, Colin Jenkins, Evan Kreiensieck, Claire Saint-Rossy, and Walter Vance.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on Facebook, Flickr, X, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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


GAO
U.S. GOVERNMENT
ACCOUNTABILITY
OFFICE