U.S. GOVERNMENT ACCOUNTABILITY OFFICE

INFORMATION TECHNOLOGY

Key Attributes of Essential Federal Mission-Critical Acquisitions

Report to Congressional Requesters

September 2020
GAO-20-249SP

GAO Highlights

Highlights of GAO-20-249SP, a report to congressional requesters

September 2020

INFORMATION TECHNOLOGY

Key Attributes of Essential Federal Mission-Critical Acquisitions

Why GAO Did This Study

The acquisition of IT systems has presented challenges to federal agencies. Accordingly, in 2015 GAO identified the management of IT acquisitions and operations as a high-risk area, a designation it retains today.

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

To identify acquisitions for the review, GAO administered a questionnaire to the 24 agencies covered by the *Chief Financial Officers Act of 1990* asking them to identify their five most important mission-critical IT acquisitions. From a total of 101 acquisitions that were identified, GAO selected 16 mission-critical IT acquisitions to profile in this report. The selection was based on various factors, including the acquisition's criticality to providing service to the nation, its total life cycle costs, and its applicability to the President's Management Agenda.

For each of the 16 selected acquisitions, GAO obtained and analyzed documents on cost, schedule, risks, governance, and related information; and interviewed cognizant agency officials.

GAO requested comments from the 12 agencies with acquisitions profiled in its draft report and the Office of Management and Budget. In response, one agency (the Social Security Administration) provided comments that discussed the planned use of its system.

View GAO-20-249SP. For more information, contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov.

What GAO Found

Federal agencies are undertaking information technology (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 these acquisitions and the programs they support, and has made numerous recommendations to agencies for improvement.

The amount agencies expect to spend on the selected acquisitions vary 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 Defense plans to spend $10.21 billion over 21 years on its health care modernization initiative, while the Department of Homeland Security intends to spend $3.19 billion over 30 years on its system supporting immigration benefits processing. Agencies reported potential cost savings associated with 13 of the 16 mission-critical acquisitions after deployment due to factors such as shutting down legacy systems, eliminating physical paper processing, and improving security, monitoring, and management.

Eleven of the 16 selected acquisitions were rebaselined during their development, meaning that the project's cost, schedule, or performance goals were modified to reflect new circumstances. Agencies reported a number of reasons as to why their acquisitions were rebaselined, including delays in defining the cost, schedule, and scope; budget cuts and hiring freezes; technical challenges; and changes in development approach.

As shown below, ten of the acquisitions relate to an additional programmatic area that GAO has designated high risk.

Federal Agency	Mission-Critical Information Technology Acquisitions
Department of Agriculture	Modernize and Innovate the Delivery of Agricultural Systems
Department of Commerce	2020 Decennial Census*
Department of Defense	Defense Healthcare Management System Modernization* Global Combat Support System-Army*
Department of Homeland Security	Student and Exchange Visitor Information System Modernization* U.S. Citizenship and Immigration Services Transformation*
Department of the Interior	Automated Fluid Minerals Support System II*
Department of Justice	Next Generation Identification System Terrorist Screening System
Department of State	Consular System Modernization
Department of Transportation	Automatic Dependent Surveillance-Broadcast
Department of the Treasury	Customer Account Data Engine 2* Integrated Enterprise Portal*
Department of Veterans Affairs	Electronic Health Record Modernization*
Small Business Administration	Application Standard Investment
Social Security Administration	Disability Case Processing System 2*

Legend: *= Acquisition relates to a programmatic area that GAO has previously designated as being high risk.

Source: GAO analysis of agency data. | GAO-20-249SP

Contents

Tables

Figure

Abbreviations

ADS-B	Automatic Dependent Surveillance Broadcast
AFMSS	Automated Fluid Minerals Support System
BLM	Bureau of Land Management
CADE 2	Customer Account Data Engine 2
CIO	chief information officer
CSM	Consular Systems Modernization
DCPS2	Disability Case Processing System 2

DHS	Department of Homeland Security
DHMSM	Department of Defense Healthcare Management System Modernization
DOD	Department of Defense
EHRM	Electronic Health Record Modernization
ELIS	Electronic Immigration System
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FSA	Farm Service Agency
FITARA	*Federal Information Technology Acquisition Reform Act*
FY	fiscal year
GCSS-Army	Global Combat Support System-Army
IEP	Integrated Enterprise Portal
ICE	Immigration and Customs Enforcement
IRS	Internal Revenue Service
IT	information technology
MIDAS	Modernize and Innovate the Delivery of Agricultural Systems
MHS GENESIS	Military Health System GENESIS
NextGen	Next Generation Air Transportation System
NGI	Next Generation Identification
OMB	Office of Management and Budget
SBA	Small Business Administration
SEVIS	Student and Exchange Visitor Information System
SSA	Social Security Administration
State	Department of State
Transportation	Department of Transportation
Treasury	Department of the Treasury
TSC	Terrorist Screening Center
TSS	Terrorist Screening System
USCIS	U.S. Citizenship and Immigration Services
USDA	Department of Agriculture
VA	Department of Veterans Affairs

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

September 8, 2020

Congressional Requesters

Information technology (IT) has the potential to enable federal agencies to accomplish their missions more quickly, effectively, and economically. However, while the federal government has undertaken numerous initiatives to better manage the billions of dollars that federal agencies annually invest in IT, these investments have too frequently failed or incurred cost overruns and schedule slippages, and contributed little to mission-related outcomes. These failed investments often suffered from a lack of disciplined and effective management, such as project planning, requirements definition, and program oversight and governance. Accordingly, in 2015 we identified improving the management of IT acquisitions and operations as a high-risk area, a designation it retains today.[1]

In recognition of agencies' continuing difficulties in managing IT, in December 2014, Congress enacted federal IT acquisition reform provisions (commonly referred to as the *Federal Information Technology Acquisition Reform Act*, or FITARA) as a part of the *Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015*.[2] FITARA was intended to improve the management and acquisition of IT for covered agencies, facilitate Congress' monitoring of agencies' progress, and hold those agencies 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

[1]GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C. Feb. 11, 2015) and *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019).

[2]*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).

management of IT acquisitions.[3] This report responds to your request that we identify and report on selected federal IT acquisitions.[4] Our specific objective was to identify essential mission-critical IT acquisitions across the federal government and determine their key attributes.[5]

To address this objective, we first identified acquisitions for possible selection by administering a questionnaire via email to each of the 24 federal agencies covered by the *Chief Financial Officers Act of 1990*.[6] In the questionnaire, 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. We also asked each agency to answer specific questions about each identified acquisition. These questions related to, among other things, the acquisition's planned services and capabilities, governance structure,

[3]See, for example, GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, GAO-20-129 (Washington, D.C.: Oct. 30, 2019); *Information Technology: Effective Practices Have Improved Agencies' FITARA Implementation,* GAO-19-131 (Washington, D.C.: Apr. 29, 2019); *Information Technology: Departments Need to Improve Chief Information Officers' Review and Approval of IT Budgets*, GAO-19-49 (Washington, D.C.: Nov. 13, 2018).

[4]For the purpose of this report, the term 'acquisition' is a broad term that also includes IT investments. According to the *Federal Acquisition Regulation*, an "acquisition" means using appropriated funds to acquire, by contract, supplies or services (including construction) by and for the use of the federal government through purchase or lease. The purchase or lease can be for supplies or services already in existence or that must be created, developed, demonstrated, or 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.

[5]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.

[6]The 24 federal agencies covered by the *Chief Financial Officers Act of 1990* are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

systems development life cycle and costs, potential risks, project time line, and anticipated impact on the agency and the nation (e.g., public health and safety).

We pretested the questionnaire at three of the federal agencies: the Department of Homeland Security, the National Aeronautics and Space Administration, and the Nuclear Regulatory Commission. In doing so, we interviewed officials in the offices of the Chief Information Officer (CIO) and the Chief Acquisition Officer 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 then administered the questionnaire and received responses from 23 of the 24 agencies. The 23 agencies identified a total of 98 IT acquisitions.[7]

To help ensure that we identified the most critical IT acquisitions for each agency, we also reviewed Federal IT Dashboard data and prior reports that we and federal 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 top three to five mission-critical IT acquisitions. These actions resulted in the selection of two additional Department of Defense acquisitions and one additional Department of the Treasury acquisition. With these additional selections, the total number of identified acquisitions we considered for our study was 101.

To select the acquisitions to be profiled in this report, we developed a set of criteria that 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 acquisition's budget, project schedule status, and chief information officer risk ratings); the *2018 President's Management Agenda*; the Office of Management and Budget's (OMB) reports on high-priority programs; our February 2015, February 2017, September 2018, and March 2019 *High-Risk Series* reports; our other relevant prior reports; critical infrastructure sectors

[7]The Department of Defense (DOD) did not provide a questionnaire response that listed five mission-critical IT acquisitions within the audit timeframe.

identified in the Presidential Policy Directive 21; and federal agencies' questionnaire results.[8]

We assigned to each criterion 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 questionnaire responses, the IT Dashboard, and prior reports that OMB, the Inspectors General, and we have issued. For each acquisition, we used this information to assign the aforementioned point values to the criteria we developed. To refine the list of acquisitions further, we calculated the total point values associated with the criteria for each identified acquisition. We then selected those acquisitions with a total point value of at least 75 points (20 total acquisitions) based on a natural breaking point provided by our analysis for this report. In order to provide a larger representation of agencies' acquisitions across the federal government, we selected the two highest-rated IT acquisitions per agency.[9] We also consulted with the former Federal CIO to confirm that the acquisitions we selected were critical to federal government operations.

As a result of these activities, we identified 16 IT acquisitions that are key to achieving the various agencies' missions across the federal government. For each of the 16 selected acquisitions, GAO obtained and analyzed documents on cost, schedule, risks, governance, and related

[8]U.S. Department of Homeland Security Federal Emergency Management Agency, *Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements* (January 17, 2017); Office of Management and Budget, *Report to Congress: 10 High Priority Programs* (Washington, D.C.: June 9, 2016) and *Quarterly Report to Congress: 10 High Priority Programs Quarterly Report* (Washington, D.C.: June 25, 2015); United States Digital Service, *The U.S. Digital Service Report to Congress*, July 2017 and *The U.S. Digital Service Report to Congress*, December 2016; GAO-15-290; *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017); *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018); GAO-19-157SP; *Presidential Policy Directive 21:Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013); and President's Management Council and Executive Office of the President, *President's Management Agenda* (Washington, D.C.: Mar. 20, 2018).

[9]We also excluded acquisitions that no longer had planned development work at the time of our review.

information; and interviewed cognizant agency officials. We then summarized key attributes into acquisition profiles that are included in this report. The profiles include IT acquisitions from 12 of the 24 agencies covered under the *Chief Financial Officers Act of 1990*.

Appendix I provides more details regarding our objectives, 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 February 2018 to September 2020 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 the federal government has spent billions of dollars on failed or troubled IT investments.[10]

In last year's update to our list of high-risk areas to monitor, we noted that some progress had been made in addressing the high-risk area of IT acquisitions and operations, but that there was a significant amount of work that remained to be completed to protect the government's investments.[11] Specifically, many of these investments suffered from a lack of disciplined and effective management, such as in planning projects, defining requirements, and overseeing and governing programs.

[10]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); *Information Technology: Effective Practices Have Improved Agencies' FITARA Implementation*, GAO-19-131 (Washington, D.C.: Apr. 29, 2019); and GAO-15-290.

[11]GAO-19-157SP.

Congress Enacted an IT Acquisition Law and Executive Branch Initiated Efforts to Improve IT Acquisition Management and Oversight

FITARA provisions were 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 as challenges in implementing selected provisions of the act.[12] These reports, along with scorecards issued by the House Committee on Oversight and Government Reform, indicate variations in the extent to which covered agencies have implemented the FITARA provisions.[13] Since the enactment of the provisions in 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 also undertaken various initiatives to improve IT acquisition management and oversight. These include:

- **Defining national essential functions for continuity.** On July 15, 2016, the President signed Presidential Policy Directive 40, *National Continuity Policy*, which established a national policy for the continuity of federal government structures and operations and national essential functions, among other things. According to Presidential Policy Directive 40 and the subsequent U.S. Department of Homeland Security (DHS) Federal Emergency Management Agency, *Federal Continuity Directive 1* issued in January 2017,[14] the national essential functions are intended to form the foundation for all continuity

[12]For example, GAO-19-131; GAO, *Data Center Optimization: Continued Agency Actions Needed to Meet Goals and Address Prior Recommendations*, GAO-18-264 (Washington, D.C.: May 23, 2018); *Information Technology Reform: Agencies Need to Improve Certification of Incremental Development,* GAO-18-148 (Washington, D.C.: Nov. 7, 2017); *Information Technology: Agencies Need to Improve Their Application Inventories to Achieve Additional Savings,* GAO-16-511 (Washington, D.C.: Sept. 29, 2016); and *Information Technology Reform: Agencies Need to Increase Their Use of Incremental Development Practices,* GAO-16-469 (Washington, D.C.: Aug. 16, 2016).

[13]Beginning in November 2015, the House of Representatives Committee on Oversight and Reform released its biannual FITARA scorecard that assigned letter grades to federal agencies on their implementation of FITARA, among other things.

[14]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).

programs and capabilities and represent the overarching responsibilities of the federal government to lead and sustain the nation during a crisis. The directive intended for the national essential functions to be the primary focus of the federal government leadership during and in the aftermath of an emergency that adversely affects the performance of government. These functions include the following:

- Defend the Constitution of the United States against all enemies, foreign and domestic, and prevent or interdict attacks against the United States or its people, property, or interests.
- Provide rapid and effective response to and recovery from the domestic consequences of an attack or other incident.
- Protect and stabilize the nation's economy and ensure public confidence in its financial systems.
- Provide for federal government services that address the national health, safety, and welfare needs of the people of the United States.

- **Establishing the Office of American Innovation and the American Technology Council.** In March 2017, the administration established the Office of American Innovation, which has a mission to, among other things, make recommendations to the President on policies and plans aimed at improving federal government operations and services. In doing so, the office is to consult with both OMB and the Office of Science and Technology Policy.[15] Further, in May 2017, the administration established the American Technology Council, which has a goal of helping to transform and modernize federal agency IT and how the federal government uses and delivers digital services. The Federal CIO and the United States Digital Service Administrator are members of this council.[16]
- **Implementing the President's Management Agenda.** In March 2018, the administration issued the "President's Management Agenda," an effort to modernize the government in three key areas—IT modernization; data, accountability, and transparency; and the workforce of the future—to push change across the federal

[15]The White House Office of Science and Technology Policy provides the President and others within the Executive Office of the President with advice on the scientific, engineering, and technological aspects of the economy, national security, homeland security, health, foreign relations, the environment, and the technological recovery and use of resources, among other topics.

[16]The United States Digital Service is an office within OMB which aims to improve the most important public-facing federal digital services.

government. According to the President's Management Agenda, modern IT must function as the backbone to how government serves the public in the digital age. The agenda also identified three priorities that are to guide the administration's efforts to modernize federal IT: (1) enhance mission effectiveness by improving the quality and efficiency of critical services, including the increased use of cloud-based solutions; (2) reduce cybersecurity risks to the federal mission by leveraging current commercial capabilities and implementing cutting edge cybersecurity capabilities; and (3) build a modern IT workforce by recruiting, reskilling, and retaining professionals able to help drive modernization with up-to-date technology.

By law, OMB is to oversee federal agencies' management of information and information technology.[17] Within OMB, primary responsibility for oversight of federal IT resides with the Administrator of the Office of E-Government and Information Technology, who also serves as the Federal CIO.[18] According to OMB, this oversight responsibility covers about 591 major and 8,054 non-major IT investments across the federal government.[19] As a part of its oversight responsibilities, the Office of E-Government and Information Technology 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:

[17]40 U.S.C. §§ 11302, 11303 (*Clinger-Cohen Act*); 44 U.S.C. § 3504 (*Paperwork Reduction Act*); 44 U.S.C. § 3602 (*E-Government Act*); 44 U.S.C. § 3553 (*Federal Information Security Modernization Act of 2014,* which largely superseded the *Federal Information Security Management Act of 2002)*.

[18]OMB's Office of E-Government and Information Technology's IT management responsibilities were established by the *E-Government Act of 2002* (44 U.S.C. § 3602).

[19]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.

- **Establishing the 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. Currently, the Federal IT Dashboard displays information on the cost, schedule, and performance of nearly 800 major IT investments at 26 federal agencies.[20] In addition, agencies are to submit ratings from their CIOs to the Dashboard, which, according to OMB's instructions, should reflect the level of risk facing an investment relative to that investment's ability to accomplish its goals. The public display of these data is intended to allow OMB, other oversight bodies, and the general public to hold agencies accountable for mission-related outcomes. Over the past nine years, we have issued a series of reports that have 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, as well as issues with the accuracy and reliability of the data it contains.[21] Accordingly, we have made recommendations to OMB to address these issues.
- **Guiding PortfolioStat sessions.** To better manage existing IT systems, in 2012 OMB launched the PortfolioStat initiative. PortfolioStat requires agencies to conduct an annual, agency-wide portfolio review to, among other things, reduce commodity IT spending and demonstrate how their IT investments align with the agency's mission and business functions. In 2014 and 2015, OMB's PortfolioStat guidance also called for it and agencies to identify high-

[20]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.

[21]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).

impact IT programs that merited additional support and oversight by OMB and/or agency leadership, and for these programs to be discussed during a PortfolioStat session. The 2015 guidance, however, changed the frequency of the PortfolioStat sessions from annually to quarterly, and the level of participation to no longer require attendance by the federal CIO or the agency's deputy secretary.

- **Identifying high-priority IT programs.** In December 2014, Congress stated in its explanatory statement accompanying the Consolidated and Further Continuing Appropriations Act, 2015 that OMB was to identify the top 10 high-priority IT programs under development in the federal government and report on their status quarterly.[22] OMB reported on these high-priority IT programs in June 2015 and June 2016.[23] Additionally, in December 2015, in an explanatory statement accompanying the Consolidated Appropriations Act, 2016, Congress stated that the U.S. Digital Service, a component of OMB, was to provide a quarterly status report on its current projects, including the top 10 high-priority programs.[24] In response, the U.S. Digital Service issued reports in December 2016 and July 2017.[25] Further, in November 2017, we issued a report that included three recommendations to OMB for enhancing the oversight of high-priority programs and continuing to report on both these programs and U.S. Digital Service projects.[26] As of May 2020, OMB had not yet addressed these recommendations.
- **Issuing guidance on incremental software development.** OMB has issued guidance on incremental software development—one approach to reducing the risks from broadly-scoped, multiyear projects.[27] An incremental development approach delivers software products in smaller modules with shorter time frames. Agile

[22]160 Cong. Rec. H9736 (daily ed. Dec. 11, 2014).

[23]OMB, *Quarterly Report to Congress: 10 High Priority Programs Quarterly Report* (Washington, D.C.: June 25, 2015) and *Report to Congress: 10 High Priority Programs* (Washington, D.C.: June 9, 2016).

[24]161 Cong. Rec. H10137 (daily ed. Dec.17, 2015).

[25]OMB, U.S. Digital Service, *Report to Congress - 2016* (Washington, D.C.: December 2016) and *Report to Congress* (Washington, D.C.: July 2017).

[26]GAO, *Information Technology: OMB Needs to Report On and Improve Its Oversight of the Highest Priority Programs*, GAO-18-51 (Washington, D.C.: Nov. 21, 2017).

[27]See OMB, *Management of Federal Information Resources*, Circular No. A-130 Revised, Transmittal Memorandum No.4 (Washington, D.C.: Nov. 28, 2000).

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.[28] 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. For many years, we have issued various reports on the status of agencies' efforts to implement incremental development and the challenges related to improving federal IT acquisitions through the use of incremental development.[29]

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.[30] 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.

[28]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.

[29]GAO, *Information Technology: Critical Factors Underlying Successful Major Acquisitions*, GAO-12-7 (Washington, D.C.: Oct. 21, 2011); *Information Technology: Agencies Need to Establish and Implement Incremental Development Policies*, GAO-14-361 (Washington, D.C.: May 1, 2014); GAO-16-469; and GAO-18-148.

[30]GAO, *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-Making*, GAO/AIMD-10.1.13 (Washington, D.C.: Feb. 3, 1997); *Information Security: Further Actions Needed to Address Risks to Bank Secrecy Act Data*, GAO-09-195 (Washington, D.C.: Jan. 30, 2009); *Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy*, GAO-12-903 (Washington, D.C.: Sept. 11, 2012); *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, GAO-11-605 (Washington, D.C.: Jul. 28, 2011).

- **Information security 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 project/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 meet customer demands in the near future.

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. These acquisitions include IT systems that have a significant impact on the United States’ national security interests, such as those that support terrorism-related screening; foreign relations, such as those that collect and record information on foreign students and exchange visitors; the economy, such as those that process taxes; and public health, such as those that are intended to provide universal health care records, among other things. Table 1 provides a summary of the acquisitions selected and the agencies that are responsible for them.

Table 1: Federal Agency Mission-Critical Information Technology Acquisitions

Department of Agriculture	Modernize and Innovate the Delivery of Agricultural Systems
Department of Commerce	2020 Decennial Census*
Department of Defense	Defense Healthcare Management System Modernization* Global Combat Support System-Army*
Department of Homeland Security	Student and Exchange Visitor Information System Modernization* U.S. Citizenship and Immigration Services Transformation*
Department of the Interior	Automated Fluid Minerals Support System II*
Department of Justice	Next Generation Identification System Terrorist Screening System
Department of State	Consular System Modernization
Department of Transportation	Automatic Dependent Surveillance-Broadcast
Department of the Treasury	Customer Account Data Engine 2* Integrated Enterprise Portal*
Department of Veterans Affairs	Electronic Health Record Modernization*
Small Business Administration	Application Standard Investment
Social Security Administration	Disability Case Processing System 2*

Legend: *= Acquisition relates to a programmatic area that GAO has previously designated as being high risk.

Source: GAO analysis of agency data. | GAO-20-249SP

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. Our most recent work highlighted, for example, the progress made for the 2020 Decennial Census; the extent to which the U.S. Citizenship and Immigration Services Transformation project has met schedule and cost goals; challenges related to the implementation of the Automated Fluid Minerals Support System; and the system configuration process for the Department of Veterans Affairs (VA) Electronic Health Record Modernization.

As previously stated, in 2015 we identified improving the management of IT acquisitions and operations as a high-risk area, which means the program or operation that the acquisition supports is vulnerable to fraud, waste, abuse, and mismanagement, or in need of transformation. In addition to this high risk area, 10 of the 16 acquisitions and the programs they support relate to an additional programmatic area that GAO has

previously designated as being high risk.[31] These areas include the 2020 Decennial Census, Department of Defense business systems modernization, strengthening Department of Homeland Security's management functions, ensuring the effective protection of technologies critical to U.S. national security interests, management of federal oil and gas resources, enforcement of tax laws, managing risks and improving VA health care, VA acquisition management, and improving and modernizing federal disability programs.

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 personally identifiable information (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. Nearly all of the acquisitions, 15 of the 16, will use PII to meet the purpose of the acquisition.[32] Fourteen of the acquisitions will also store PII.

OMB and the U.S. Digital Service have recognized many of the acquisitions in their high-priority programs reports in 2015, 2016, and 2017. These reports highlighted IT programs under development that OMB or the U.S. Digital Service identified to be of high priority for oversight and high impact to the public. Specifically, OMB identified five of the 16 selected acquisitions in 2015 and six of the 16 in 2016. The U.S. Digital Service identified four of the 16 in 2016 and two of the 16 in 2017. One of the acquisitions, the U.S. Citizenship and Immigration Services Transformation, was recognized in all four reports.

At times, a major IT project's cost, schedule, and performance goals—known as a baseline—need to be modified to reflect new circumstances. While these changes—generally referred to as rebaselining—can be done for valid reasons—including, for example, changes in a project's objectives, scope, requirements, or funding stream—they can also be

[31]Each acquisition profile identifies the relevant high-risk report number. More information on our high-risk list can be found at https://www.gao.gov/highrisk/overview.

[32]We included the 2020 Decennial Census technical integrator contract in this count. Although the technical integrator contract itself does not use or store PII, the key system the contractors will be integrating will use and store PII.

used to mask cost overruns and schedule delays. Eleven of the 16 selected acquisitions were rebaselined during their development. Agencies reported a number of reasons as to why their acquisitions were rebaselined. Ten agencies reported delays in defining the cost, schedule, and scope; one agency reported budget cuts and hiring freezes; four agencies reported technical challenges; and five agencies reported changes in development approach as a cause for rebaselining.[33]

The amount agencies expect to spend on the selected acquisitions vary 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. Agencies reported potential cost savings associated with 13 of the 16 mission-critical acquisitions after deployment. In general, these agencies reported that they expect cost savings and cost avoidance due to a number of factors. Six agencies reported expected cost savings as a result of multiple legacy systems being shut down, and two agencies reported expected cost savings from the use of cloud-based capabilities. Seven agencies cited improved efficiencies in streamlined processes as an expected savings in costs, while three agencies cited the elimination of physical paper processing as the source of expected cost savings. Three agencies also reported that they expected cost savings through improving security, monitoring, and management.[34]

The respective agencies reported that seven of the 16 acquisitions are expected to be fully deployed within the next 2 years or had been deployed during the time of our review, while the agencies for five of the selected acquisitions could not provide a final expected full deployment date. The officials for these agencies stated that a final deployment date could not be determined because of the iterative nature of the Agile software development processes being used. With this type of iterative development approach, agencies deploy functionality on an ongoing basis, rather than delivering all functionality at one time, such as the waterfall approach. Officials of two agencies also stated that the

[33]Some agencies cited multiple reasons for rebaselining, so one agency may be reflected multiple times in the total count shown.

[34]Some agencies cited multiple factors for reporting cost savings and cost avoidance, so one agency may be reflected multiple times in the total count shown.

Coronavirus Disease 2019 pandemic had delayed their development and deployment timelines.

Agencies have a variety of options when developing or acquiring IT systems. Thirteen of the 16 acquisitions used a combination of development solutions, including customized software development by agency personnel, contractor developed software, commercial off-the-shelf software and platform solutions, and open source software.[35] Most of the agencies were using an incremental system development lifecycle methodology, such as Agile. Specifically, 13 of the 16 acquisitions are governed by an Agile or other type of incremental systems development lifecycle methodology, while six use a more traditional waterfall approach.[36]

Agencies identified several risk factors for their acquisitions. These risk factors related to the categories of risk we previously discussed. Agencies identified the risk of not implementing the acquisition for eight of the 16 acquisitions as high risk. The second most identified high risk area was information privacy, which was identified for four of the 16. Agencies identified cost and budget as a moderate risk for nine of the 16 acquisitions, and the second most identified moderate risk areas were schedule and organizational—eight of the 16 acquisitions. Agencies identified information security risk for seven of the 16 acquisitions as low risk, and the second most identified low risk areas were organizational, information privacy, and technical—six of the 16 acquisitions each.

Agencies also reported that they faced several challenges in effectively implementing these acquisitions. For example, agencies reported that workforce issues, technical challenges, schedule slippages, inadequate funding, and budget constraints occurred during the development stage. In addition, according to agency officials for 12 of the 16 acquisitions, they faced workforce issues including contract transitions, inadequate skills among contract staff, or delays in onboarding contractor and federal support that challenged the successful implementation of the acquisitions. In addition, nine of the 16 acquisitions faced technical challenges such as transitioning to a cloud environment, unexpected complexity of the

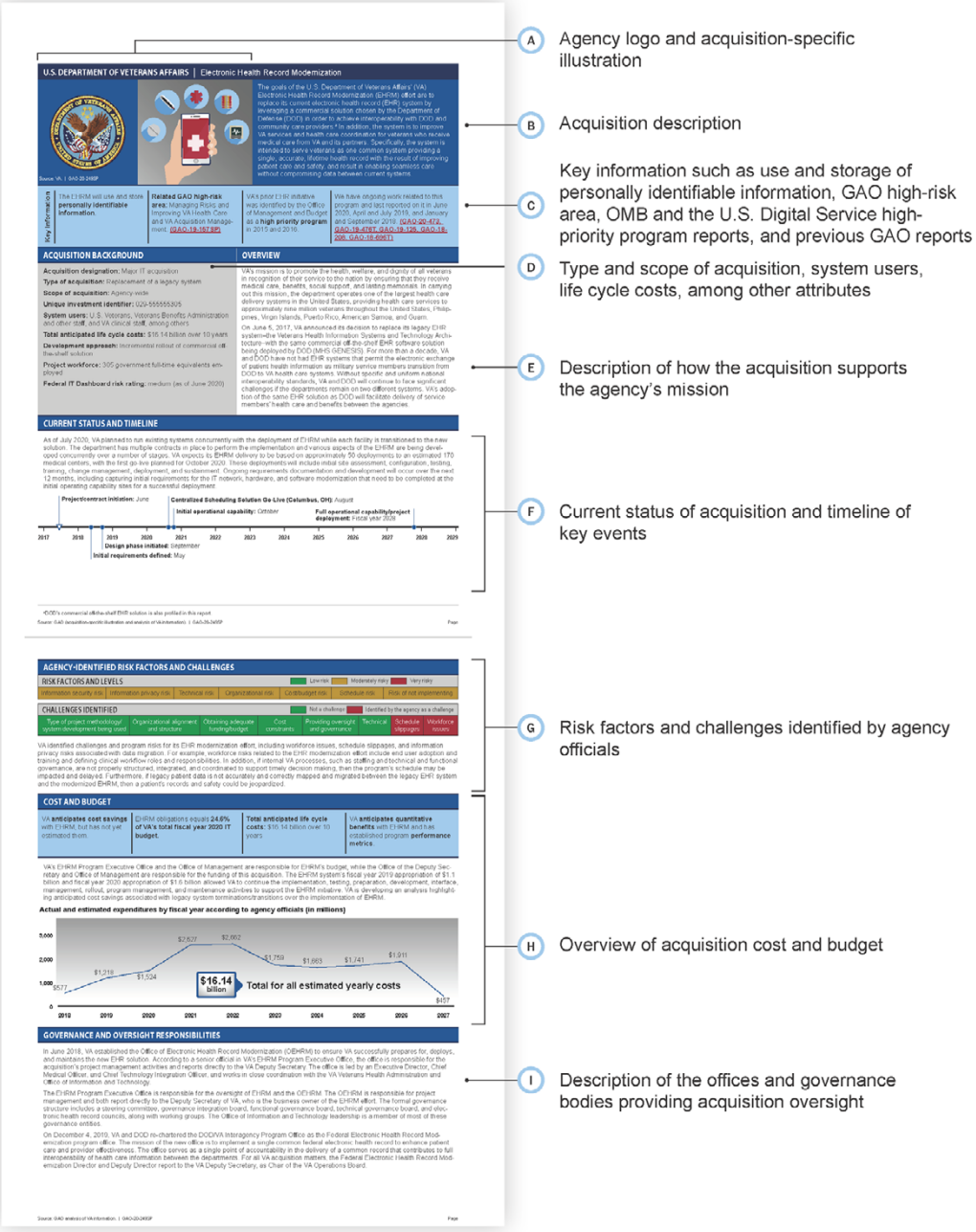
[35]Commercial off-the-shelf software is sold in substantial quantities in the commercial marketplace and is purchased without modification, or with minimal modification, to its original form.

[36]One acquisition, the 2020 Decennial Census technical integrator contract, is not a systems development acquisition.

system, and cybersecurity vulnerabilities. According to agencies, ten of the 16 acquisitions faced challenges with schedule slippages due to, for example, changes in the acquisition's strategy for development, contract delays, and hiring freezes. Lastly, eight of the 16 acquisitions faced cost constraints or challenges in obtaining funding due to, for example, budget cuts and outdated code complexities that required more resources to solve than the agency initially estimated.

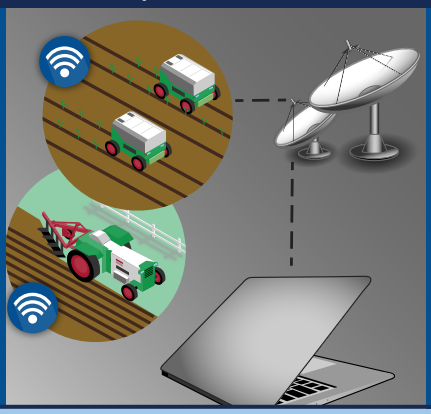
The following section contains profiles of the 16 mission-critical IT acquisitions that we selected and reviewed, grouped by federal departments and agencies, in alphabetical order. The profiles and the data presented in this report reflect key attributes of the selected federal IT acquisitions as of August 2020, unless otherwise noted. Each profile presents an overview of the acquisition, its current status, and its life cycle cost estimates, among other information. Figure 1 provides an illustration of the layout of each profile. The agency profiles follow the figure.

Figure 1: Illustration of Acquisition Profile



Source: GAO | 20-249SP

U.S. DEPARTMENT OF AGRICULTURE | Modernize and Innovate the Delivery of Agricultural Systems



Source: USDA. | GAO-20-249SP

The goal of the Modernize and Innovate the Delivery of Agricultural Systems (MIDAS) program is to streamline and automate farm program processes by replacing obsolete hardware and software. This acquisition is an enhancement to an existing system that is intended to improve accuracy and participation in the Farm Service Agency's (FSA) benefits program by providing farmers and ranchers the flexibility to visit any county FSA office to update their information for farm benefits. It is also to link with FSA's web-based systems to allow the sharing of farm and customer information among U.S. Department of Agriculture (USDA) component agencies, reduce duplication of data entries and, thereby, increase data integrity while preserving customer privacy and security.

Key Information

- MIDAS will use and store **personally identifiable information**.
- MIDAS is currently being used as the system of record and entry for farm records.
- MIDAS was **rebaselined** in 2015 due to timeline and cost changes and in 2017 due to cost reduction.
- We have ongoing work related to this program and last reported on it in June 2015 and July 2011. **(GAO-15-506, GAO-11-586)**

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Enhancement to an existing system

Scope of acquisition: FSA, Risk Management Agency, Natural Resources Conservation Service, and National Agricultural Statistics Service

Unique investment identifier: 005-000001870

System users: 9,900 during peak use

Total anticipated life cycle costs: $567.96 million over 12 years

Development approach: Waterfall and incremental development using contractor-developed software and commercial off-the-shelf software

Project workforce: Not yet determined

Federal IT Dashboard risk rating: low (as of June 2020)

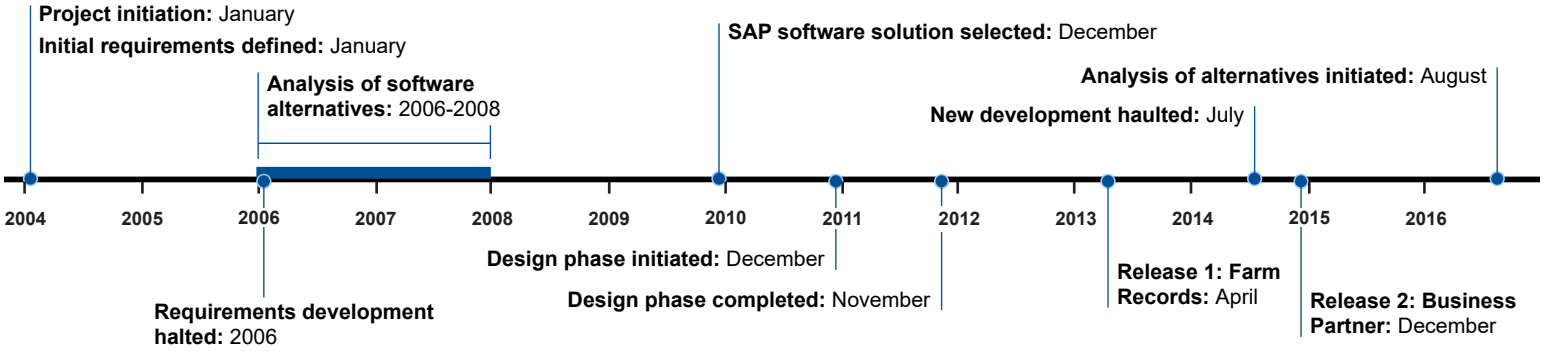
OVERVIEW

USDA manages benefit programs that support farm and ranch production, natural resources and environmental conservation, and rural development. FSA is one of three USDA service center agencies that manage benefit programs for farmers and ranchers.[a] It currently manages 23 farm benefit programs, which range from providing emergency assistance for livestock, honeybees, and farm-raised fish to providing incentives for resource conservation.

Over the last two decades, FSA has provided services to customers supporting the farm benefit programs at its approximately 2,100 local offices. To participate in an FSA program, a customer may need to visit the local service center office multiple times throughout the year because certain transactions cannot be performed electronically. In early 2004, FSA began planning the MIDAS program to streamline and automate farm program processes and to replace obsolete hardware and software. However, the agency has experienced significant challenges in managing this program. After halting the development of MIDAS in 2006, FSA changed its approach from acquiring customized software to acquiring commercial off-the-shelf enterprise resource planning software in 2009 and delivering the project in increments.

CURRENT STATUS AND TIMELINE

In July 2014, the Secretary of Agriculture halted any new development on MIDAS after two software releases due to concerns with the program's performance and delays in defining the cost, schedule, and scope for the remaining elements of MIDAS. In 2016, FSA began an analysis of alternatives to determine recommendations for the best path forward for existing MIDAS applications. FSA officials said that the analysis was still underway as of May 2020. FSA continues to maintain the MIDAS application with incremental improvements to existing functionality.



[a]The other two agencies are the Natural Resources Conservation Service, which administers programs that provide funding to landowners and other partners, and Rural Development, which offers business loans and grant programs for rural development.

Source: GAO (acquisition-specific illustration and analysis of USDA information). | GAO-20-249SP

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS — Agency deemed not applicable | Low risk | Moderately risky | Very risky

Risk of not implementing	Schedule risk	Information security risk	Technical risk	Organizational risk	Cost/budget risk	Information privacy risk

CHALLENGES IDENTIFIED — Not a challenge | Identified by the agency as a challenge

Organizational alignment and structure	Type of project methodology/ system development being used	Providing oversight and governance	Obtaining adequate funding/budget	Cost constraints	Schedule slippages	Technical	Workforce issues

USDA identified several program risks and challenges with regard to MIDAS. For example, the agency's *MIDAS Acquisition Plan* identified the risk of pilferage and exposure of personally identifiable information. Further, according to USDA, if this acquisition were terminated before the enhancement work was completed, MIDAS would not maintain interoperability with other components of FSA's technical architecture, which would directly impact its ability to access customer data in service centers and deliver daily customer services. According to USDA, the Farm Production and Conservation's Information Solutions Division is working to identify the best platforms, solutions, and strategies that will maximize effective use of limited IT budgets by eliminating redundant costs, improve customer service with modern IT solutions, and produce faster increased-value delivery of mission critical capabilities, such as the Farm Bill enablement.

COST AND BUDGET

USDA has not determined if there will be cost savings associated with MIDAS.

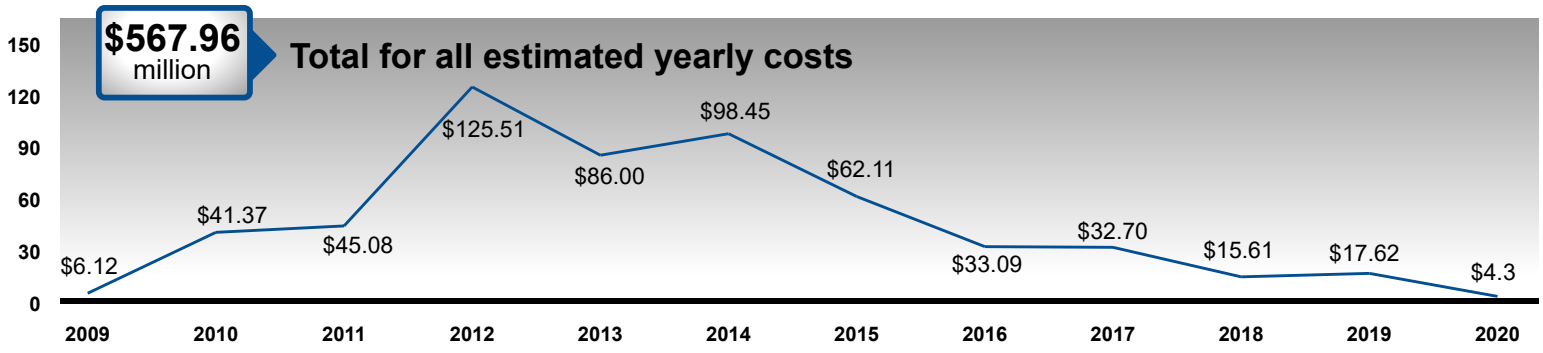
MIDAS obligations equal **0.2% of USDA's total fiscal year 2020 IT budget.**

Total anticipated life cycle costs: $567.96 million over 12 years

USDA **anticipates quantitative benefits with MIDAS** and has established program performance metrics.

USDA's Office of Budget and Program Analysis is responsible for the budget for MIDAS, while FSA is responsible for funding. USDA has not determined potential cost savings because the analysis of alternatives has not been completed; therefore, the information to determine cost savings is not available. USDA requested a fiscal year 2020 budget of $4.3 million to continue support of the MIDAS program.

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



GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

The USDA Senior Management Oversight Committee is responsible for agency-level oversight of MIDAS. Membership consists of the USDA Under Secretary; USDA Chief Information Officer, USDA Chief Financial Officer, and the FSA Administrator as voting members; and the FSA Chief Information Officer, FSA Program Director, FSA Chief Financial Officer, and the Deputy Administrator for Farm Programs as non-voting members. The Senior Management Oversight Committee reviews program updates, including budget, overall timelines, and performance. The MIDAS Integrated Program Team, under the leadership of the MIDAS Program Manager, is responsible for the project management of MIDAS. FSA is partnering with Natural Resources and Conservation Services and the Risk Management Agency to develop and implement a comprehensive IT strategy.

U.S. DEPARTMENT OF COMMERCE | 2020 Decennial Census (Technical Integrator Contract)

Source: Department of Commerce. | GAO-20-249SP

Through several acquisitions that comprise the 2020 Decennial Census program, the U.S. Census Bureau (Census Bureau) is changing the way that population information is collected and managed by switching from a largely paper-based manual system to one that relies more heavily on information technology (IT). As part of the larger program, this acquisition comprises a technical integrator contract, which is to provide evaluation of the systems and infrastructure and acquisition of the infrastructure (e.g., cloud or data center) to meet the bureau's scalability and performance needs; integration of all of the systems supporting the 2020 census; and assistance with technical, performance and scalability, and operational testing activities. Mobile integration, IT security, engineering, testing, and implementation are also to be provided through this acquisition.

Key Information

The 2020 Decennial Census will use and store **personally identifiable information**.

Related GAO high-risk area: 2020 Decennial Census (GAO-19-157SP)

The 2020 Decennial Census was identified as a **high priority program** by the Office of Management and Budget in 2015 and 2016.

We have ongoing work related to this program and last reported on it in August, June, and February 2020 and October, July, May, and April 2019. (GAO-20-671R, GAO-20-551R, GAO-20-368R, GAO-20-111R, GAO-19-685T, GAO-19-399, GAO-19-431T)

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: New asset with new capabilities

Scope of acquisition: Census Bureau

Unique investment identifier: 006-000402400

Total anticipated life cycle costs: $1.4 billion over 8 fiscal years

Project workforce: 26 government full-time equivalents employed and approximately 825 full-time equivalent contract personnel

Federal IT Dashboard risk rating: medium (as of June 2020)

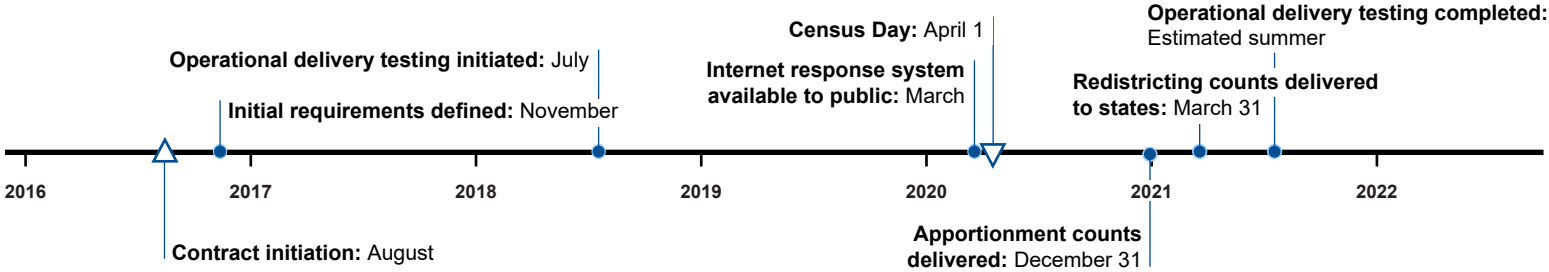
OVERVIEW

As part of the U.S. Department of Commerce, the Census Bureau's most important function is to conduct the decennial census. The Census Bureau provides vital data that are used to apportion the number of seats in Congress; supports redistricting efforts, such as defining the representative boundaries for congressional districts, state legislative districts, school districts, and voting precincts; and enforces voting rights and civil rights legislation. The Census Bureau faces the challenge of cost-effectively counting a population that is growing steadily larger, more diverse, and increasingly difficult to enumerate.

According to the Decennial Census Programs Directorate, the Census Bureau previously had disparate groups developing various applications and software to support the census program. The technical integrator team was instituted through this acquisition to integrate the 52 IT systems comprising the 2020 census system of systems. The objective of the contract is to ensure that the Census Bureau's system of systems integrates, scales, performs, is secure, and meets 2020 census business objectives. In addition, the technical integrator is to provide back-end infrastructure and support for six regional census centers, 248 area census offices, and several island area offices.

CURRENT STATUS AND TIMELINE

As of April 2020, the Census Bureau, along with the technical integrator, had performed several major operational tests, including end-to-end testing, and had deployed applications and systems for 10 of 16 planned operational deliveries for the 2020 Decennial Census. According to the Decennial Contracts Execution Office, while the Census Bureau expected to complete the remaining operational deliveries by quarter three of 2021, the delivery schedule for these operational deliveries was impacted by the Coronavirus Disease 2019 pandemic.[a] The Census Bureau planned to resume work related to these deliveries in June 2020 and was developing a revised schedule for deploying them in May 2020. These operational deliveries related to response processing, data products/dissemination, providing data for redistricting, island area census, and post enumeration survey.



[a]For further detail on how the Coronavirus Disease 2019 pandemic affected Census operations, see *GAO 2020 Census: Recent Decision to Compress Census Timeframes Poses Additional Risks to an Accurate Count,* GAO-20-671R (Washington, D.C.: Aug. 27, 2020); and *2020 Census: COVID-19 Presents Delays and Risks to Census Count,* GAO-20-551R (Washington, D.C.: June 9, 2020).

Source: GAO (acquisition-specific illustration and analysis of Department of Commerce information). | GAO-20-249SP

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk | Moderately risky | Very risky

Information security risk	Information privacy risk	Technical risk	Organizational risk	Cost/budget risk	Schedule risk	Risk of not implementing

CHALLENGES IDENTIFIED

Not a challenge | Identified by the agency as a challenge

Type of project methodology/ system development being used	Providing oversight and governance	Organizational alignment and structure	Obtaining adequate funding/budget	Cost constraints	Schedule slippages	Technical	Workforce issues

Census Bureau officials identified several challenges for this acquisition. Specifically, the Assistant Director for Decennial Census Programs, Systems and Contracts noted that the bureau would need to continue to assess contractor staffing levels to ensure that a sufficient number of staff are available to perform any additional systems testing needed for changes to upcoming census operations due to the Coronavirus Disease 2019 pandemic. We previously reported in February 2020 that schedule management challenges may compress the time available for the remaining system development and testing and increase the risk that systems will not function as intended. We have ongoing work intended to monitor the risks to the bureau's implementation of IT to support the 2020 census and its efforts to mitigate these risks.

COST AND BUDGET

According to the Census Bureau, the 2020 Decennial Census program, as currently designed, is **expected to cost $108 per housing unit** (including contingency). The bureau estimates that the 2020 Census will be the **most expensive census to date**.

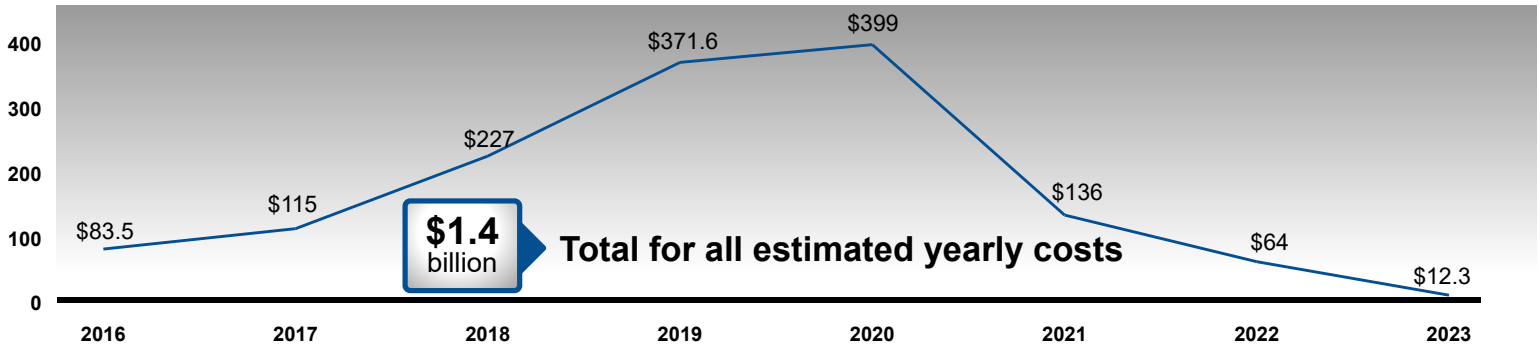
2020 Decennial Census acquisition obligations equal approximately **37.8% of the department's total fiscal year 2020 IT budget**.

Total anticipated life cycle costs: $1.4 billion over 8 fiscal years

Department of Commerce has **established performance measures and metrics** for the technical integrator contract, including cost and performance measures.

As part of the Census Bureau, the Decennial Census Program Directorate is responsible for the acquisition's budget and funding. In an August 2018 report on the 2020 Decennial Census effort, we reported that, in 2015, the Census Bureau estimated that it could conduct the census at a cost of $12.3 billion in constant 2020 dollars.[b] As a result of re-baselining in early fiscal year 2018, the 2020 cost estimate increased by over $3 billion to $15.6 billion (in current decennial time frame costs).[c] Due to budget uncertainty, the Census Bureau decided to scale back census field testing in 2017 and 2018. However, the *Consolidated Appropriations Act, 2019*, appropriated $3.551 billion for the periodic censuses and programs account. According to Census Bureau officials, this level of funding was sufficient to carry out 2020 census activities as planned at that time. However, the delays to key operations could adversely impact downstream operations, undermine the overall quality of the count, and escalate census costs.

Technical Integrator Contract actual and estimated expenditures by fiscal year according to agency officials (in millions)



GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

The Decennial Census Program Directorate is responsible for overseeing the 2020 Decennial Census IT acquisition and serves as the business owner of the effort. Led by an associate director, the Directorate also works to advise the Census Bureau's Director and Deputy Director on decennial programs. This acquisition, as well as other Census-related IT contracts, is governed, in part, by an executive steering committee and a governing board. The steering committee is to provide, for example, IT and budget management, as well as guidance in establishing program development timelines. The governing board is to govern and oversee 2020 Census efforts; approve the annual budget and changes to cost, schedule, and scope; and review risks and issues to be escalated to the steering committee, among other things. According to officials in the Decennial Census Programs Directorate, the 2020 Census Technical Integrator contract is managed by a government program manager who reports to the Chief, Decennial Contracts Execution Office. The officials added that the Decennial Contracts Execution Office serves as a participant in the Executive Steering Committee. Other governance-related functions include the 2020 Census Change Control Board, the Risk and Issue Board, Census Integration Group Meetings, Decennial Division Chief Meetings, and 2020 Census Contract and Budget Meetings.

[b]GAO, *2020 Census: Census Bureau Improved the Quality of Its Cost Estimation, but Additional Steps Are Needed to Ensure Reliability*, GAO-18-635 (Washington, D.C.: Aug. 17, 2018).

[c]According to October 2017 Department of Commerce documents, the reported figures are inflated to the current 2020 census time frame (fiscal years 2012 to 2023); the bureau had cited constant 2020 dollars for prior figures.

Source: GAO analysis of Department of Commerce information. | GAO-20-249SP

U.S. DEPARTMENT OF DEFENSE | Defense Healthcare Management System Modernization

Source: DOD. | GAO-20-249SP

The U.S. Department of Defense's (DOD) Defense Healthcare Management System Modernization (DHMSM) program was established in June 2013 to acquire and field a configurable and scalable modernized electronic health record (EHR) system called Military Health System (MHS) GENESIS.[a] The new system is intended to replace multiple legacy systems and provide an electronic integrated capability for the 54 hospitals, 377 medical clinics, and 270 dental clinics that serve 9.5 million DOD beneficiaries worldwide. The goal of the DHMSM program is to unify and increase accessibility of integrated healthcare delivery and decision making and to facilitate healthcare delivery and care.

Key Information

The DHMSM will use and store **personally identifiable information.**

Related GAO high-risk area: DOD Business Systems Modernization. (GAO-19-157SP)

DHMSM was identified by the Office of Management and Budget as a **high priority program** in 2015 and 2016.

We have ongoing work related to this program and last reported on it in August and October 2015, and July 2014. (GAO-15-530, GAO-16-184T, GAO-14-609)

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Replacement of legacy systems

Scope of acquisition: Agency-wide

Unique investment identifier: 007-000100033

System users: Approximately 158,000 clinical end users for 9.5 million beneficiaries

Total anticipated life cycle costs: $10.21 billion over 21 years

Development approach: Waterfall system development using commercial off-the-shelf software

Project workforce: 113 government full-time equivalents employed and approximately 363 full-time equivalent contract personnel

Federal IT Dashboard risk rating: medium (as of June 2020)

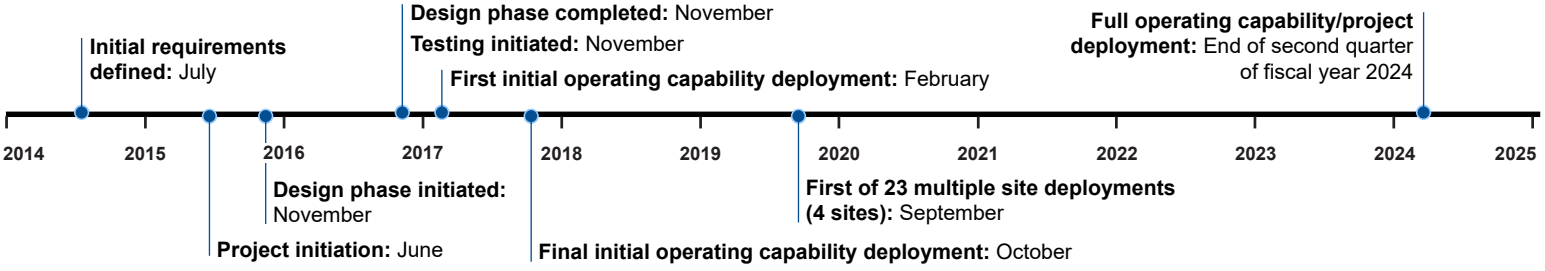
OVERVIEW

One important mission of DOD is providing and maintaining readiness for medical services and support to members of the military services, including during military operations. For more than a decade, DOD has attempted to modernize its health care system to permit interoperable transference and sharing of service members' electronic health information with other entities, such as the Department of Veterans Affairs, commercial providers, and other healthcare practitioners. Historically, patient health information has been scattered across paper records and electronic records kept by many different caregivers in many different locations, making it difficult for a clinician to access all of a patient's health information at the time of care. Lacking access to these critical data, a clinician may be challenged in making the most informed decisions on treatment options, potentially putting the patient's health at risk. To address this, DOD acquired a commercially available EHR system to replace its existing Armed Forces Health Longitudinal Technology Application, Composite Health Care System, and Essentris inpatient systems. DOD anticipates the system to be fully implemented by the end of the second quarter of fiscal year 2024.

The DHMSM Program Manager anticipates that the modernized EHR will include benefits, such as increased capacity, reduction in duplicate medical tests and turnaround time on results, improved patient safety and clinical effectiveness, improved medication reconciliation and reduced adverse drug reactions, improved medical records and document storage, and improved readiness. DOD medical staff plan to use the EHR to inform their delivery of medical services, including enroute care, dentistry, emergency department, health, immunization, laboratory, radiology, operating room, pharmacy, vision, audiology, and inpatient/outpatient services. In addition, medical staff are to use the EHR to perform administrative support, front desk operations, logistics, and business intelligence.

CURRENT STATUS AND TIMELINE

As of May 2020, DOD had completed project initiation, defined initial requirements, initiated the design phase, and begun operational tests and evaluations for DHMSM. As of July 2020, DOD was in the implementation phase of the program and plans to have it fully implemented and operational by the end of the second quarter of fiscal year 2024. According to the DHMSM Program Manager, full implementation and deployment will begin once all designated initial operating capability sites have completely transitioned to the EHR system and no longer rely on legacy systems for day-to-day operations. The program deployed MHS GENESIS at its first initial operating capability site in February 2017 and its final initial operating capability site in October 2017. DOD plans to deploy MHS GENESIS in 23 additional multiple site deployments by the end of the second quarter of fiscal year 2024.



Source: GAO (acquisition-specific illustration and analysis of DOD information). | GAO-20-249SP

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk | Moderately risky | Very risky

Technical risk	Organizational risk	Information security 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

Type of project methodology/ system development being used	Organizational alignment and structure	Cost constraints	Schedule slippages	Technical	Providing oversight and governance	Obtaining adequate funding/budget	Workforce issues

DOD identified risk factors and challenges related to DHMSM, including shared governance, obtaining adequate resources, and workforce issues. For example, DHMSM's Program Executive Office identified DOD and VA program and operations shared governance as a potential program risk. The officials in the Program Executive Office within Defense Healthcare Management Systems stated that the lack of a joint, multi-faceted, structured, functional, and technical VA and DOD governance plan at the enterprise level puts DOD at risk of execution failures, as well as cost, schedule, and performance delays. In addition, the DHMSM Program Management Office noted that, if it does not obtain the necessary government and contractor resources to support the current deployment model, then it will not be able to provide adequate oversight of DHMSM during deployments. In addition, according to the DHMSM Program Manager, the DHMSM Program Management Office is facing challenges in filling open personnel positions.

COST AND BUDGET

DOD anticipates a significant **return on investment** and **$87 million in cost savings** with DHMSM.

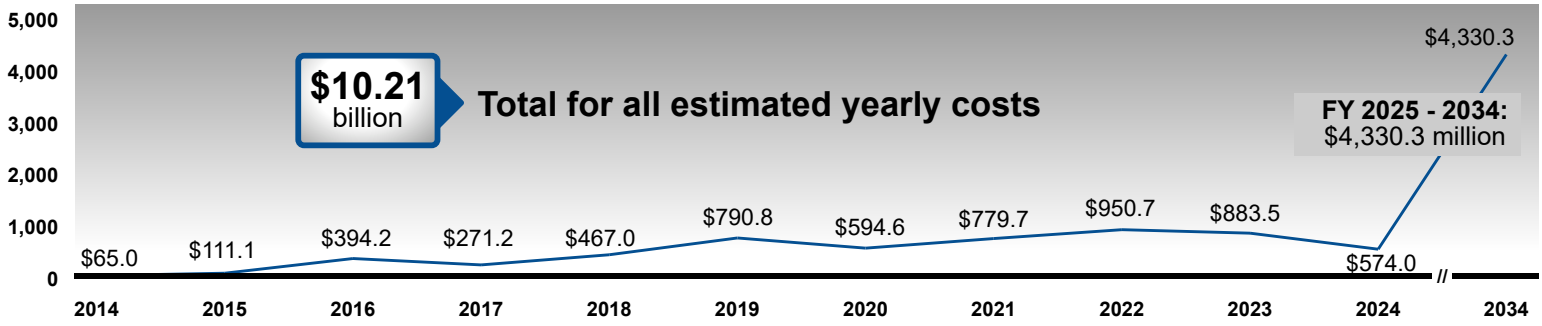
DHMSM obligations equals **1.6% of DOD's total fiscal year 2020 IT budget.**

Total anticipated life cycle costs: $10.21 billion over 21 years

DOD **anticipates quantitative benefits** with DHMSM and has established **program performance metrics.**

DOD's Defense Health Agency, Program Executive Office within Defense Healthcare Management Systems and the DHMSM Program Management Office are responsible for the program's budget, and share funding responsibility with the Office of the Under Secretary of Defense for Acquisition and the Assistant Secretary for Defense for Acquisition. DOD conducted a return on investment analysis that compared the alternative (sustainment of legacy systems) to the DHMSM life cycle costs plus cost of status quo parallel operations while legacy systems were phased out. The result was that there would be a significant return. Specifically, once MHS GENESIS is fully deployed, annual costs were estimated to be $87 million less than continuing the sustainment and maintenance of the legacy systems. Additionally, the analysis concluded that efficiency and effectiveness gains associated with MHS GENESIS would outweigh the costs and result in a positive return on investment.

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



GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

DOD's Assistant Secretary of Defense for Acquisition and the Program Executive Office, Defense Healthcare Management Systems are responsible for the oversight of DHMSM, while the DHMSM Program Management Office is responsible for the project management of the acquisition. The Defense Health Agency is the business owner. The DHMSM governance structure includes acquisition oversight and functional support. The DOD Senior Stakeholders Group (co-chaired by the Under Secretary of Defense for Acquisition and Sustainment and Assistant Secretary of Defense (Health Affairs)) provides strategic recommendations and direction for DHMSM. In addition, the Program Executive Office, Defense Healthcare Management Systems receives approval from the functional sponsor, the Assistant Secretary of Defense (Health Affairs).

The Department of Defense Chief Information Officer (CIO) is a chartered member of the DOD Electronic Health Records Senior Stakeholders Group and Defense Healthcare Management Systems Configuration Steering Board. As a chartered member, the DOD CIO provides senior oversight, strategic recommendations, and direction on health-related acquisition programs. The DOD CIO is also part of the Configuration Steering Board, which is responsible for reviewing proposed changes to program requirements or system configurations with potential impacts to program cost or schedule, and for ensuring that the changes are consistent with program objectives.

On December 4, 2019, DOD and VA re-chartered the DOD/VA Interagency Program Office as the Federal Electronic Health Record Modernization program office. The mission of the new office is to implement a single common federal electronic health record to enhance patient care and provider effectiveness. The office serves as a single point of accountability in the delivery of a common record that contributes to full interoperability of health care information between the departments. For all DOD acquisition matters, the Federal Electronic Health Record Modernization Director and Deputy Director report to the Under Secretary of Defense for Acquisition and Sustainment.

[a]VA also plans to move from its customized Veterans Health Information Systems and Technology Architecture platform to the Electronic Health Record Modernization system–the same commercial off-the-shelf solution as MHS Genesis. The VA's EHR solution is also profiled in this report.

Source: GAO analysis of DOD information. | GAO-20-249SP

U.S. DEPARTMENT OF DEFENSE | Global Combat Support System-Army

Source: DOD. | GAO-20-249SP

The U.S. Department of Defense's (DOD) Global Combat Support System-Army (GCSS-Army) is part of the Army's ongoing transition to modernize its enterprise IT resource planning systems. The goal of the transition to the new system is to provide a single source of data for management and decision-making, as well as to improve overall financial management and audit readiness. GCSS-Army is to replace several information systems that support the logistics functions of supply, maintenance, and property accountability that are performed by tactical units at multiple locations. According to the GCSS-Army Project Manager, modernizing these systems will enhance combat effectiveness and ensure warfighting readiness.

Key Information

The GCSS-Army will use and store **personally identifiable information**.

Related GAO high-risk area: DOD Business Systems Modernization. (GAO-19-157SP)

GCSS-Army is intended to **replace several legacy systems**.

We have ongoing work related to this program and last reported on it in April 2015. (GAO-15-378R)

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Replacement of several legacy systems and adding a component to the existing system

Scope of acquisition: U.S. Army

Unique investment identifier: 007-000005070

System users: Currently 69,000 using GCSS-Army and another 51,000 after deployment

Total anticipated life cycle costs: $3.3 billion over 13 years

Development approach: Incremental development using multiple approaches, including customized software developed by agency personnel, contractor developed software, and commercial off-the-shelf software

Project workforce: 14 government full-time equivalents employed and 281 full-time equivalent contract personnel

Federal IT Dashboard risk rating: low (as of June 2020)

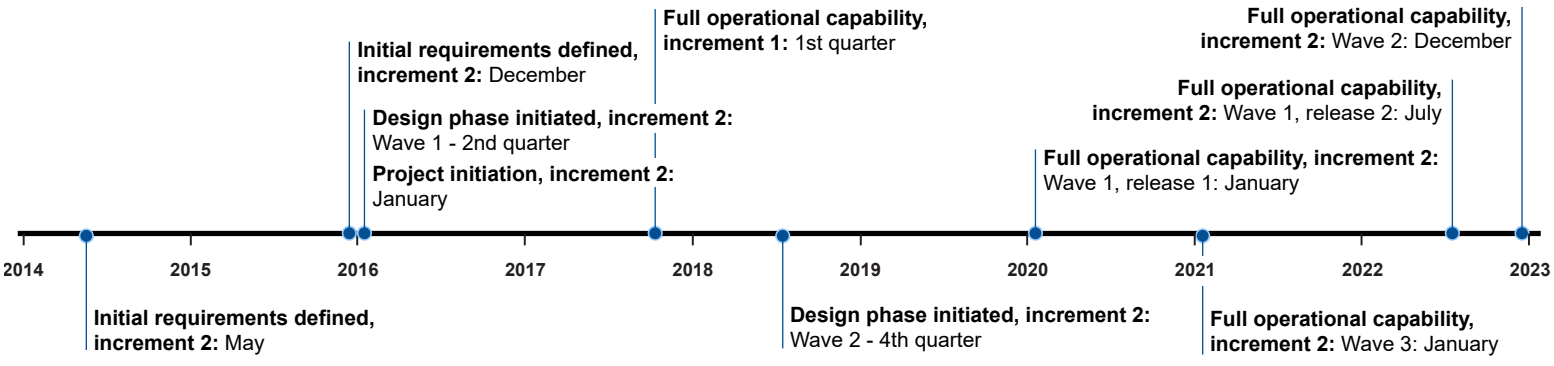
OVERVIEW

The lack of accurate and timely information in the management of Army logistics operations has been a long-standing issue at DOD. We have previously reported that the Army experienced challenges in maintaining visibility of military materials and equipment during the redeployment of forces from Operation Desert Storm. Based on a review of those challenges, the Army identified the need for a standard management information system that used a common database capable of anticipating, allocating, and synchronizing the flow of resources. To address this need, in 1995, the Army undertook a comprehensive management initiative to fully integrate the functional areas of supply, distribution, and maintenance in order to provide logisticians better visibility of military material and equipment. The initiative included developing an Army-specific information management system. However, it changed course in 2003 and selected a commercial off-the-shelf software solution, GCSS-Army, which is to be implemented in two increments. DOD completed increment one during the first quarter of fiscal year 2018 and, as of May 2020, was in the process of developing increment two.

GCSS-Army will replace several information systems that support the logistics functions of supply, maintenance, and property accountability, and are performed by tactical units at multiple locations. These systems, once integrated, are intended to provide a single source of data for management and decision-making, as well as to improve overall financial management and audit readiness.

CURRENT STATUS AND TIMELINE

GCSS-Army is to be implemented in two increments. As of May 2020, the Army had completed GCSS-Army increment one during the first quarter of fiscal year 2018, and was in the process of implementing GCSS-Army increment two, which was initiated in January 2016. Incre-



Source: GAO (acquisition-specific illustration and analysis of DOD information). | GAO-20-249SP

ment two is to have three functionally distinct waves. Wave one (Enterprise Aviation), deployed its first release in January 2020, beginning the interface of Army's current aviation logistics and maintenance information system (Aircraft Notebook) with GCSS-Army. The second release for wave one is intended to complete the interface of Aircraft Notebook with GCSS-Army and is scheduled to complete development and testing in July 2022. Wave two (Business Intelligence/Business Warehouse), scheduled for completion in December 2022, is to provide Combatant Commanders and senior leaders near-real time visibility of combat power by providing aviation readiness and Army prepositioned stocks data from GCSS-Army into reports and visualizations, among other things.[a] Wave three, scheduled for fielding in January 2021, is to replace the Army's legacy system used to maintain and manage current Army prepositioned stocks worldwide.

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk | Moderately risky | Very risky

Organizational risk	Information security risk	Information privacy risk	Technical risk	Risk of not implementing	Cost/budget risk	Schedule risk

CHALLENGES IDENTIFIED

Not a challenge | Identified by the agency as a challenge

Type of project methodology/ system development being used	Organizational alignment and structure	Workforce issues	Cost constraints	Schedule slippages	Providing oversight and governance	Technical	Obtaining adequate funding/budget

The Army identified several risk factors for this acquisition, including workforce hiring, testing, and cleansing corrupt or inaccurate data. For example, their integrator's workforce has faced challenges recruiting capable GCSS-Army and integrator experts. However, as of May 2020, Army reported that it had obtained capable integrator experts for the acquisition. Army also identified potential testing risks, such as software errors and redundant testing activities that could delay operational testing for all three releases. As a result, Army noted that it is looking to reduce redundant integration and testing activities by utilizing Agile testing methodologies. There is also a shared risk of corrupt and incomplete data among the numerous system owners, including GCSS-Army, that share and transfer data. Further, in April 2020, Army revised their technical approach for the GCSS-Army increment two, wave one solution, assisting the Program Office in minimizing these technical risks.

COST AND BUDGET

DOD **anticipates over $14 billion in financial benefits** with GCSS-Army through fiscal year 2027.

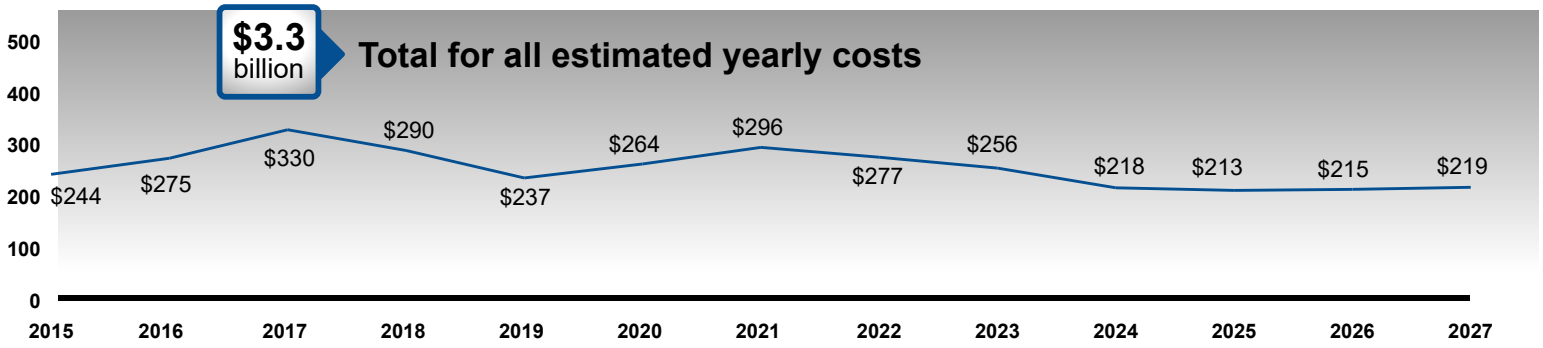
GCSS-Army obligations equal **0.7% of DOD's total fiscal year 2020 IT budget.**

Total anticipated life cycle costs: $3.3 billion over 13 years

DOD **anticipates cost avoidance and productivity improvements** with GCSS-Army.

The Army Budget Office and Army Deputy Chief of Staff are responsible for the GCSS-Army budget, while the Assistant Secretary of the Army (Acquisition, Logistics, and Technology) and the Army Deputy Chief of Staff are responsible for the funding of this acquisition. According to Army's Test and Audit Technical Management Division, it expects to achieve a total estimated savings of about $1.1 billion, cost avoidances of $2.2 billion, and productivity improvements of $10.6 billion with the implementation of GCSS-Army increment one and another $500 million in financial benefits for increment two.

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



GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

According to the GCSS-Army Project Manager, the Program Executive Office for Enterprise Information Systems and the Assistant Secretary of the Army (Acquisition, Logistics and Technology) are responsible for the oversight of this acquisition, and they share project management responsibilities with the Project Manager of the Army Enterprise Systems Integration Program. The business owners are the Deputy Chief of Staff, Army Training and Doctrine Command Capabilities Manager-Aviation Brigade, and Army Combined Arms Support Command. According to Army's Test and Audit Technical Management Division, in August 2019, the GCSS-Army increment one product office merged organizations with the GCSS-Army increment two product office in an effort to realize efficiencies and maintain cohesion between the two organizations. As a result of this merger, the established, formal governance structure for GCSS-Army increment one has been adopted for development of increment two.

[a]Army prepositioned stocks are strategically-placed caches of warfighting equipment afloat and ashore that provide speed of response for geographic combatant commanders to execute operation plans and conduct contingency operations.

Source: GAO analysis of DOD information. | GAO-20-249SP

U.S. DEPARTMENT OF HOMELAND SECURITY | Student and Exchange Visitor Information Systems Modernization

Source: DHS. | GAO-20-249SP

The purpose of the Student and Exchange Visitor Information Systems (SEVIS) Modernization acquisition is to modernize and maintain the legacy system run by the U.S. Department of Homeland Security (DHS) to collect and record information on foreign students, exchange visitors, and their dependents throughout the duration of their approved stay in the U.S. education system. The modernization effort was initiated in order to address technical vulnerabilities identified in 2006. In May 2019, DHS determined that the work completed to mitigate the vulnerabilities had been successful and approved the program to use the acquisition for adaptive maintenance for future improvements.

Key Information

- SEVIS will use and store **personally identifiable information**.
- **Related GAO high-risk area:** Strengthening DHS Security management functions. (GAO-19-157SP)
- SEVIS was **rebaselined** in 2018 due to contracting delays and technical issues.
- We last reported on this program in March 2019 and July 2012. (GAO-19-297, GAO-12-895T)

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Enhancement to an existing system

Scope of acquisition: Agency-wide

Unique investment identifier: 024-000005363

System users: 18,000 government users; 44,000 program employee users; 1.5 million active F, M, and J status holders and dependents

Total anticipated life cycle costs: $182 million over 5 years

Development approach: Customized development by agency personnel

Project workforce: 18 government full-time equivalent positions and 54 full-time equivalent contract personnel

Federal IT Dashboard risk rating: low (as of June 2020)

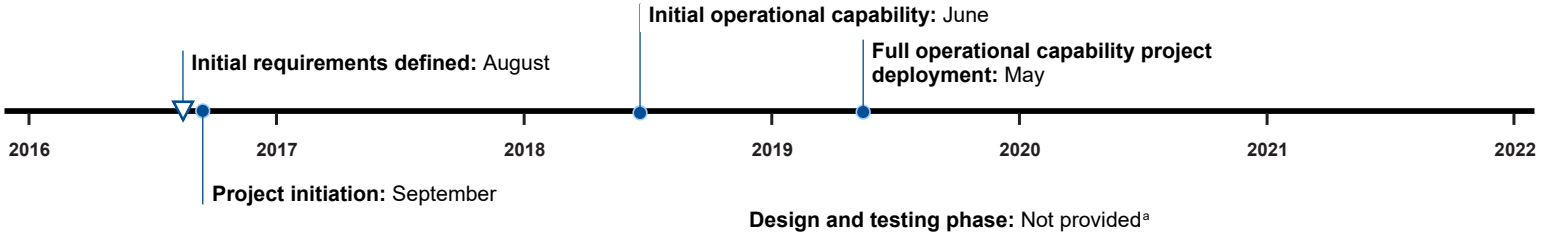
OVERVIEW

Within DHS, U.S. Immigration and Customs Enforcement (ICE)'s mission is to protect the United States from cross-border and immigration-related crime that may threaten national security and public safety. The Student Exchange Visitor Program, a program within ICE, was established to manage the oversight of foreign students and exchange visitors (that is, nonimmigrants), their dependents, and schools. SEVIS is a web-based system used to maintain information on foreign students who are participating in the U.S. education system or exchange visitor program.

In 2006, an independent evaluation identified 14 Student Exchange Visitor Program vulnerabilities. To address these vulnerabilities, DHS set out to replace SEVIS, but, because of schedule and cost delays, did not complete this replacement. Subsequently, DHS determined that the majority of the vulnerabilities could be mitigated through stabilizing and updating the existing system through the SEVIS Modernization acquisition. In May 2019, the DHS Acquisition Review Board determined that the efforts to mitigate vulnerabilities resulted in a stable, reliable, and satisfactory system and that continued modernization efforts were no longer required. Moving forward, ICE will use adaptive maintenance for future improvements to SEVIS.

CURRENT STATUS AND TIMELINE

ICE was authorized by the Acquisition Review Board, through this acquisition, to use adaptive maintenance for additional improvements that advance system performance to further mitigate the remaining two vulnerabilities—person-centric and paper certificates of eligibility vulnerabilities. The person-centric vulnerability is the inability to track an individual nonimmigrant and ensure accurate matching of interface data. The paper certificate of eligibility vulnerability is the reliance on paper forms in immigration processing. According to the SEVIS Program Management Office, to address these vulnerabilities, the SEVIS modernization effort will focus on enhancing searching algorithms and work with external stakeholders to implement a totally paperless process at the port of entry and improve interfaces that will allow timely access to electronic records.



[a]According to agency officials, a date for the design and testing phase could not be provided due to the iterative and ongoing nature of the acquisition's development.

Source: GAO (acquisition-specific illustration and analysis of DHS information). | GAO-20-249SP

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk | Moderately risky | Very risky

Technical risk	Information security risk	Organizational risk	Information privacy risk	Risk of not implementing	Schedule risk	Cost/budget risk

CHALLENGES IDENTIFIED

Not a challenge | Identified by the agency as a challenge

Organizational alignment and structure	Providing oversight and governance	Obtaining adequate funding/budget	Type of project methodology/ system development being used	Cost constraints	Schedule slippages	Technical	Workforce issues

DHS identified a number of program risks and challenges, including workforce and cost constraints, while implementing enhancements to SEVIS. For example, according to the ICE Program Manager, SEVIS has experienced workforce issues, such as delays in onboarding, and schedule slippages because of contract delays. Further, a lack of federal staffing to support SEVIS has caused challenges in keeping up with oversight duties, which could potentially lead to poor technical performance, schedule slips, and cost growth. In addition, the SEVIS Program Manager reported cost challenges when migrating SEVIS to the ICE cloud, which caused greater hosting costs than initially estimated. In addition, SEVIS has also experienced budget constraints due to the fee-funded nature of the project.[b] Specifically, according to the SEVIS Program Manager, delays in fee increase approvals could impact the ability to fund SEVIS.

COST AND BUDGET

DHS **anticipates cost avoidance** by mitigating vulnerabilities on its legacy system and avoiding costs on new equipment and software.

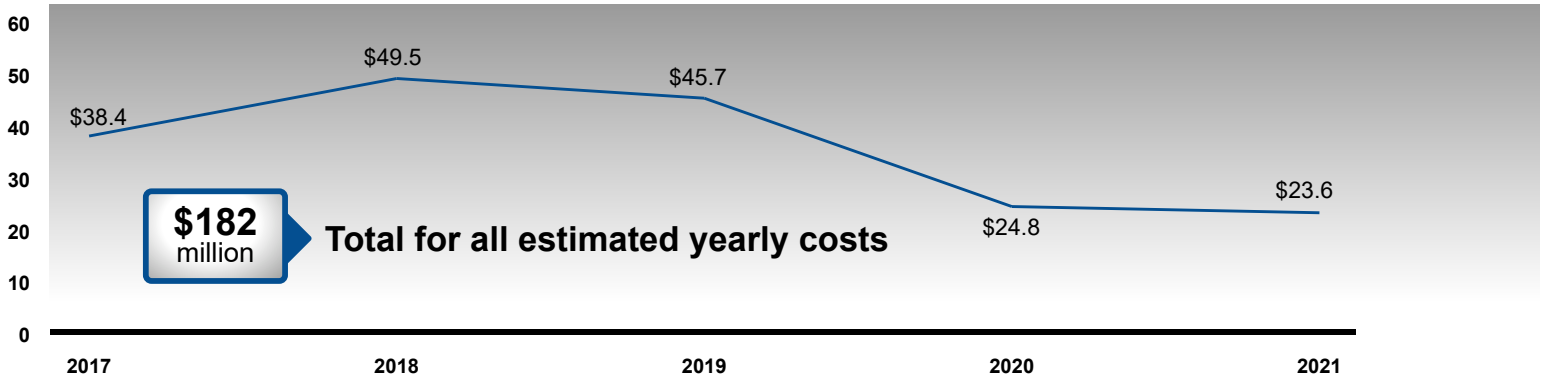
SEVIS obligations equal **0.3% of the total fiscal year 2020 DHS IT budget.**

Total anticipated life cycle costs: $182 million over 5 years

DHS **anticipates quantitative benefits** with SEVIS, including improved reliability and auditability.

Homeland Security Investigations, National Security Investigations Division, and the SEVIS program, in cooperation with the ICE Office of the Chief Information Officer, are responsible for managing the funding for the SEVIS Modernization program. According to ICE officials, the SEVIS program avoided the reconstruction of new software by mitigating vulnerabilities via the current legacy system and using existing technologies from Customs and Border Protection.

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



GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

The Homeland Security Investigations Executive Steering Committee and the ICE Component Acquisition Executive are responsible for the oversight of SEVIS. The mission of the steering committee is to provide effective governance, oversight, and guidance to the SEVIS program and is comprised of various members including the DHS and ICE chief information officers and the ICE chief acquisition officer. The Component Acquisition Executive is the senior acquisition official within the component who provides acquisition and program management oversight, policy, and guidance to ensure statutory, regulatory, and higher-level policy requirements are fulfilled. The ICE Program Manager is responsible for the development, modernization, enhancement, and infrastructure support for the program. According to ICE, the Chief Information Officer has the ability to halt the work under SEVIS if it is not performing as intended.

[b]Nonimmigrant foreign students and exchange visitors must generally pay a SEVIS fee, which helps to support the system and its program office. See 8 U.S.C. § 1372(e); 8 C.F.R. § 214.13.

Source: GAO analysis of DHS information. | GAO-20-249SP

U.S. DEPARTMENT OF HOMELAND SECURITY (DHS) | U.S. Citizenship and Immigration Services Transformation

Source: DHS. | GAO-20-249SP

The goal of the U.S. Department of Homeland Security's (DHS) U.S. Citizenship and Immigration Services (USCIS) Transformation program is to modernize the current paper-based immigration benefits process, enhance national security and system integrity, and improve customer service and operational efficiency. The Transformation program, established in 2006, is a digital modernization program that is to streamline and enhance USCIS immigration benefits processing operations by addressing processing inefficiencies and transform its historically paper-based system into an electronic account-based system. Since its inception, we have reported that the program has faced management and development challenges, limiting its progress and ability to achieve its goals.

Key Information

Transformation will use and store **personally identifiable information**.

Related GAO high-risk area: Strengthening DHS management functions. (GAO-19-157SP, and GAO-17-317)

Transformation was identified by OMB and the U.S. Digital Service as a **high priority program** in 2015, 2016, and 2017.

USCIS Transformation was **rebaselined** various times from 2015 to 2018 due to a number of factors, including changes in development approach and business process and reorganization efforts.

We last reported on this program in December 2019, May 2018, March 2017, September 2016, and July 2016, among others. (GAO-20-170SP, GAO-18-339SP GAO-17-486T, GAO-16-828, GAO-16-467)

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: A new asset with new capabilities and replacement of multiple legacy systems

Scope of acquisition: USCIS

Unique investment identifier: 024-000003015

System users: USCIS, Immigration and Customs Enforcement

Total anticipated life cycle costs: $3.19 billion over 30 years

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

Project workforce: 49 government full-time equivalents employed and at least 200 developer contractor staff

Federal IT Dashboard risk rating: low (as of June 2020)

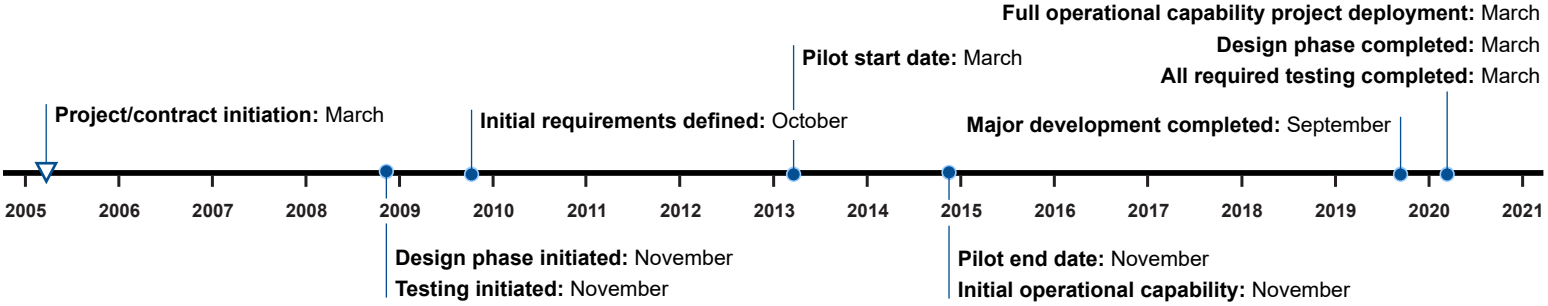
OVERVIEW

Within DHS, the mission of USCIS is to administer the nation's lawful immigration system. Part of USCIS's mission is to provide accurate information while ensuring the integrity of the U.S. immigration system and adjudicating requests efficiently and fairly. USCIS receives approximately eight million applications, petitions, and other benefit requests (collectively referred to as benefit request forms) annually from individuals seeking immigration and non-immigration benefits. USCIS has historically received paper-based applications for adjudication and relied on a complex paper-based process to execute its mission.

According to USCIS officials, the Transformation program is intended to streamline and enhance USCIS case processing operations by delivering digital capabilities and services through the USCIS Electronic Immigration System (ELIS). ELIS is an internal electronic case management system for electronically filed benefit request forms and certain paper forms. In addition, the Transformation program will continue expanding digital capabilities and services through ELIS in order to achieve business outcomes such as reducing the processing times for applications and petitions (lead time), reducing the time for case adjudications (cycle time), decreasing the reliance on paper (cost avoidance), and increasing the number of cases digitally processed in ELIS (agency workload). DHS also expects ELIS to link to other agency systems, such as those belonging to the Departments of Justice and State, for data sharing and security purposes.

CURRENT STATUS AND TIMELINE

The Transformation program has two projects in progress (Citizenship and Immigrant). The objectives of the Citizenship project are to enhance the ELIS platform with additional capabilities to support digital processing of naturalization and citizenship product lines. The objectives of the Immigrant project are to enhance the ELIS platform with additional capabilities to support digital processing of Lawful Permanent Resident and Family-based Adjustment of Status workload. USCIS has been able to decommission 12 systems due to replacement by the Transformation program, including the Reengineered Naturalization Application Casework System, the USCIS Legacy Electronic Filing System, and the Electronic Immigration System (Legacy ELIS).



Source: GAO (acquisition-specific illustration and analysis of DHS information). | GAO-20-249SP

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk | Moderately risky | Very risky

Risk of not implementing	Technical risk	Schedule risk	Information security risk	Organizational risk	Cost/budget risk	Information privacy risk

CHALLENGES IDENTIFIED

Not a challenge | Identified by the agency as a challenge

Providing oversight and governance	Obtaining adequate funding/budget	Cost constraints	Organizational alignment and structure	Type of project methodology/ system development being used	Schedule slippages	Technical	Workforce issues

USCIS identified a number of program risks and challenges related to the Transformation program. For example, in 2017, the Transformation program was re-baselined due to management and development challenges that limited its progress and ability to achieve its goals. These included workforce issues, such as contracting transitions and the lack of skills among contract staff; schedule slippages due to changes in the acquisition strategy and development approach; organizational challenges due to organizational restructuring; and technical challenges stemming from the transition to a cloud environment.

COST AND BUDGET

DHS anticipates $2 million in **cost savings**.

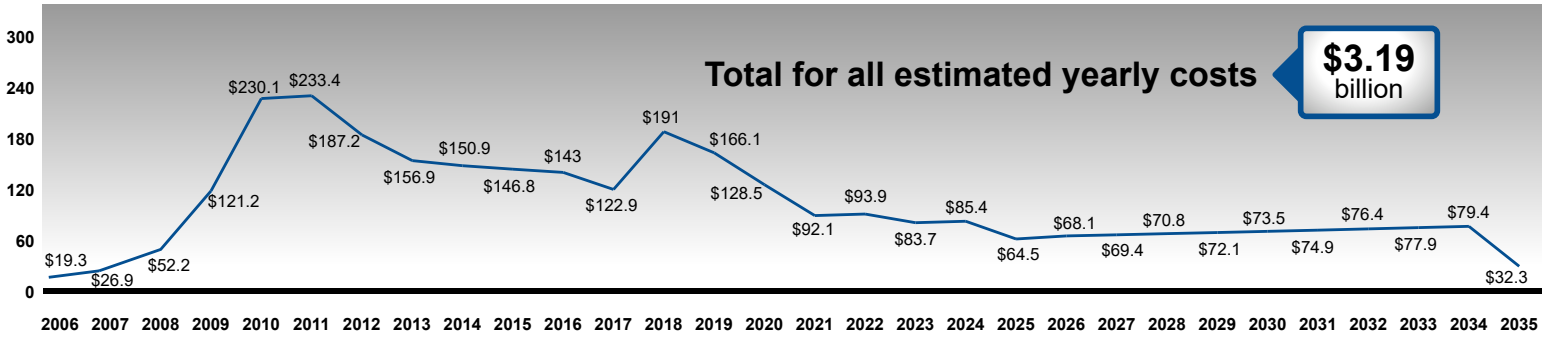
Transformation obligations equal **1.8% of DHS's total fiscal year 2020 IT budget.**

Total anticipated life cycle costs: $3.19 billion over 30 years

DHS has established **performance metrics** and **anticipates quantitative benefits** from the Transformation program.

The DHS Office of the Chief Financial Officer is responsible for the budget and funding for the Transformation program, which had a budget of $166.1 million for fiscal year 2019 and $128.5 million for fiscal year 2020. According to USCIS officials in the Office of Information Technology for the Transformation Delivery Division, cost avoidances are expected by reducing the use of Amazon Web Services, automating the startup and shutdown of Amazon Web Services, and by a reduction in costs associated with paper-based processing of applications/petitions throughout the entire life cycle (i.e., initial ingestion, processing, transfer, and storage).

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



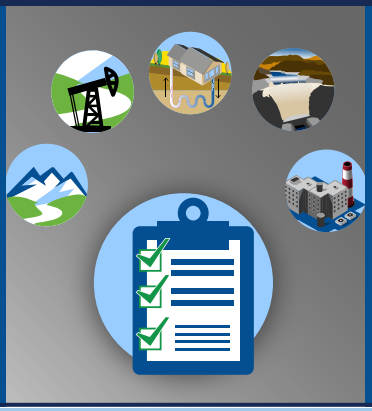
GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

The Transformation program incorporates a multi-tiered governance model. Tier 1 is a department-level governance board with quarterly Acquisition Review Board meetings chaired by the DHS Under Secretary for Management as the Acquisition Decision Authority. Tier 2 is a component-level governance board with monthly Executive Steering Committee meetings chaired by the USCIS Deputy Director as the Component Acquisition Executive. Tier 3 is a program-level governance board with bi-weekly Program Management Integrated Product Team meetings chaired by the Transformation Program Manager.

Source: GAO analysis of DHS information. | GAO-20-249SP

U.S. DEPARTMENT OF THE INTERIOR | Automated Fluid Minerals Support System II

Source: Department of the Interior. | GAO-20-249SP



The Automated Fluid Minerals Support System (AFMSS) is a Bureau of Land Management (BLM) system that facilitates collection, management, and sharing of information on authorized use of fluid minerals (i.e., oil, gas, and geothermal); regulatory well permits/reports; and field operations data across federal onshore operations on public lands. According to BLM's AFMSS Project Manager, AFMSS II is to modernize AFMSS and provide standardized electronic processes across BLM that will benefit both government and industry users by allowing electronic processing of permits, notifications, and reports for fluid mineral development across 700 million acres of federal mineral estate. This acquisition is intended to eventually replace AFMSS.

Key Information

The AFMSS II will use and store **personally identifiable information**.

Related GAO high-risk area: management of federal oil and gas resources. (GAO-19-157SP)

AFMSS was **rebaselined** in 2016 due to a number of factors, including change of scope and technical challenges.

We have ongoing work related to this program and last reported on it in March 2020, May 2018, and April 2017. (GAO-20-329, GAO-18-250, GAO-17-307)

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Replacement of a legacy system and both an enhancement and component to an existing system

Scope of acquisition: BLM

Unique investment identifier: 010-000000086

System users: 4,500 federal and industry users, including non-government user accounts that may be associated with permits, notices, reports, or other items in AFMSS

Total anticipated life cycle costs: $52.2 million over 10 years

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

Project workforce: Approximately 40 government employees with partial duties and a lesser number of full-time equivalent contract personnel

Federal IT Dashboard risk rating: low (as of June 2020)

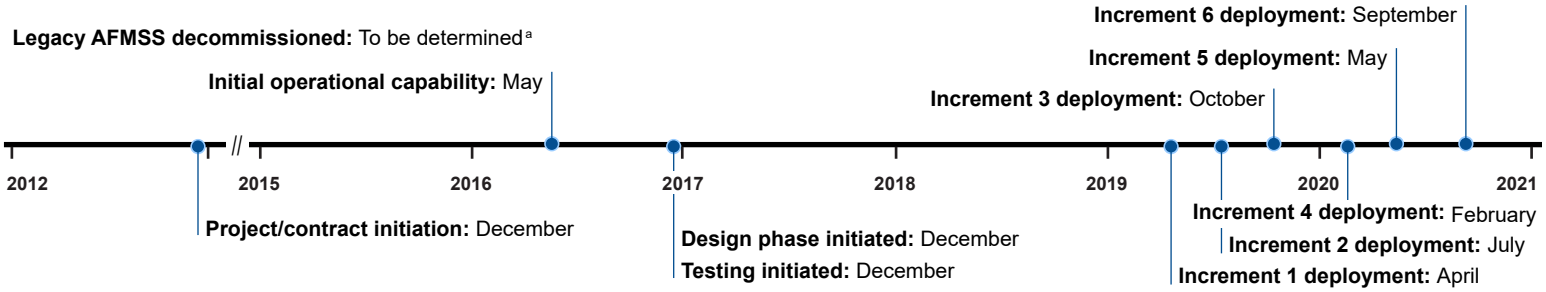
OVERVIEW

The Department of the Interior's mission, among other things, is to provide for the environmentally-sound production of oil, gas, minerals, and other resources found on the nation's public lands and to protect the lands owned by American Indians. BLM, a component agency, is responsible for managing oil and gas resources that lie under federal and private land for which the federal government retains mineral rights.

To support this responsibility, BLM uses AFMSS to maintain information on oil and gas activities on federal and Indian lands. The bureau plans to replace AFMSS with AFMSS II to address stakeholder concerns regarding the speed and transparency in oil and gas permitting and data integrity issues identified by us and the department's Office of the Inspector General. AFMSS II is to automate workflows to allow BLM to better manage its workload across all of its 33 oil and gas offices and to address the technological and business deficiencies of the legacy AFMSS. Once deployed, the system is intended to deliver standardized electronic processes that will allow an individual anywhere to complete and process permits, notifications, and reports for fluid mineral development across 700 million acres of federal mineral estate. In addition, BLM expects AFMSS II to facilitate statewide and nationwide dashboards and performance metrics, including increased agility for BLM to address shifting workloads without having to physically redeploy its workforce. As of July 2020, AFMSS and AFMSS II were operating concurrently until all replacement modules are completed and AFMSS can be decommissioned.

CURRENT STATUS AND TIMELINE

According to BLM's AFMSS Project Manager, AFMSS II is being developed in modules, which allows for easier adaptability for system enhancements based on regulatory requirements, technological changes, and other business needs. As such, all phases of development were occurring simultaneously, with testing being initiated in 2015 and the initial operating capability occurring in May 2016. However, in March 2016, the acquisition was re-baselined because of change in scope, technical challenges, and shifting of system development life cycle approaches with the system's new vendor. According to BLM's AFMSS Project Manager, as of July 2020, AFMSS II was in the design, testing,



Source: GAO (acquisition-specific illustration and analysis of Department of the Interior information). | GAO-20-249SP

development, and implementation phase per its incremental development methodology. The bureau planned to deploy the newly-developed AFMSS II on February 2020 and decommission the prior iteration of AFMSS in August 2020, but both dates have been delayed due to the Coronavirus Disease 2019 pandemic.

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk | Moderately risky | Very risky

Technical risk	Risk of not implementing	Schedule risk	Information security risk	Organizational risk	Cost/budget risk	Information privacy risk

CHALLENGES IDENTIFIED

Not a challenge | Identified by the agency as a challenge

Organizational alignment and structure	Providing oversight and governance	Obtaining adequate funding/budget	Cost constraints	Type of project methodology/ system development being used	Schedule slippages	Technical	Workforce issues

BLM identified a number of program risks and challenges in their efforts to modernize AFMSS. For example, according to BLM's AFMSS Project Manager, a staffing plan is being developed to address personnel challenges related to staff turnover, limited availability of key personnel, and the inability to hire petroleum engineers and petroleum engineer technicians. The Project Manager stated that BLM has implemented an incremental (Agile) software development methodology to address user acceptance challenges and allow for more frequent customer feedback and adjustments to customer needs and priorities.

COST AND BUDGET

BLM **anticipates cost savings** with AFMSS II, but has not yet estimated them.

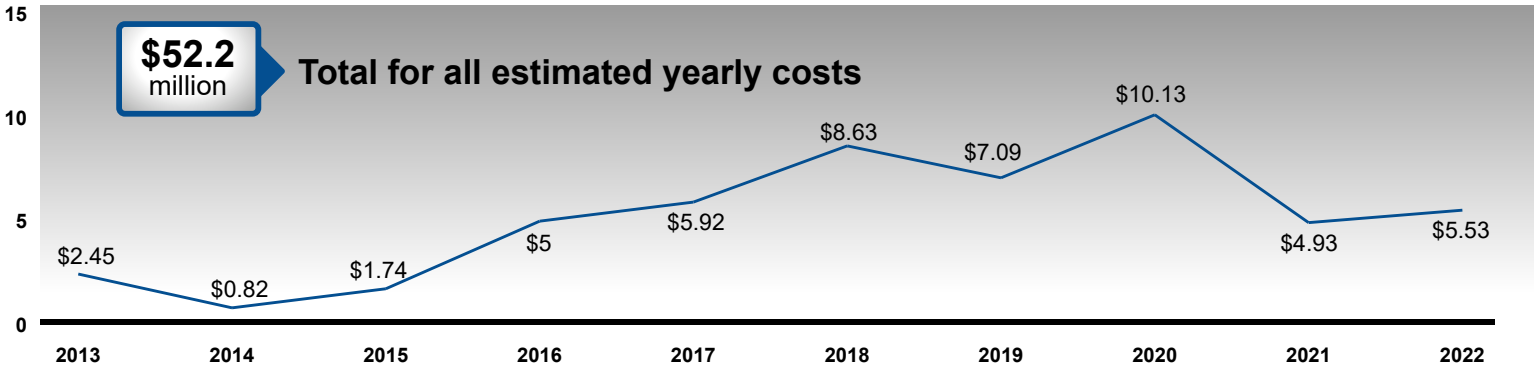
BLM's AFMSS II obligations equal **0.3% of the department's total fiscal year 2020 IT budget.**

Total anticipated life cycle costs: $52.2 million over 10 years

BLM **anticipates quantitative benefits** with AFMSS II and has established **program performance metrics**.

BLM's Energy, Minerals, and Realty Directorate is responsible for the budget and funding of AFMSS II. According to BLM's AFMSS Project Manager, the agency anticipates that the modernized system will reduce both government and industry costs by decreasing permit, notification, and reporting costs, along with reducing training costs associated with the standardization across all offices. In addition, the Project Manager stated that standardized data collection may reduce reporting costs because of reduced time spent on gathering and preparing the reports. Furthermore, flow rate calculations are being performed by hand and take hours to produce. According to BLM's AFMSS Project Manager, AFMSS II will allow for mobile inspections, which will reduce data entry by allowing an inspector to capture data on an electronic device and then upload the results to a database that will interface with AFMSS II.

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



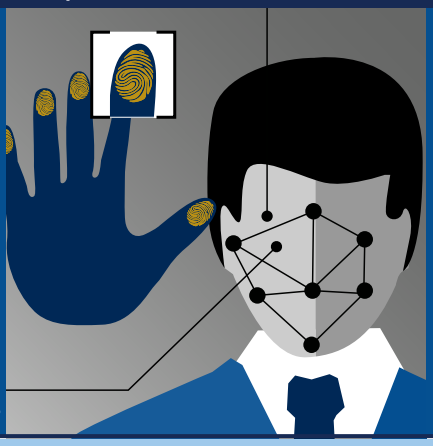
GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

According to BLM's AFMSS Project Manager, the BLM Investment Management Group is responsible for the oversight of AFMSS II, while the Branch of Project Management provides project management of the acquisition. Both groups fall under BLM's National Operations Center, which is responsible for IT. The Energy, Minerals, and Realty Directorate is the business owner and requesting office for this acquisition. The Information Technology Investment Board was established to provide acquisition governance and to ensure that an acquisition is aligned to effectively advance BLM's mission by enforcing policies, processes, and procedures. In addition, the Information Technology Investment Board is charged with providing overall governance and is considered BLM's decision-making board, while the AFMSS II Integrated Project Team is responsible for the successful implementation of the acquisition. Furthermore, OMB requests annual briefings on the AFMSS II acquisition to discuss its status of development, the system capabilities of production modules, performance measures, timelines, budget, constraints, and challenges.

[a]According to officials in the Bureau of Land Management, the Coronavirus Disease 2019 pandemic has delayed the estimated date for providing full operational capability and decommissioning the legacy AFMSS system. As of May 2020, the bureau had not yet determined a new time frame.

Source: GAO analysis of Department of the Interior information. | GAO-20-249SP

U.S. DEPARTMENT OF JUSTICE | Next Generation Identification System



Source: Department of Justice. | GAO-20-249SP

The Federal Bureau of Investigation's (FBI) Next Generation Identification (NGI) system is a continuous technical refresh initiative designed to provide authorized criminal justice and civil agencies with a range of biometric identification services and criminal history information. NGI is an incremental replacement of the Integrated Automated Fingerprint Identification System. The system comprises multiple systems and services, such as the Advanced Fingerprint Identification Technology, the Repository for Individuals of Special Concern, the Interstate Photo System, and facial recognition tools, among others.[a] NGI has been operational since 2014 and will be undergoing deployment to a cloud platform within the next three years. Officials report the NGI program will accommodate increased information processing demands for local, state, tribal, federal, and international agencies.

Key Information

The NGI system will use and store **personally identifiable information**.

NGI is the **world's largest repository** of biometric and criminal history information.

NGI is expected to maintain an average response time of 10 seconds or less for individuals of concern.

We last reported on this program in June 2019 and March 2017. **(GAO-19-579T, GAO-17-489T)**

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Enhancement to an existing system

Scope of acquisition: Agency-wide

Unique investment identifier: 011-000003457

System users: Approximately 38,084 federal, state, and tribal law enforcement users

Total anticipated life cycle costs: $1.6 billion over 14 years

Development approach: Incremental software development using multiple approaches, including a customized interface; and contractor developed, commercial off-the-shelf, and open source software

Project workforce: 68 government full-time equivalents employed and approximately 94 contract full-time equivalents

Federal IT Dashboard risk rating: medium (as of June 2020)

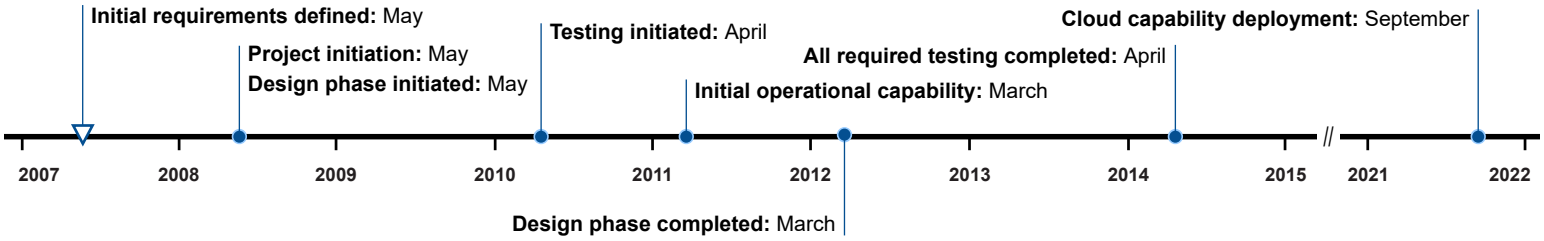
OVERVIEW

The FBI (a bureau of the U.S. Department of Justice) is developing the NGI system in order to provide key information to aid in combating violent crime, promoting safe communities, and upholding the rights of crime victims. Criminal Justice Information Services officials reported that NGI is to provide better accuracy and reduced response times for identifying individuals and any associated criminal history. The Unit Chief of the bureau's Planning and Control Unit reported that NGI is expected to maintain an average response time of 10 seconds or less for individuals of concern, four hours or less for latent fingerprint searches, 30 minutes or less for 95 percent of electronically submitted criminal fingerprint searches, two hours or less for 95 percent of electronically submitted civil fingerprint identification searches, and four hours or less to process 95 percent of facial recognition searches.

According to the Department of Justice's 2019 *IT Strategic Plan*, cloud adoption is critical to achieving the objectives for the system, and the bureau will continue to migrate systems, including NGI, to the cloud over the next three years. To this end, Criminal Justice Information Services officials stated that hosting NGI in a cloud platform will provide the bureau with on-demand computer storage resources to better meet the changing workload requirements for law enforcement.

CURRENT STATUS AND TIMELINE

According to Criminal Justice Information Services, the NGI system recently improved its algorithm search capabilities for latent prints submitted by local, state, and other federal agencies. In 2013, the FBI deployed a pilot test of iris recognition technology for NGI. Criminal Justice Information Services is moving toward an incremental development methodology for NGI, which should allow for adaptive planning, prioritization of the most valuable enhancements, and rapid responses to change. According to bureau officials, full NGI cloud adoption is scheduled for completion in September 2021.



[a]According to the FBI, individuals of special concern are wanted persons, sex offender registry subjects, known or suspected terrorists and other persons of special interest.

Source: GAO (acquisition-specific illustration and analysis of Department of Justice information). | GAO-20-249SP

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Not risky | Low risk | Moderately risky | Very risky

Technical risk	Risk of not implementing	Schedule risk	Information security risk	Organizational risk	Cost/budget risk	Information privacy risk

CHALLENGES IDENTIFIED

Not a challenge | Identified by the agency as a challenge

Providing oversight and governance	Cost constraints	Schedule slippages	Technical	Organizational alignment and structure	Obtaining adequate funding/budget	Type of project methodology/ system development being used	Workforce issues

According to officials at the FBI, Criminal Justice Information Services anticipates there could be challenges obtaining an adequate budget due to current budget constraints. Officials added that there is a shortage of qualified contractors to fill contract positions supporting operations and management as well as development for NGI. The officials attributed this challenge, in part, to overly restrictive policies that mandate contractor performance onsite at FBI facilities. In addition, Criminal Justice Information Services has faced challenges with the incremental software methodology currently being used to develop NGI's technical refresh initiative. In August 2020, the FBI Criminal Justice Information Services Division stated that they have overcome this challenge and the incremental methodology being used has increased transparency, predictability, and value delivery.

COST AND BUDGET

FBI **anticipates cost savings** with NGI, but has not yet estimated them.

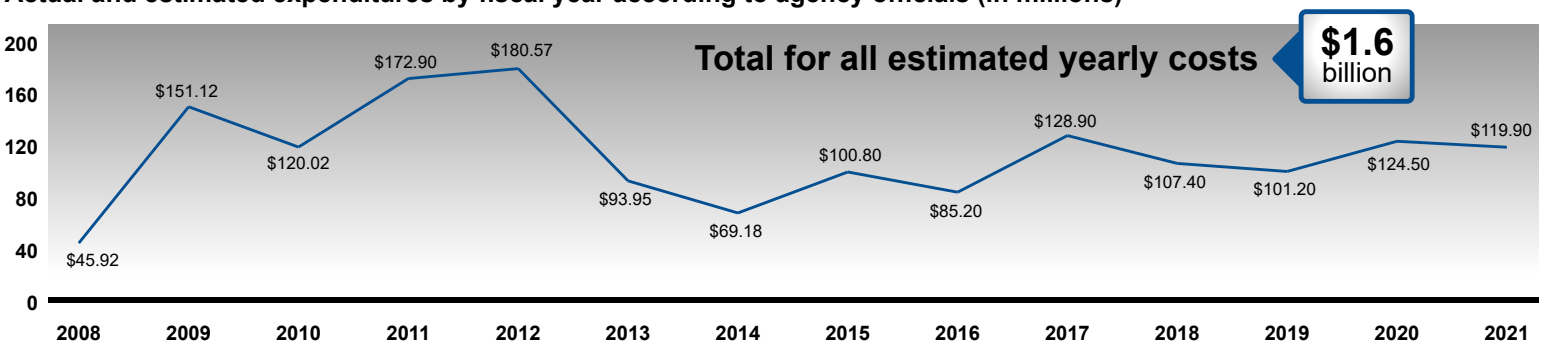
NGI obligations equal **4.0% of the department's total fiscal year 2020 IT budget**.

Total anticipated life cycle costs: $1.6 billion over 14 years

FBI **anticipates quantitative benefits** with NGI and has established **performance measures**.

The FBI's Criminal Justice Information Services division, Resource Management, Financial Management Unit, and the Planning and Control Unit are responsible for NGI's budget. Funding to support this system is a mix of direct appropriations, automation, and user fees. According to the Office of the Chief Information Officer, the NGI acquisition will allow the bureau to carry out its goal of supporting reliable and resilient IT services that maximize the use of cloud computing, modernize government-hosted applications, and securely manage systems. The bureau expects increased returns on its investments by standardizing and simplifying technology to increase efficiency by using shared services, sourcing strategically, and leveraging IT governance to increase transparency.

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



GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

According to the Planning and Control Unit Chief, the Chief Financial Officer, the Chief Acquisition Officer, and the Chief Information Officer correspond with each other regularly on major programs and work together to define the budget for the overall IT portfolio for NGI. The Criminal Justice Information Services IT Management Section's Biometric Technology Services Unit is the business owner and is responsible for project management and for operations and maintenance of NGI. Initiation and oversight of the performance of acquisitions are tracked and performed, in coordination with FBI Finance and Facilities Division Contracting Officers, by the Planning and Control Unit within the Criminal Justice Information Services IT Management section.

U.S. DEPARTMENT OF JUSTICE | Terrorist Screening System

Source: Department of Justice. | GAO-20-249SP

The Terrorist Screening System (TSS) modernization effort is a continuous technical refresh initiative designed to enhance and consolidate the main business functions of the Federal Bureau of Investigation's (FBI) Terrorist Screening Center (TSC) into one user interface.[a] The goal of this initiative is to combine the government's terrorist watch lists and applications, and to enhance search capabilities to support terrorism-related screening. TSC officials anticipate that this acquisition will provide new screening and encounter management capabilities.

Key Information

- The TSS will use and store **personally identifiable information**.
- The TSS is to perform identity resolution for known or suspected terrorist and national security threats.
- TSS was **rebaselined** in 2018 and 2019 due to an increase in scope.
- We last reported on similar efforts in May 2012. **(GAO-12-476)**

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Enhancement to an existing system

Scope of acquisition: FBI

Unique investment identifier: 011-000003177

System users: Approximately 4,000 users

Total anticipated life cycle costs: $712 million over 18 years

Development approach: Incremental software development using multiple approaches, including a customized interface, contractor developed, commercial off-the-shelf software, and open source software

Project workforce: The department could not provide information

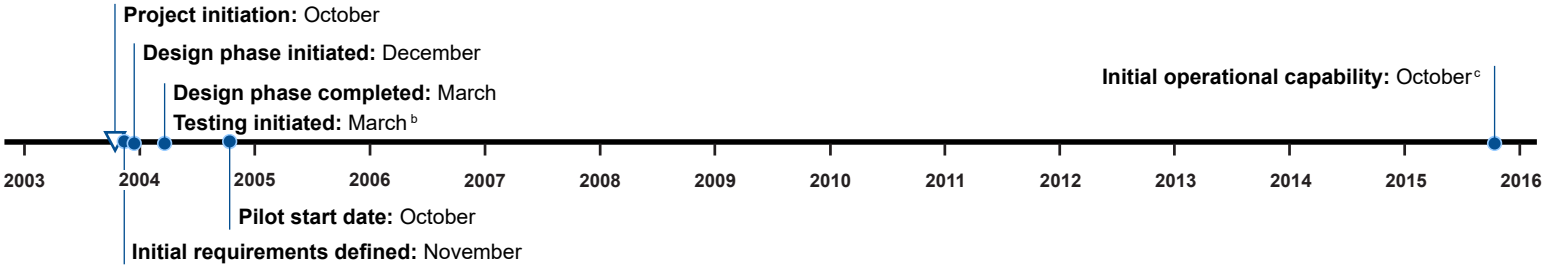
Federal IT Dashboard risk rating: Not identified (as of June 2020)

OVERVIEW

The mission of TSC is to maintain a consolidated watch list of known or suspected terrorists and to send records from the list to agencies to support terrorism-related screening. In carrying out this mission, the TSC uses many applications, such as screening databases, repositories, and automated tools, to perform identity resolution for known or suspected terrorist and national security threats. According to officials in TSC, these applications were previously separate and stand-alone—requiring multiple logins to perform job functions and additional database and server support. In 2006, TSC began efforts to combine these stand-alone applications into one unified system—TSS. TSC officials anticipate this acquisition will provide new encounter management capabilities that will allow law enforcement officers to more effectively access information in real time, such as during an encounter with a potential or known suspected terrorist. For example, according to the IT Unit Chief, an accurate, real-time no-fly list enables more secure and timely air travel both domestically and internationally.

CURRENT STATUS AND TIMELINE

According to TSC officials, several legacy systems were decommissioned between fiscal years 2017 and 2019. TSC added that production and deployments for new TSS applications and system enhancements are in a continuous development mode. The IT Unit Chief added that their IT staff continues to manage and provide technical functionality modifications for TSS—such as performance profiling and analysis; encounter viewer and editor upgrades; administrative tool upgrades; among others—which are to provide accurate screening and adherence to national privacy laws and regulation benefits.



[a]TSC is a multi-agency center administered by the FBI. It is responsible for sharing information with homeland security, law enforcement, the intelligence community, and select international partners.

[b]According to TSC officials, TSS is undergoing continuous enhancements, and therefore, could not provide a date for completion of testing.

[c]Agency could not provide a final deployment date due to the continuous nature of the acquisition's development.

Source: GAO (acquisition-specific illustration and analysis of Department of Justice information). | GAO-20-249SP

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk | Moderately risky | Very risky

Technical risk	Schedule risk	Organizational risk	Cost/budget risk	Information privacy risk	Risk of not implementing	Information security risk

CHALLENGES IDENTIFIED

Not a challenge | Identified by the agency as a challenge

Organizational alignment and structure	Obtaining adequate funding/budget	Cost constraints	Type of project methodology/ system development being used	Technical	Workforce issues	Schedule slippages	Providing oversight and governance

FBI identified several program risks in its efforts to modernize TSS. For example, one identified risk is that if the TSC IT infrastructure is not updated to address security vulnerabilities, TSC may be exposed to other vulnerabilities, such as hacker threats and TSS data not being properly updated. Furthermore, the Unit Chief also reported that, if TSC is not able to provide 24/7 support, analysts would not be able to maintain, update, or access TSS data—preventing the potential positive identification of a suspected terrorist.

COST AND BUDGET

Department of Justice **estimated at least $250,000 in cost savings** related to infrastructure and reduced system requirements.

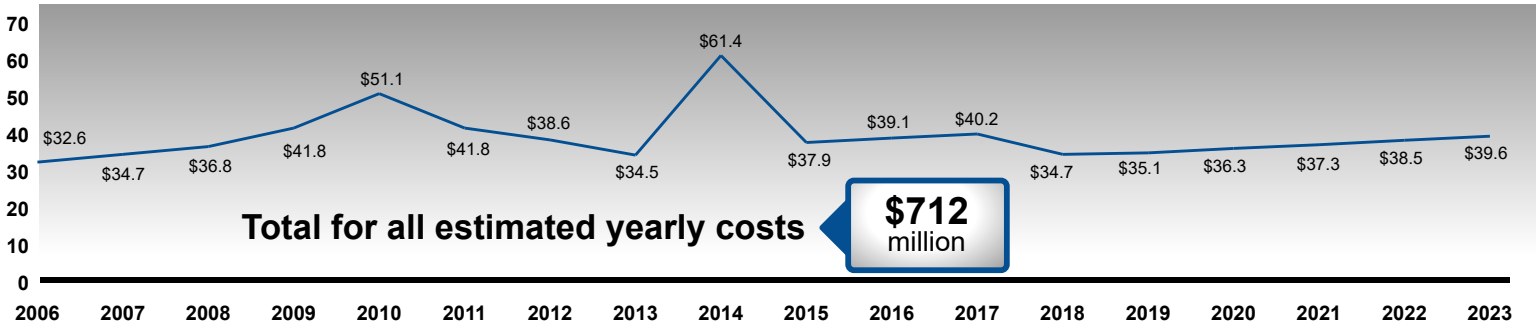
TSS obligations are **1.1% of the department's total fiscal year 2020 IT budget**.

Total anticipated life cycle costs: $712 million over 18 years

According to the Federal IT Dashboard, **benefits for this acquisition** accrue from identified terrorists and secure air travel.

TSC officials state that the FBI's National Security Branch is responsible for the budgeting and funding of TSS. According to TSC's IT Unit Chief, cost avoidance is expected with the TSS modernization effort when considering the cost of the loss of human life; the cost to replace or repair critical U.S. and international infrastructure; the cost to replicate TSS across all intelligence organizations; and the cost of multiple interfaces between organizations to ensure accurate, complete, and real-time law enforcement information sharing. According to TSC, Department of Justice's Chief Financial Officer coordinates with the Chief Information Officer and the Director of TSC for budget approval.

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



GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

TSC and Chief Information Officer are responsible for oversight of investment costs and schedule reporting of the TSS acquisition. TSC is the business owner of TSS. The Information Technology Branch and Information Technology Enterprise Services Division share project management responsibilities with the National Security Branch TSC. According to the TSC IT Unit Chief, the Office of Management and Budget was provided with monthly metrics and a risk analysis related to the TSS investment.

Source: GAO analysis of Department of Justice information. | GAO-20-249SP

U.S. DEPARTMENT OF STATE | Consular Systems Modernization

Source: State. | GAO-20-249SP

The U.S. Department of State's (State) Consular Systems Modernization (CSM) acquisition 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 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**.
- CSM was identified as a **high priority program** by the Office of Management and Budget and the U.S. Digital Service in 2015 and 2016.
- CSM was **rebaselined in 2018** due to new technologies being used.
- The Office of Inspector General last reported on this acquisition in March 2016. **(AUD-FM-16-31)**

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Replacement of a legacy system

Scope of acquisition: Agency-wide

Unique investment identifier: 014-000000032

System users: 42,000 internal users and approximately 34,000,000 external users (e.g., the public and non-Department of State government employees and contractors)

Total anticipated life cycle costs: Approximately $617.86 million over 11 years

Development approach: Incremental and Agile development using commercial off-the-shelf and customized development solutions

Project workforce: 17 government full-time equivalent personnel employed and approximately 75 full-time equivalent contract personnel

Federal IT Dashboard risk rating: medium (as of June 2020)

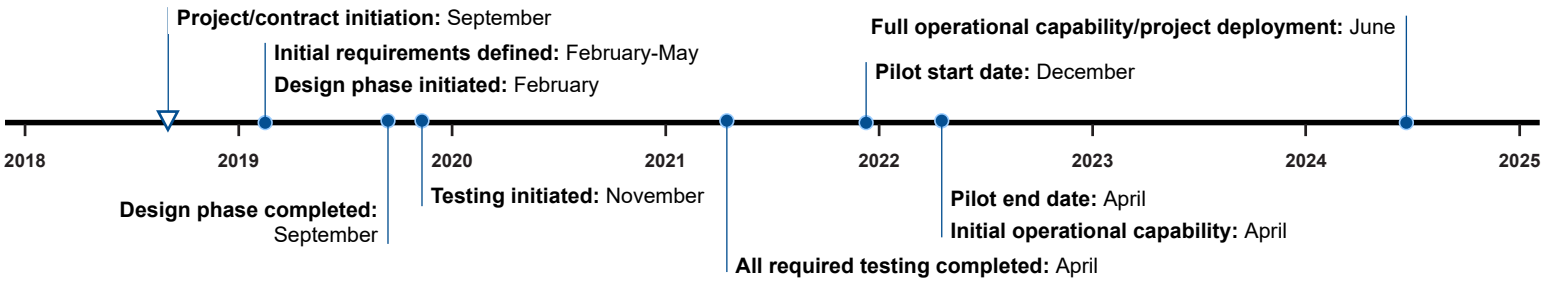
OVERVIEW

State is charged with protecting the lives and interests of U.S. citizens overseas and strengthening the security of U.S. borders. To help achieve these tasks, the department provides consular services through the Bureau of Consular Affairs. The tasks include the adjudication of visa and passport applications, protecting U.S. border security, 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, which is expected to provide a paperless processing mechanism, improved self-service options, enhanced communication, increased automation and reuse, integrated fraud detection and prevention, enhanced financial and management information data, a standardized user interface, and increased system performance. 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

The ConsularOne initiative comprises six projects for modernizing consular services. As of July 2019, the bureau had deployed activities related to the first two projects: a service that provides the public the ability to apply, pay, and schedule an appointment online for transmitting citizenship to a child born abroad and an enterprise payment service. Due to the use of an incremental development approach, Bureau of Consular Affairs officials said that, as of November 2019, the CSM acquisition and supporting ConsularOne initiative were in the design, testing, pilot, implementation, and maintenance phases. Specifically, bureau officials stated that more than one service was being developed simultaneously, and, as a result, the CSM acquisition was in various phases of the systems development life cycle. Next steps for the system are completing functionality for the first two projects, which includes a major online passport renewal release with a completion date of December 2021.



Source: GAO (acquisition-specific illustration and analysis of State information). | GAO-20-249SP

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk | Moderately risky | Very risky

Technical risk	Risk of not implementing	Schedule risk	Information security risk	Organizational risk	Cost/budget risk	Information privacy risk

CHALLENGES IDENTIFIED

Not a challenge | Identified by the agency as a challenge

Organizational alignment and structure	Providing oversight and governance	Obtaining adequate funding/budget	Cost constraints	Type of project methodology/ system development being used	Schedule slippages	Technical	Workforce issues

The Bureau of Consular Affairs identified several risks and challenges associated with the CSM acquisition. For example, acquisition delays occurred due to changes in the bureau's IT acquisition process, which added additional stages for approval of contracts from start to award. This caused prior contract artifacts to be reassessed and resubmitted, thus delaying project timeline schedules. In addition, the transition from an onsite solution to a cloud-based solution altered the way the bureau operated and affected the CSM schedule. Moving CSM to a cloud platform changed the architectural foundations that were originally planned for a non-cloud based environment. These factors increased the risk to meet the original timelines and created challenges that CSM continues to overcome.

COST AND BUDGET

Department of State **anticipates long-term cost savings** for CSM, but had not yet determined estimates.

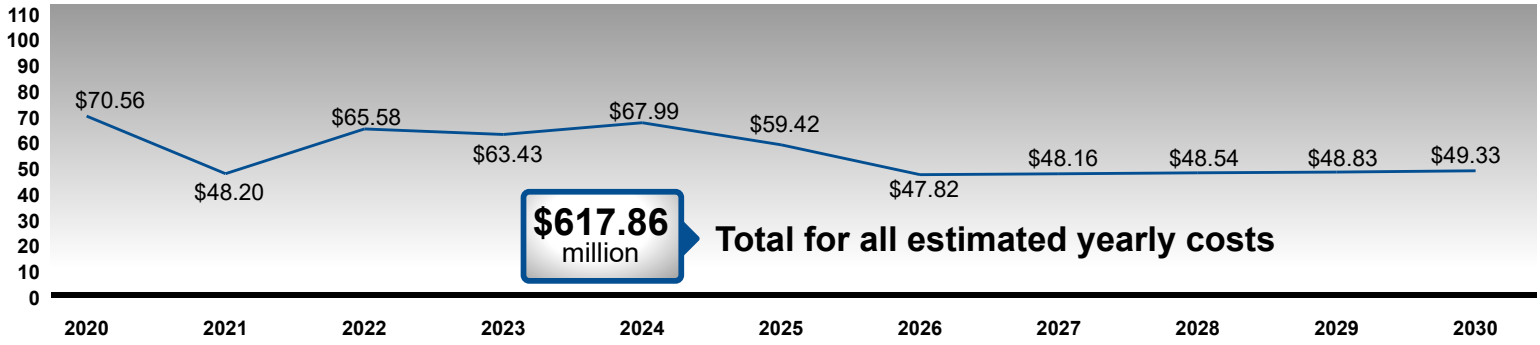
CSM obligations equal **1.8% of the department's total fiscal year 2020 IT budget.**

Total anticipated life cycle costs: $617.86 million over 11 years

The department **anticipates quantitative benefits** and had established **performance measures** for CSM.

The Bureau of Consular Affairs is responsible for the CSM budget and funding. According to bureau officials, without the ability to modernize legacy consular technology, State would incur increased costs by continuing to invest in legacy systems. In addition, the officials reported that the effectiveness of its mission to protect the U.S. border and citizens abroad would be at risk.

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



GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

The Office of Consular Systems and Technology within the Bureau of Consular Affairs serves as the business owner for the modernization effort. The CSM acquisition, which is part of a larger initiative called ConsularOne, is governed by the Office of Consular Systems and Technology's New Service Design and Development Division. As part of its responsibilities, the division is to monitor and assess contractor performance. In addition, the division established a performance evaluation board to review performance monitoring reports and evaluate contractor performance. The board is to consist of a CSM Program Manager, Deputy Program Manager, Development Manager, and Chief Engineer. The division also established performance monitors to evaluate and oversee the contractors' work on a continuous basis, prepare performance monitoring reports, and, when needed, recommend changes to the Performance Evaluation Board.

Source: GAO analysis of State information. | GAO-20-249SP

U.S. DEPARTMENT OF TRANSPORTATION | Automatic Dependent Surveillance-Broadcast

Source: Transportation. | GAO-20-249SP

The Automatic Dependent Surveillance–Broadcast (ADS-B) acquisition is a modernized surveillance technology that is intended to provide improved air traffic information for pilots and air traffic controllers. Described as the cornerstone technology for the Next Generation Air Transportation System (NextGen),[a] ADS-B is to increase efficiency and safety to meet the Federal Aviation Administration's (FAA) initiative to transform the National Airspace System by improving the condition of America's transportation-related infrastructure and reducing aviation-related fatalities. Additional anticipated system benefits include (1) increased capacity for areas with limited or no radar surveillance; (2) increased safety for users of weather and traffic broadcast services; (3) increased efficiency for airlines with future ADS-B cockpit applications; (4) more accurate trajectory information for automation used for sequencing and spacing, conflict avoidance, and search and rescue services; and (5) cost avoidance for the FAA due to a reduction in the existing radar inventory.

Key Information

ADS-B is a **key technology for implementing changes to the National Airspace System**—enabling common situational awareness necessary for air and ground shared responsibilities.

FAA mandated that, **starting January 1, 2020, aircraft must be equipped with an ADS-B technology** to fly in most controlled airspace.[b]

ADS-B was **re-baselined** in 2011 due to an increase in scope

The U.S. Department of Transportation's **Office of Inspector General** reported on ADS-B in December 2019. **(AV2020014)**

We last reported on air traffic control modernization in August 2017 and November 2016. **(GAO-17-450, GAO-17-241R)**

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Asset with new capabilities

Scope of acquisition: FAA

Unique investment identifier: 021-142305975

System users: Approximately 7,000 air transport aircraft and 88,000 general aviation and air taxis

Total anticipated life cycle costs: $5.04 billion over 29 years

Development approach: Waterfall development using contractor-developed, modified commercial off-the-shelf solutions

Project workforce: An average of 24 full-time equivalent employees and 87 full-time equivalent contract personnel per year over the life cycle of the acquisition

Federal IT Dashboard risk rating: low (as of June 2020)

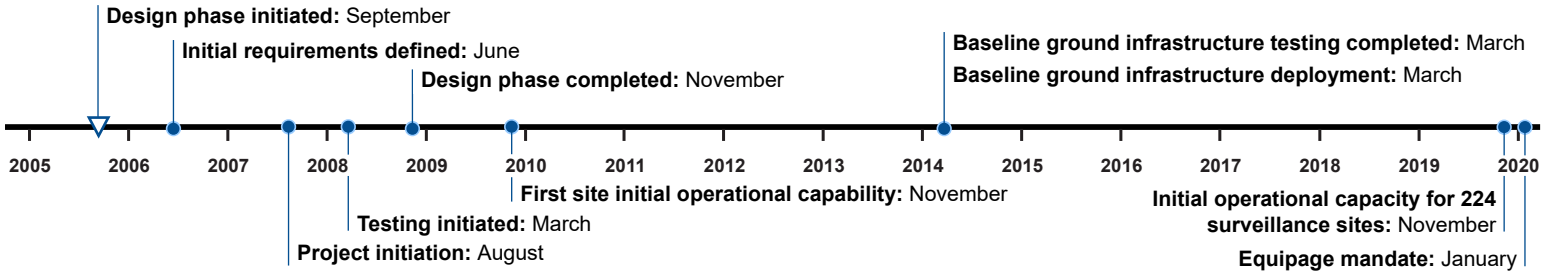
OVERVIEW

The U.S. Department of Transportation's (Transportation) 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, 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, as well as provide operational, user, and government benefits. ADS-B forms the foundation for NextGen by moving from ground radar and navigational aids to precise tracking using satellite signals. In addition, it 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 may receive and process surveillance information using the aircraft's multifunction display, and pilots could use the display to enhance situational awareness of the surrounding airspace. Further, ADS-B equipment may also be placed on ground vehicles to allow air traffic controllers and pilots to locate and identify them when they are on runways or taxiways.

CURRENT STATUS AND TIMELINE

The Surveillance and Broadcast Services Program Office established an implementation plan to develop and implement critical ADS-B services in four segments. These segments represent fiscal years 2007-2010, 2010-2014, 2014-2020, and 2020-2025. Activities for the current segment of ADS-B—2014-2020—include (1) continued provision of services and applications to achieve efficiency, safety, and cost savings benefits; (2) expanded surveillance coverage in the Gulf of Mexico to reduce delays; and (3) the implementation of a fuel-saving procedure in oceanic airspace. According to an official in FAA's Air Traffic Systems, Surveillance and Broadcast Services Program Office, the program reached initial operational capability for 224 of 225 surveillance sites as of November 2019.



Source: GAO (acquisition-specific illustration and analysis of Transportation information). | GAO-20-249SP

Next steps for the ADS-B acquisition include reaching initial operational capability for the final surface surveillance site by September 2020 for the current ADS-B segment (2014-2020) and initiating the next ADS-B segment to sustain existing ADS-B services (2020-2025). The next segment, among other things, is intended to provide upgrades to address air traffic tracking performance issues related to the display of fused data, provide enhanced resiliency capabilities for certain information security risks, and provide enhancements to the tool used to monitor the performance and compliance of an aircraft's ADS-B avionics.

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Not risky | Low risk | Moderately risky | Very risky

Technical risk	Schedule risk	Information security risk	Organizational risk	Cost/budget risk	Information privacy risk	Risk of not implementing

CHALLENGES IDENTIFIED

Not a challenge | Identified by the agency as a challenge

Organizational alignment and structure	Providing oversight and governance	Obtaining adequate funding/budget	Cost constraints	Schedule slippages	Workforce issues	Type of project methodology/ system development being used	Technical

FAA's Surveillance and Broadcast Services Program Office identified risks and challenges associated with the ADS-B acquisition. For example, identified risks included sharing ADS-B data with another country and equipping applicable foreign aircraft carriers with ADS-B (e.g., Latin and South American carriers). The officials noted that prior to the January 2020 equipage mandate they experienced technical challenges with ADS-B related to the lack of a sufficient number of users for testing efforts. In addition, Program Office officials reported the use of a performance-based service contract as a challenge, specifying that the use of this contracting approach was highly complex.

COST AND BUDGET

Transportation **anticipates life cycle cost avoidance** of $743 million with ADS-B.

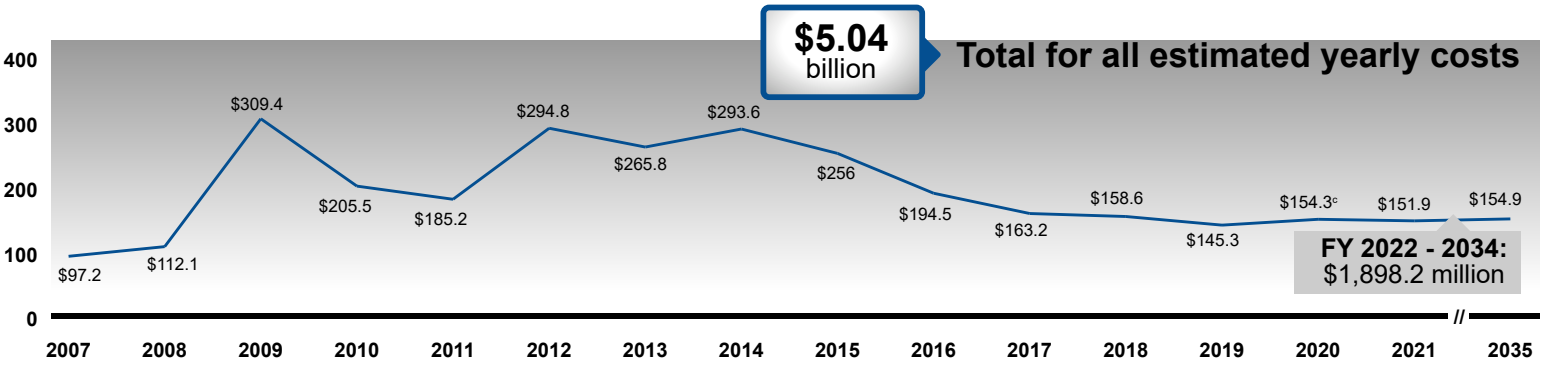
ADS-B obligations equal **6.5% of Transportation's total fiscal year 2020 IT budget.**

Total anticipated life cycle costs: approximately $5.04 billion over 29 years

Transportation **anticipates quantitative benefits** and had established **performance measures** for ADS-B.

The Program Management Organization within FAA is responsible for the ADS-B budget and funding. According to officials in the Surveillance Broadcast Services Program Office, FAA reviewed the quantity and locations of existing radars that must be retained to provide a surveillance backup for ADS-B, as well as protections related to the interaction of unequipped and equipped aircraft. As a result of this review, FAA determined that existing radars could be removed from 97 sites between fiscal years 2020 and 2030, resulting in a life cycle cost avoidance estimate of $743 million in base year 2019 dollars.

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



GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

The ADS-B effort is overseen by the Performance Control Board for the Surveillance and Broadcast Services Program Office. The program office is part of the FAA's Air Traffic Organization—the business owner of the acquisition. The Surveillance and Broadcast Services Program Office's Performance Control Board functions in both a governance and program management capacity to support system implementation throughout the National Airspace System. In this capacity, the board is to monitor ADS-B system development progress, system and applications deployment and implementation progress, post-implementation operations and maintenance performance, activity targets, earned value measures, technical performance measures, and business performance measures, among other things.

The ADS-B effort is also overseen by the Joint Resources Council, which comprises senior-level representatives from FAA's lines of business. The council is responsible for approval of all acquisition programs and oversees the execution and reporting of these programs. As part of its oversight responsibilities, the council is charged with approving and establishing baselines for all required FAA acquisition management system documents. This includes program requirements documents, acquisition program baselines, business cases, and implementation strategy and planning documents. The council is also responsible for making acquisition program decisions to modify program, cost, and schedule baselines, and conducts quarterly acquisition program reviews.

[a]The Next Generation Air Transportation System, or NextGen, is the Federal Aviation Administration's modernization of the nation's air transportation system. Its goal is to increase the safety, efficiency, capacity, predictability, and resiliency of American aviation.

[b]14 C.F.R. § 91.225.

[c]According to DOT officials, funding beyond FY 2020 are early estimates and future year costs are subject to change and are dependent on future appropriations.

Source: GAO analysis of Transportation information. | GAO-20-249SP

U.S. DEPARTMENT OF THE TREASURY | Customer Account Data Engine 2

Source: Department of the Treasury. | GAO-20-249SP

The Internal Revenue Service's (IRS) Customer Account Data Engine (CADE) 2 is intended to replace components of the IRS's core tax processing system and benefit taxpayers by delivering timely, accurate, and complete data for faster issue resolution and improved customer service. The IRS expects CADE 2 to improve tax administration and ensure fiscal responsibility through the use of data-centric technologies. The IRS considers the acquisition a top priority IT investment and its successful implementation is essential to reaching the agency's data-centric vision for tax administration. The IRS Enterprise Program Management Office reports that CADE 2 will be able to aggregate more than 2 billion taxpayer records for roughly 200 million individual taxpayers and make their data available to organizations across the IRS. In addition, IRS states that CADE 2 is intended to calculate, store, and leverage enhanced financial information to improve IRS financial management and reporting.

Key Information

CADE 2 will use and store **personally identifiable information.**	**Related GAO high-risk area:** Enforcement of tax laws. (GAO-19-157SP)	CADE 2 was **rebaselined** seven times from 2016 - 2019 due to a number of factors, including budget cuts, hiring freezes, and change in scope.	CADE 2 is intended to enhance the IRS's financial systems and **reduce the financial material weakness** for individual taxpayer processing.	We last reported on this program in June 2018, June 2016, and February 2015. (GAO-18-298, GAO-16-545, GAO-15-297)

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: An enhancement to an existing system

Scope of acquisition: IRS

Unique investment identifier: 015-000000051

System users: Approximately 200 million individual taxpayers, as well as organizations within the IRS

Total anticipated life cycle costs: $1.68 billion over 12 years

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

Project workforce: Over 175 government full-time equivalents employed and more than 200 full-time equivalent contract personnel

Federal IT Dashboard risk rating: low (as of June 2020)

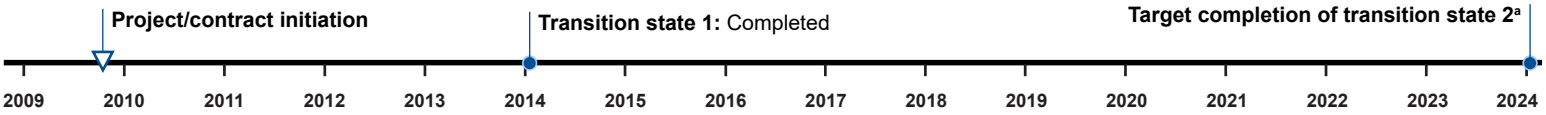
OVERVIEW

In carrying out its mission, IRS annually collects more than $3 trillion in taxes from millions of individual taxpayers and others. It also manages the distribution of more than $400 billion in refunds. The Individual Master File–the IRS's core tax processing system–is one of the oldest and highest risk systems in the federal government. Annual changes have been made to the system to address tax code changes and, where possible, updates to the underlying hardware. The result is decades upon decades of tax law implemented in a system that was written in a now outdated language code, is highly complex to maintain, and has limited skilled resources supporting it. The IRS initially intended to replace the almost 60-year-old legacy system with CADE 2 in order to modernize tax processing, simplify the IRS portfolio by reducing operations/management costs, and enable IRS to more efficiently and effectively deliver benefits to U.S. taxpayers, the IRS, and the Treasury. However, according to the IRS Chief Information Officer, the agency recognized that the scope for CADE 2 was too broad and complex, resulting in de-scoping several of the CADE 2 projects to focus solely on modernizing parts of the Individual Master File, which accounts for a large portion of tax processing activities. IRS also intends CADE 2 to address a financial material weakness and maintain a clean audit opinion. Further, according to the IRS Chief Information Officer, CADE 2 will benefit the IRS by enabling increased agility in response to changing taxpayer priorities and legislation, reduced IT costs and complexity, reduced workforce risk, and reduced burden of manually intensive processes on IRS employees by enabling automated calculations.

CURRENT STATUS AND TIMELINE

CADE 2 involves multiple projects, each with different start dates and requirements. To limit risk and demonstrate incremental progress toward modernization, IRS plans to deliver CADE 2 in three phases, called transition states. The first transition state was completed in 2014. As of July 2020, the agency was implementing the second transition state for CADE 2, which is focused on reengineering the core components of the Individual Master File using a hybrid-Agile and waterfall approach, conducting requirements design, and testing in iterative cycles.

Due to significant budget cuts and a shortage of skilled staff, the second transition state's release plan was revised three times between 2016 and 2017. For example, in late 2017, the release plan was revised to accommodate reduced fiscal year 2018 funding levels and anticipated future reductions. According to the IRS CIO, transition state 2 is expected to be completed in 2024. The third transition state had not been started as of July 2020 and IRS could not provide an expected completion date.



[a]According to IRS, the target completion date for transition state 3 is to be determined.

Source: GAO (acquisition-specific illustration and analysis of Department of the Treasury information). | GAO-20-249SP

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk | Moderately risky | Very risky

Information security risk	Cost/budget risk	Schedule risk	Technical risk	Organizational risk	Risk of not implementing	Information privacy risk

CHALLENGES IDENTIFIED

Not a challenge | Identified by the agency as a challenge

Organizational alignment and structure	Providing oversight and governance	Type of project methodology/ system development being used	Obtaining adequate funding/budget	Cost constraints	Schedule slippages	Technical	Workforce issues

The IRS identified a number of risk factors and challenges for CADE 2 related to obtaining adequate funding, schedule slippages, technical complexity, and workforce issues. Due to budget cuts and hiring freezes, the second transition state was revised three times between 2016 and 2017. According to the CADE 2 Program Manager, budget constraints in 2017 directly led to the pausing of 10 projects for CADE 2. IRS officials also reported technical challenges due to the lack of staff who could understand the core tax processing system's base code. The code reflects every tax law change made since 1962 and includes embedded business logic that only a small number of the IRS's personnel understand. In addition, IRS staff reported that ongoing retirements, a limited ability to fill open positions, and the shifting of resources because of tax reform demands have affected the timely development of CADE 2.

COST AND BUDGET

Treasury's IRS **anticipates benefits** with CADE 2, but does not expect to realize measurable cost savings.

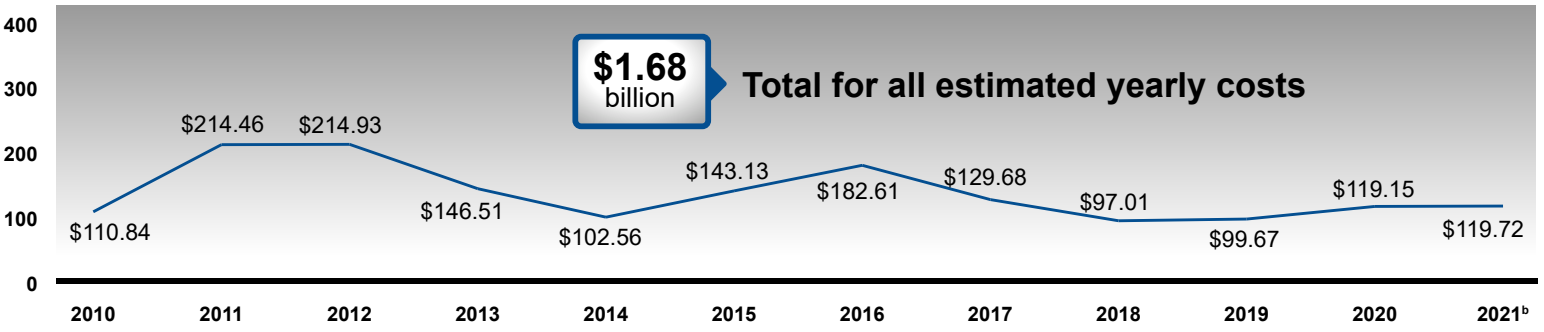
CADE 2 obligations equal **2.5% of Treasury's total fiscal year 2020 IT budget.**

Total anticipated life cycle costs: $1.68 billion over 12 years

Treasury's IRS anticipates **quantitative benefits** with CADE 2 and has established program **performance metrics**.

The IRS CIO is responsible for the budget and funding of CADE 2 and is charged with validating the business requirements with the Chief Financial Officer, who is responsible for the overall IRS budget, including the CADE 2 acquisition. According to the CADE 2 Program Manager, there will be benefits for modernizing the tax systems, but they do not expect to realize measurable cost savings. We previously recommended that the IRS Chief Technology Officer report at least quarterly on scope and cost performance for CADE 2, consistent with best practices. In response to our recommendation, the agency began reporting on planned versus actual delivery of functionality for CADE 2 starting in fiscal year 2016.

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



GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

The CADE 2 Governance Board, which is chaired by the Associate Chief Information Officer of the Enterprise Program Management Office, is charged with ensuring that acquisition objectives are met, decisions and issues are resolved in a timely manner, risks are managed appropriately, and the expenditure of resources are allocated in a fiscally sound manner. The CADE 2 Governance Board approves program risk response plans and milestone exits, and resolves escalated issues.

According to the CADE 2 Program Manager, the IRS CIO and the Enterprise Program Management Office are responsible for the oversight and project management of this acquisition, while the Wage and Investment Division and Chief Financial Officer are the business owners. Specifically, the Chief Information Officer is responsible for management and execution of the acquisition and management of the oversight process with external oversight entities, such as the Treasury Inspector General for Tax Administration. The Enterprise Program Management Office assists with program management through shared standards and best practices and works to integrate with Treasury's business and delivery partners. In addition, Treasury's Inspector General for Tax Administration performs periodic audits that vary in scope and timeline with CADE 2.

[b]The agency could not provide estimated expenditures beyond fiscal year 2021.

Source: GAO analysis of Department of the Treasury information. | GAO-20-249SP

U.S. DEPARTMENT OF THE TREASURY | Integrated Enterprise Portal

Source: Department of the Treasury. | GAO-20-249SP

The Integrated Enterprise Portal (IEP) acquisition is intended to enhance the existing portal by improving interactions and communications for taxpayers, employers, the Internal Revenue Service (IRS), and third parties. The acquisition is also to enhance the security and reliability of the portal, as well as modernize the portal's design and increase its capacity. IEP is to provide self-service options, establish secure information exchange options, build internal capabilities, and become the primary means for taxpayers and businesses to file tax information. The IEP serves as a preferred channel for interactions with the IRS, is currently the primary information source for taxpayers and tax professionals, and will play a central role in advancing taxpayer issue resolution by providing guidance and outreach, and improving service interactions for taxpayers.

Key Information

The IEP will use **personally identifiable information.**

Related GAO high-risk area: Enforcement of tax laws. (GAO-19-157SP)

The U.S. Digital Service identified providing secure access to IRS taxpayer information as a **high priority program** in 2016.

We last reported on this program in July 2018 and July 2017. (GAO-18-391, GAO-17-395)

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Operations and maintenance and an enhancement to an existing system

Scope of acquisition: IRS

Unique investment identifier: 015-000000056

System users: Over 100 million users, including tax payers, industry partners, and IRS employees

Total anticipated life cycle costs: $697.65 million over 10 years

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

Project workforce: Approximately 45 government full-time equivalents employed. The baseline number of full-time equivalents the contractor uses is 440 and fluctuates based on the needs of the IRS

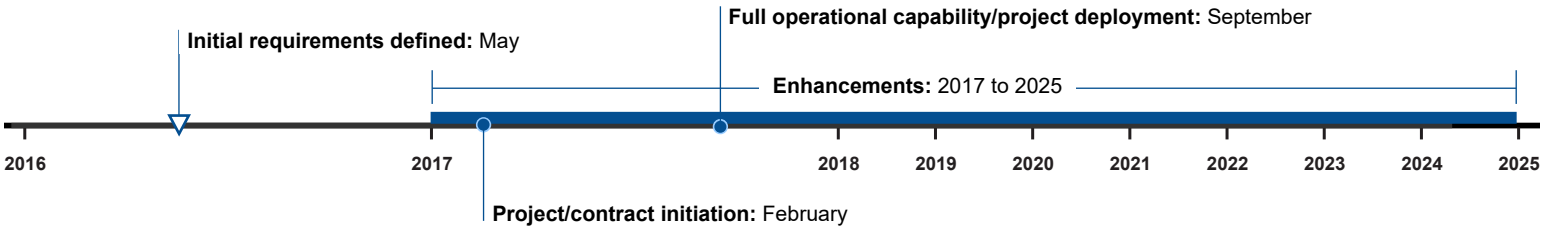
Federal IT Dashboard risk rating: low (as of June 2020)

OVERVIEW

The mission of the IRS, an agency within the Department of the Treasury, is to help America's taxpayers understand and meet their tax responsibilities and to enforce the tax law with integrity and fairness to all. To assist in this mission, the IRS offers a variety of external web services for its employees and the public, such as services for tax professionals to complete transactions online with the IRS and services to allow individuals to check the status of their refund. To assist IRS in meeting these responsibilities, the agency sought an acquisition designed to manage their existing services and accommodate the changing dynamics of their requirements due to Congressional mandates placed on the IRS and tax changes. These services are provided through IEP's four portals: the Public User Portal (also known as irs.gov), the Registered User Portal, the Employee User Portal, and the Transaction Portal Environment, each with its own IT infrastructure and governance.

CURRENT STATUS AND TIMELINE

As of July 2020, IEP was in the operations and maintenance phase. According to IRS' Executive Officer of IT Enterprise Operations, IEP was deployed in 2017 and IRS continues to make enhancements to the portal through an indefinite delivery, indefinite quantity contract.[a] The agency implemented new services through the IEP acquisition in 2018 that included web application security scanning, new service catalogs, performance analytics, enhanced monitoring, and capacity management. In 2019 and 2020, IRS completed additional enhancements including the migration of 20 Public User Portal (irs.gov) applications to the cloud, expanding network capacity and redundancy. In addition, in April 2020, IRS completed development, implementation, and support for the *Get My Payment* application, which is accessed through IEP.



[a]Indefinite delivery, indefinite quantity contracts provide for an indefinite quantity of services for a fixed time.

Source: GAO (acquisition-specific illustration and analysis of Department of the Treasury information). | GAO-20-249SP

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Not risky | Low risk | Moderately risky | Very risky

Technical risk	Schedule risk	Cost/budget risk	Risk of not implementing	Information security risk	Organizational risk	Information privacy risk

CHALLENGES IDENTIFIED

Not a challenge | Identified by the agency as a challenge

Organizational alignment and structure	Providing oversight and governance	Obtaining adequate funding/budget	Cost constraints	Type of project methodology/ system development being used	Schedule slippages	Technical	Workforce issues

According to IRS' Executive Officer of IT Enterprise Operations, risk factors associated with enhancing the IEP, including organizational, information security, and privacy, have had a low impact, while others have had no impact. In addition, IRS did not formally identify any challenges associated with the ongoing enhancements to its IEP. If future high-impact risks or challenges arise, the IRS has established a formal risk management process to manage risks to program progress and outcomes. Specifically, this plan describes the methodology for identifying and assessing risks, determining mitigation and contingency plans, implementing risk responses, monitoring and reporting the progress in reducing the risk, and incorporating approaches that could avoid identified risks.

COST AND BUDGET

IRS **does not anticipate any cost savings** with IEP.

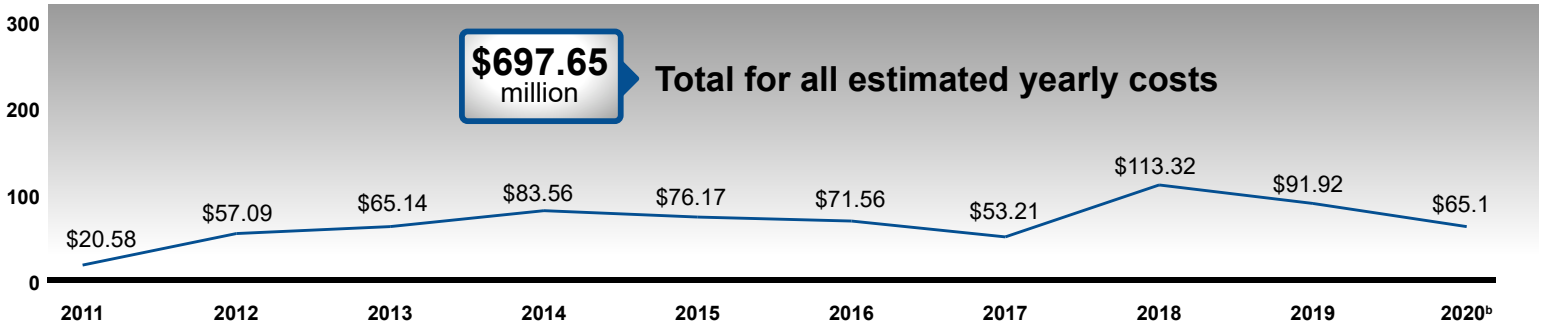
IEP's obligations equal **1.4% of Treasury's total fiscal year 2020 IT budget.**

Total anticipated life cycle costs: $697.65 million over 10 years

IRS has described **quantitative benefits** with IEP and has established program **performance metrics**.

According to IRS' Executive Officer of IT Enterprise Operations, the Enterprise Technology Implementation Division is responsible for the IEP's budget, while their Office of Information Technology's Online Division is responsible for the funding of this acquisition. IRS does not expect any associated cost savings with IEP, but has identified quantitative uptime benefits because of its security features. For example, IRS has enabled security measures at the perimeter that are intended to prevent cyber attacks and exploits. In addition, to measure and achieve benefits, IRS tracks average response time for users and time completing tax transactions, and has enabled analytic tools along with monitoring and identifying vulnerabilities to protect taxpayer data.

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



GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

According to IRS' Executive Officer of IT Enterprise Operations, the Enterprise Technology Implementation Division under IT Enterprise Operations and the Office of Information Technology Acquisitions are responsible for IEP's project management activities and oversight. The Office of Information Technology's Online Services is the business owner of IEP. The IEP project has a formal, three-tiered governance structure that provides a framework for the interactions at the executive, management, and operational levels. At the executive level (tier 1), IRS senior leaders hold quarterly executive checkpoints and monthly governance board meetings to ensure the project is progressing as expected. At the management level (tier 2), formal and informal management reviews between various key IRS officials are conducted to manage task order performance and address issues escalated from the operational level. At the operational level (tier 3), daily and weekly operational reviews are conducted to review project areas, work schedules, and progress against milestones and risks. In addition, IRS has issued IT governance standards that establish the requirements on which IT governance procedures and processes are built. These standards are to be used to provide oversight and decision-making criteria for all IRS IT governance boards.

[b]The agency could not provide estimated expenditures beyond the current fiscal year.

Source: GAO analysis of Department of the Treasury information. | GAO-20-249SP

U.S. DEPARTMENT OF VETERANS AFFAIRS | Electronic Health Record Modernization

Source: VA. | GAO-20-249SP

The goals of the U.S. Department of Veterans Affairs' (VA) Electronic Health Record Modernization (EHRM) effort are to replace its current electronic health record (EHR) system by leveraging a commercial solution chosen by the Department of Defense (DOD) in order to achieve interoperability with DOD and community care providers.[a] In addition, the system is to improve VA services and health care coordination for veterans who receive medical care from VA and its partners. Specifically, the system is intended to serve veterans as one common system providing a single, accurate, lifetime health record with the result of improving patient care and safety, and result in enabling seamless care without compromising data between current systems.

Key Information

The EHRM will use and store **personally identifiable information.**

Related GAO high-risk area: Managing Risks and Improving VA Health Care and VA Acquisition Management. (GAO-19-157SP)

VA's prior EHR initiative was identified by the Office of Management and Budget as a **high priority program** in 2015 and 2016.

We have ongoing work related to this program and last reported on it in June 2020, April and July 2019, and January and September 2018. (GAO-20-473, GAO-19-476T, GAO-19-125, GAO-18-208, GAO-18-696T)

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Replacement of a legacy system

Scope of acquisition: Agency-wide

Unique investment identifier: 029-555555305

System users: U.S. Veterans, Veterans Benefits Administration and other staff, and VA clinical staff, among others

Total anticipated life cycle costs: $16.14 billion over 10 years

Development approach: Incremental rollout of commercial off-the-shelf solution

Project workforce: 305 government full-time equivalents employed

Federal IT Dashboard risk rating: medium (as of June 2020)

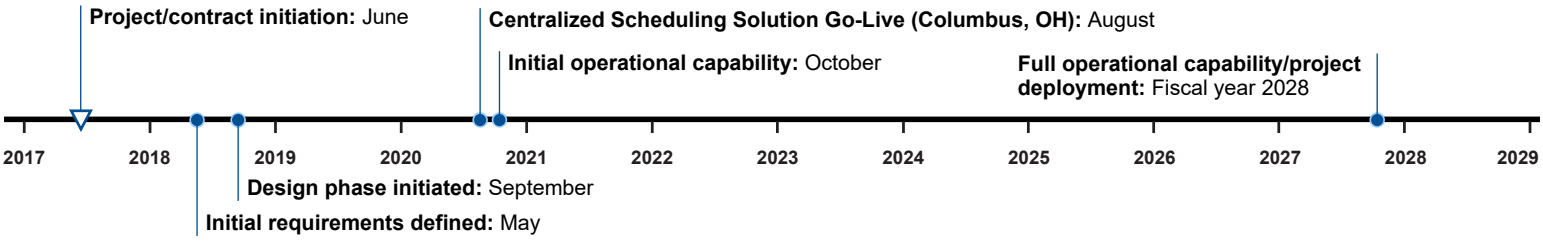
OVERVIEW

VA's mission is to promote the health, welfare, and dignity of all veterans in recognition of their service to the nation by ensuring that they receive medical care, benefits, social support, and lasting memorials. In carrying out this mission, the department operates one of the largest health care delivery systems in the United States, providing health care services to approximately nine million veterans throughout the United States, Philippines, Virgin Islands, Puerto Rico, American Samoa, and Guam.

On June 5, 2017, VA announced its decision to replace its legacy EHR system–the Veterans Health Information Systems and Technology Architecture–with the same commercial off-the-shelf EHR software solution being deployed by DOD (MHS GENESIS). For more than a decade, VA and DOD have not had EHR systems that permit the electronic exchange of patient health information as military service members transition from DOD to VA health care systems. Without specific and uniform national interoperability standards, VA and DOD will continue to face significant challenges if the departments remain on two different systems. VA's adoption of the same EHR solution as DOD will facilitate delivery of service members' health care and benefits between the agencies.

CURRENT STATUS AND TIMELINE

As of July 2020, VA planned to run existing systems concurrently with the deployment of EHRM while each facility is transitioned to the new solution. The department has multiple contracts in place to perform the implementation and various aspects of the EHRM are being developed concurrently over a number of stages. VA expects its EHRM delivery to be based on approximately 50 deployments to an estimated 170 medical centers, with the first go-live planned for October 2020. These deployments will include initial site assessment, configuration, testing, training, change management, deployment, and sustainment. Ongoing requirements documentation and development will occur over the next 12 months, including capturing initial requirements for the IT network, hardware, and software modernization that need to be completed at the initial operating capability sites for a successful deployment.



[a]DOD's commercial off-the-shelf EHR solution is also profiled in this report.

Source: GAO (acquisition-specific illustration and analysis of VA information). | GAO-20-249SP

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk | Moderately risky | Very risky

Information security risk	Information privacy risk	Technical risk	Organizational risk	Cost/budget risk	Schedule risk	Risk of not implementing

CHALLENGES IDENTIFIED

Not a challenge | Identified by the agency as a challenge

Type of project methodology/ system development being used	Organizational alignment and structure	Obtaining adequate funding/budget	Cost constraints	Providing oversight and governance	Technical	Schedule slippages	Workforce issues

VA identified challenges and program risks for its EHR modernization effort, including workforce issues, schedule slippages, and information privacy risks associated with data migration. For example, workforce risks related to the EHR modernization effort include end user adoption and training and defining clinical workflow roles and responsibilities. In addition, if internal VA processes, such as staffing and technical and functional governance, are not properly structured, integrated, and coordinated to support timely decision making, then the program's schedule may be impacted and delayed. Furthermore, if legacy patient data is not accurately and correctly mapped and migrated between the legacy EHR system and the modernized EHRM, then a patient's records and safety could be jeopardized.

COST AND BUDGET

VA **anticipates cost savings** with EHRM, but has not yet estimated them.

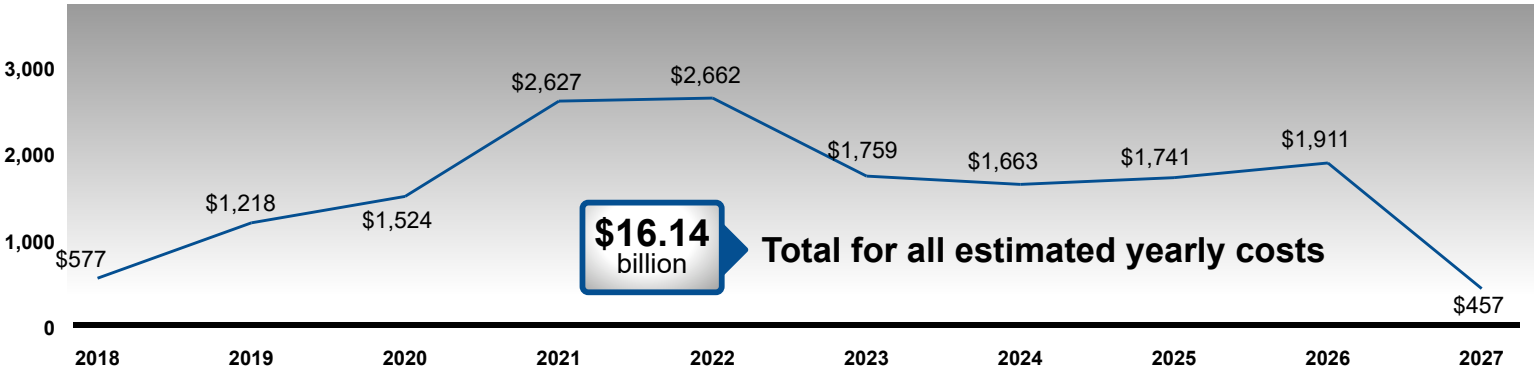
EHRM obligations equals **24.6% of VA's total fiscal year 2020 IT budget.**

Total anticipated life cycle costs: $16.14 billion over 10 years

VA **anticipates quantitative benefits** with EHRM and has established program **performance metrics**.

VA's EHRM Program Executive Office and the Office of Management are responsible for EHRM's budget, while the Office of the Deputy Secretary and Office of Management are responsible for the funding of this acquisition. The EHRM system's fiscal year 2019 appropriation of $1.1 billion and fiscal year 2020 appropriation of $1.6 billion allowed VA to continue the implementation, testing, preparation, development, interface, management, rollout, program management, and maintenance activities to support the EHRM initiative. VA is developing an analysis highlighting anticipated cost savings associated with legacy system terminations/transitions over the implementation of EHRM.

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



GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

In June 2018, VA established the Office of Electronic Health Record Modernization (OEHRM) to ensure VA successfully prepares for, deploys, and maintains the new EHR solution. According to a senior official in VA's EHRM Program Executive Office, the office is responsible for the acquisition's project management activities and reports directly to the VA Deputy Secretary. The office is led by an Executive Director, Chief Medical Officer, and Chief Technology Integration Officer, and works in close coordination with the VA Veterans Health Administration and Office of Information and Technology.

The EHRM Program Executive Office is responsible for the oversight of EHRM and the OEHRM. The OEHRM is responsible for project management and both report directly to the Deputy Secretary of VA, who is the business owner of the EHRM effort. The formal governance structure includes a steering committee, governance integration board, functional governance board, technical governance board, and electronic health record councils, along with working groups. The Office of Information and Technology leadership is a member of most of these governance entities.

On December 4, 2019, VA and DOD re-chartered the DOD/VA Interagency Program Office as the Federal Electronic Health Record Modernization program office. The mission of the new office is to implement a single common federal electronic health record to enhance patient care and provider effectiveness. The office serves as a single point of accountability in the delivery of a common record that contributes to full interoperability of health care information between the departments. For all VA acquisition matters, the Federal Electronic Health Record Modernization Director and Deputy Director report to the VA Deputy Secretary, as Chair of the VA Operations Board.

U.S. SMALL BUSINESS ADMINISTRATION | Application Standard Investment – Certify Project

Source: SBA. | GAO-20-249SP

The Application Standard Investment (with previous development work conducted under Certify.SBA.gov) is intended to replace legacy systems and serve as a single entry portal for programs managed by the U.S. Small Business Administration's (SBA) Office of Government Contracting and Business Development. The acquisition, which is part of the larger Certify.SBA.gov project, is to eliminate paper applications, thus reducing the burden and costs on small businesses that apply for SBA federal contracting and business development programs. This acquisition is intended to allow SBA analysts to review eligibility applications for small business contracting programs and allow the analysts and businesses to track the status of applications and maintain the applications online. In addition, the acquisition is anticipated to provide confidence in the security of personally identifiable information and financial data, and reduce risks associated with identify theft.

Key Information

- The Certify project's Application Standard Investment will use and store **personally identifiable information**.
- SBA **spent approximately $27 million on Certify.SBA.gov** prior to initiation of the Application Standard Investment acquisition in September 2019.
- Certify.SBA.gov was identified as a **high priority project** by the U.S. Digital Service in 2016 and 2017.
- Certify.SBA.gov was **rebaselined** in 2016 due to a change in scope and development approach.
- We last reported on this effort in May 2019 and March 2019. **(GAO-19-563T, GAO-19-168)**

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Replacement of a legacy system; leveraging a new asset with new capabilities

Scope of acquisition: Offices of the Chief Information Officer and Government Contracting and Business Development

Unique investment identifier: 028-000000062

System users: 60,000 users

Total anticipated life cycle costs: $18.55 million over 10 years

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

Project workforce: Five SBA government full-time equivalent employees and 14 full-time equivalent contract personnel

Federal IT Dashboard risk rating: medium (as of June 2020)

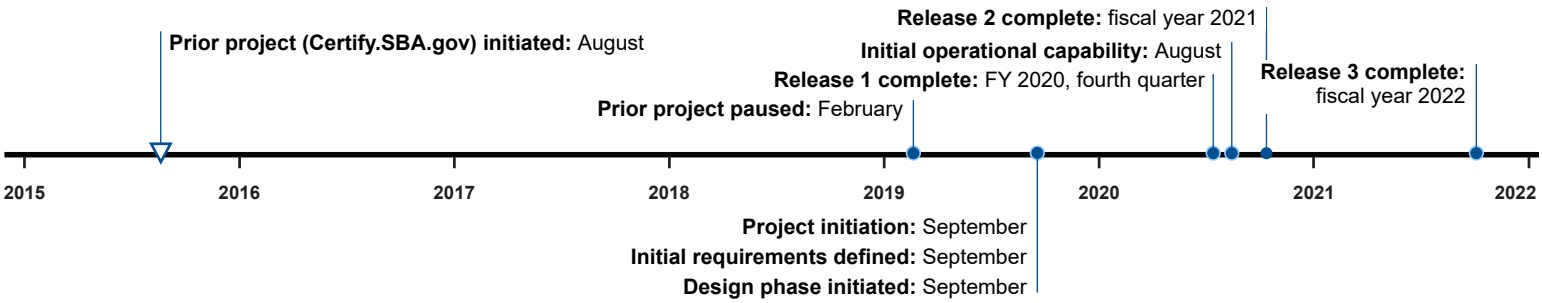
OVERVIEW

SBA was created to aid, counsel, assist, and protect the interests of small business concerns, preserve free competitive enterprise, and maintain and strengthen the U.S. economy. As part of SBA, the Office of Government Contracting and Business Development works to enhance the effectiveness of small business programs by working with SBA's program offices and others to develop policies, regulations, and statutory changes. To help meet its mission, in August 2016, SBA planned to develop new capabilities for Certify.SBA.gov, its online portal that allows business owners to upload required documents and track their submission, among other things. While SBA had implemented some of the planned capabilities, the agency paused development efforts for Certify.SBA.gov in February 2019 due to concerns regarding missed milestones and delivery dates, and cost overruns.

In September 2019, after researching alternate options for Certify.SBA.gov, SBA restarted Certify project development efforts under the Application Standard Investment acquisition. New capabilities are to include portal access for external users, data validation, integrated messaging between SBA staff and contracting officers, single sign-on and data integration, and cybersecurity services integration. The acquisition is to replace legacy systems supporting a woman-owned small business repository, business development information, electronic annual reviews, certification tracking, and small business search capabilities, among other things.

CURRENT STATUS AND TIMELINE

According to Office of the Chief Information Officer (CIO) officials, as of November 2019, the acquisition was in the implementation phase, but, due to the use of an incremental development approach, other development phases were also ongoing. Activities for the Acquisition Standard Investment were to be completed in three releases for (1) workflow integration and reporting activities for historically underutilized businesses, woman-owned small businesses, and a business development program for small disadvantaged businesses; (2) replacement of a small business search database; and (3) activities supporting data cleanup and change management.



Source: GAO (acquisition-specific illustration and analysis of SBA information). | GAO-20-249SP

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk | Moderately risky | Very risky

Technical risk	Schedule risk	Information security risk	Organizational risk	Cost/budget risk	Risk of not implementing	Information privacy risk

CHALLENGES IDENTIFIED

Not a challenge | Identified by the agency as a challenge

Organizational alignment and structure	Providing oversight and governance	Cost constraints	Obtaining adequate funding/budget	Type of project methodology/ system development being used	Schedule slippages	Technical	Workforce issues

Officials in SBA's Offices of the CIO and Government Contracting and Business Development identified a number of risks and challenges for the Application Standard Investment. These risks included (1) a lack of long-term budget for the Certify project, (2) the lack of government staff support, and (3) the lack of technical support from the Office of the CIO. Officials also reported schedule slippages due to program leadership prioritizing other projects. In addition, officials in the Office of the CIO reported that the lack of an allocated budget for long-term investment and continuous program development, as well as the use of incremental (Agile) methodologies for the acquisition, were challenging.

COST AND BUDGET

SBA **anticipates cost savings** for the Application Standard Investment, but had not yet estimated the savings.

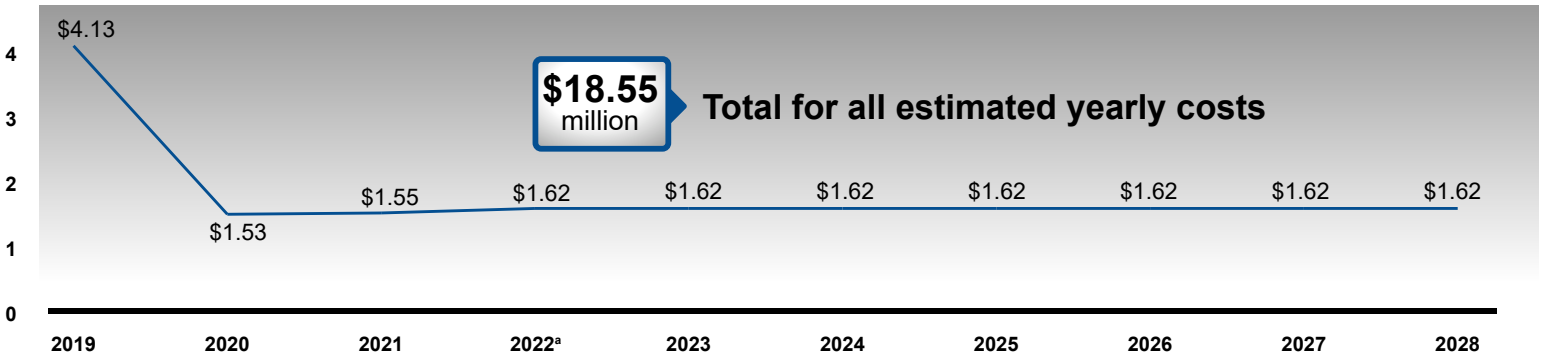
Application Standard Investment obligations equal **6.3% of SBA's total fiscal year 2020 IT budget.**

Total anticipated life cycle costs: $18.55 million over 10 years

SBA **anticipates quantitative benefits** with Application Standard Investment, but had not yet established performance measures.

SBA spent approximately $27 million on the Certify.SBA.gov acquisition before development efforts were paused and then restarted under the Application Standard Investment. According to officials in SBA's Office of the CIO, their office and the Office of Government Contracting and Business Development share responsibility for the budget and funding of the new acquisition. While SBA had not estimated cost savings for the acquisition as of May 2020, the agency planned to achieve savings by automating report production. SBA had an enacted budget of $7.4 million for fiscal year 2020 to continue the Application Standard Investment development and implementation efforts.

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



GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

SBA's Offices of the CIO and Government Contracting and Business Development share responsibility for overseeing the Certify project. The CIO and Chief Financial Officer are charged with co-chairing the Business Technology Investment Council, which serves as SBA's Investment Review Board and principal governance body in managing IT investments. Council meetings are to be held at least quarterly to ensure that oversight and review functions are being met, but the co-chairs may call ad-hoc meetings to deal with urgent issues that arise or agency projects. In addition to the CIO's involvement with the council, responsibilities include governance, and operational monitoring and management.

[a]SBA did not anticipate an increase in estimated life cycle costs beyond FY 2022, barring new legislation and inflation.

Source: GAO analysis of SBA information. | GAO-20-249SP

U.S. SOCIAL SECURITY ADMINISTRATION | Disability Case Processing System 2

Source: SSA. | GAO-20-249SP

The Disability Case Processing System 2 (DCPS2) is a priority initiative of the U.S. Social Security Administration (SSA) and is intended to replace 52 disparate Disability Determination Services' component systems that state agencies use to make eligibility determinations. DCPS2 is a common case processing system that is to modernize the SSA's entire disability claims process, including assigning cases and managing workloads; documenting contacts with claimants and other appropriate parties; preparing disability determinations, determination rationales, and notices; facilitating quality reviews; and providing a fiscal solution that is expected to reduce or eliminate duplicate and erroneous payments and optimize overall fiscal productivity. In addition, DCPS2 is anticipated to provide flexibility and the high performance necessary to process disability claims in a timely and efficient manner.

Key Information

DCPS2 will use and store **personally identifiable information.**

Related GAO high-risk area: Improving and modernizing federal disability programs. (GAO-19-157SP)

DCPS2 was identified as a **high priority program** by the Office of Management and Budget in 2016.

DCPS2 was **rebaselined** in 2015 due to a change in development approach and in 2018 due to an increase in scope.

We reported on this acquisition and related case processing efforts in September 2018, July 2018, and July 2016. (GAO-18-703T, GAO-18-501, GAO-16-815T)

ACQUISITION BACKGROUND

Acquisition designation: Major IT acquisition

Type of acquisition: Replacement of legacy systems

Scope of acquisition: Agency-wide

Unique investment identifier: 016-000002141

System users: Approximately 15,440 employees

Total anticipated life cycle costs: $176.8 million over 7 years

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

Project workforce: 56 government full-time equivalent employees and 70 full-time equivalent contract personnel

Federal IT Dashboard risk rating: low (as of June 2020)

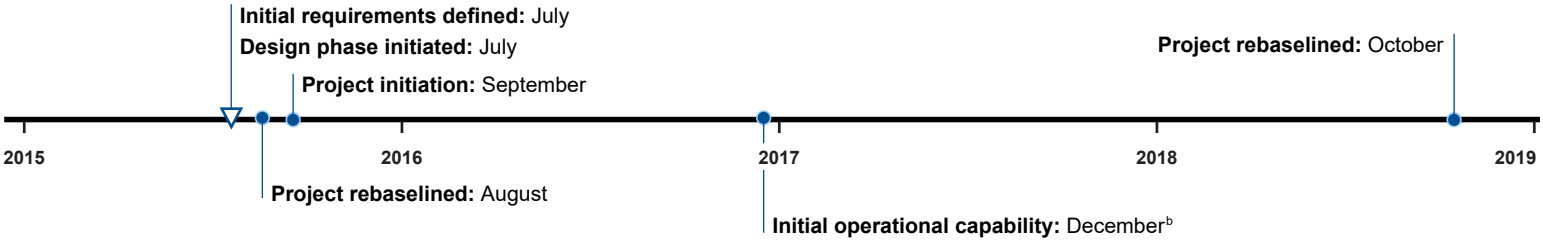
OVERVIEW

SSA administers programs under the *Social Security Act* that provide benefits to individuals with disabilities. To carry out this role, SSA partners with state Disability Determination Services to evaluate disability cases and make disability determinations. Historically, each of the Disability Determination Services has used a customized and independently-operated system to process disability cases. After a failed attempt to modernize these aging (legacy) systems in 2010, SSA began another effort in September 2015 to develop a modernized and integrated disability case processing system that moves disability determinations from intake through appeals—DCPS2. DCPS2 leverages modern technologies, cloud environments, and open source products. DCPS2 is expected to minimize the average processing time for initial disability claims, decrease case processing-related task time, and provide increased system availability. DCPS2 is also to improve service for the public and reduce administrative costs. SSA expects that all state Disability Determination Services will be able to implement DCPS2 and retire their legacy systems. According to officials in the Office of the Deputy Commissioner for Operations, certain states began retiring legacy systems and replacing them with DCPS2 in fiscal year 2019.

CURRENT STATUS AND TIMELINE

SSA's Office of the Chief Program Officer reported that the system was re-baselined twice during its development–in August 2015 and October 2018. Specifically, rebaselining took place to transition to shorter incremental release cycles and to update the DCPS2 completion date and cost to include additional development and deployment activities. According to the Office of the Deputy Commissioner for Operations, the agency is using Agile best practices in an iterative and incremental approach to plan deliverables in two-month increments and deliver releases to the DCPS2 user community on a monthly basis.

According to SSA officials, as of May 2020, DCPS2 had been deployed at 42 of 52 state Disability Determination Services sites.[a] The officials added that two of these sites—Maine and Wyoming—terminated their legacy contracts effective September 2019 and solely use DCPS2 to process disability claims determinations. The remaining 40 sites were still using portions of their legacy systems as well as DCPS2 to support the processing of disability claims determinations or had not yet terminated their legacy system contracts.



[a]The 42 sites are: Alabama, Arizona, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Indiana, Iowa, Kansas, Louisiana, Maine, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Vermont, Virginia, Washington, Washington, D.C., West Virginia, Wisconsin, and Wyoming.

Source: GAO (acquisition-specific illustration and analysis of SSA information). | GAO-20-249SP

While two additional releases were forecasted to be completed in July and September 2020, according to SSA officials, the agency could not provide a time frame for completing system development due to the incremental (Agile) development approach that it is using. Nevertheless, SSA officials stated in April 2020 that DCPS2 is capable of processing all but a very limited number of claim types and future releases would be provide the additional functionality needed to fully process all claim types.

AGENCY-IDENTIFIED RISK FACTORS AND CHALLENGES

RISK FACTORS AND LEVELS

Low risk | Moderately risky | Very risky

Technical risk	Schedule risk	Information security risk	Organizational risk	Information privacy risk	Cost/budget risk	Risk of not implementing

CHALLENGES IDENTIFIED

Not a challenge | Identified by the agency as a challenge

Organizational alignment and structure	Providing oversight and governance	Obtaining adequate funding/budget	Cost constraints	Schedule slippages	Technical	Type of project methodology/ system development being used	Workforce issues

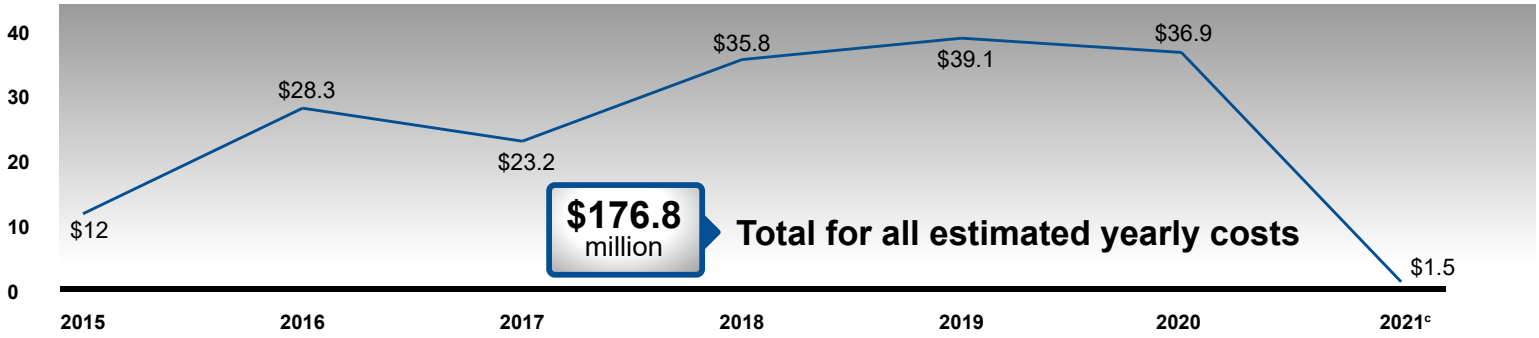
SSA identified several risks and challenges associated with DCPS2. The risks included limited agency resources to support the incremental software migration, complexity of Disability Determination Services code requirements that could be unmanageable, insufficient end-to-end testing that could cause low-quality deliverables, and dependencies on other projects that could affect scheduled milestones. The challenges included obtaining project staff with appropriate skills and the use of Agile methods while leveraging cloud infrastructure, current programming languages, and a web-enabled database.

COST AND BUDGET

SSA **anticipates cost savings** with DCPS2, but has not yet estimated them.	DCPS2 obligations equal **0.7% of SSA's total fiscal year 2020 IT budget.**	**Total anticipated life cycle costs:** $176.8 million over 7 years	SSA **anticipates quantitative, operational, and technical benefits** with DCPS2 and had **established performance measures**.

According to the Chief Program Officer for DCPS2, SSA's Office of the Chief Information Officer for Systems is responsible for the acquisition's budget and funding. According to agency officials in the Office of the Deputy Commissioner for Operations, DCPS2 is critical to the agency's vision of modernizing the disability process and to retire the existing legacy systems. Officials in the Office of the Chief Program Officer reported that delaying or terminating funding in any manner would substantially impact the project, hindering the agency's ability to process disability claims in a timely and efficient manner.

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



GOVERNANCE AND OVERSIGHT RESPONSIBILITIES

As the business owner of the DCPS2 effort, SSA's Office of the Deputy Commissioner for Operations is charged with providing budget and management guidance for disability claims activities as carried out by the State Disability Determination Services. The Office of the Chief Program Officer, a temporary organization within the Office of the Deputy Commissioner for Operations, is responsible for developing the system. According to the DCPS2 program charter, the Chief Program Office is to oversee project management activities, such as the cost-benefit analysis, risk management, security management, schedule and implementation planning, and architectural and technical oversight. SSA's Office of the Deputy Commissioner for Systems is responsible for developing, overseeing, and maintaining the agency's IT systems. The office is headed by the Deputy Commissioner, who also serves as the agency's Chief Information Officer.

[b]Due to the iterative nature of the systems development process being used by SSA, officials in the Office of the Chief Program Officer could not provide a date that DCPS would reach full operational capability.

[c]The amount shown for FY 2021 is a projection for only the first quarter of the fiscal year.

Source: GAO analysis of SSA information. | GAO-20-249SP

Agency Comments and Our Evaluation

We requested comments on a draft of this report from the 12 agencies with systems profiled in this report and the Office of Management and Budget. In response, we received written comments from one agency: the Social Security Administration (SSA).

In its comments, SSA stated that the Disability Case Processing System 2 (DCPS2) is part of an enterprise-wide integration of its electronic case processing system. SSA said that DCPS2 is to be used by all disability determination service sites to adjudicate the agency's disability determinations. Further, SSA noted in its comments that implementing DCPS2 as the nation's common case processing system is expected to improve service to the public, modernize disability determination processes, and increase information security. The SSA's comments are reprinted in appendix III.

In addition to the aforementioned comments, the Social Security Administration and eight other agencies (the Departments of Commerce, Defense, Homeland Security, Justice, the Treasury, Transportation, Veterans Affairs, and the Small Business Administration) provided technical comments, which we incorporated as appropriate. Three agencies (the Departments of Agriculture, Interior, and State) and the Office of Management and Budget told us that they had no comments on the draft report.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of the Departments of Agriculture, Commerce, Defense, Homeland Security, the Interior, State, the Treasury, Transportation, and Veterans Affairs; the U.S. Attorney General (Department of Justice); the Administrator of the Small Business Administration; the Commissioner of the Social Security Administration; the Director of the Office of Management and Budget; and other interested parties. This report is available at no charge on the GAO website at http://www.gao.gov.

If you or your 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 IV.

Carol C. Harris
Director, Information Technology Acquisition Management Issues

List of Requesters

The Honorable Carolyn B. Maloney
Chairwoman
The Honorable James Comer
Ranking Member
Committee on Oversight and Reform
House of Representatives

The Honorable Gerald E. Connolly
Chairman
The Honorable Jody Hice
Ranking Member
Subcommittee on Government Operations
Committee on Oversight and Reform
House of Representatives

The Honorable Will Hurd
House of Representatives

The Honorable Jim Jordan
House of Representatives

The Honorable Robin L. Kelly
House of Representatives

Appendix I: Objective, Scope, and Methodology

The objective of this review was to identify essential mission-critical IT acquisitions across the federal government and determine their key attributes.[1] To address the objective, we first identified acquisitions for possible selection by administering a questionnaire via email to each of the 24 major federal agencies covered by the Chief Financial Officers Act of 1990.[2] In the questionnaire 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. We also asked each agency to answer specific questions about each of the acquisitions.[3] These questions related to the acquisition's planned services and capabilities, governance structure, systems development life cycle, potential risks, project timeline, anticipated life cycle costs, 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 pretested the questionnaire by interviewing officials in the offices of the Chief Information Officer (CIO) and the Chief Acquisition Officer at the Department of Homeland Security, the National Aeronautics and Space Administration, and the Nuclear Regulatory Commission. In doing so, we

[1]For the purpose of this report, the term 'acquisition' is a broad term that also includes IT investments. According to the Federal Acquisition Regulation, 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. The purchase or lease can be for supplies or services already in existence or that 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.

[2]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.

[3]For the purpose of this report, mission-critical acquisitions are those that further 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, 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.

sought to ensure that our questions were clear and logical and that respondents could answer the questions without undue burden. We then administered the questionnaire and received responses from 23 of the 24 agencies, for a nearly 96 percent response rate.[4] The 23 agencies identified a total of 98 IT acquisitions.

To help ensure that we identified the most critical IT acquisitions for each agency, we also reviewed Federal IT Dashboard data and prior reports that we and federal 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 top three to five mission-critical IT acquisitions. Fourteen of the 24 agencies' Inspectors General provided responses for a total of 47 IT acquisitions. Subsequent to our review of relevant information, our discussions with subject matter experts, as well as the information obtained from the Inspectors General, we selected an additional two acquisitions for the Department of Defense and one additional acquisition for the Department of the Treasury. With these additional selections, the total number of identified acquisitions we considered for our study was 101.

To select the acquisitions to be profiled in this report, we developed a set of criteria and assigned each criteria point values to select our mission-critical acquisitions. We developed these criteria based on our reviews of the "National Essential Functions" identified in Presidential Policy Directive 40, National Continuity Policy; the U.S. Department of Homeland Security's Federal Emergency Management Agency, Federal Continuity Directive 1; agencies' inspectors general reports and whether they considered the acquisition mission-critical; Federal IT Dashboard data (e.g., the acquisition's budget, project schedule status, and chief information officer risk ratings); the 2018 President's Management Agenda; Office of Management and Budget's (OMB) high priority programs reports to Congress; the United States Digital Service reports to Congress on the federal government's high priority projects; our February 2015, February 2017, September 2018, and March 2019 High-Risk Series reports; our other relevant prior reports; critical infrastructure

[4]The Department of Defense (DOD) did not provide a questionnaire response that listed five mission-critical IT acquisitions within the audit timeframe.

sectors identified in the Presidential Policy Directive 21; and federal agencies' questionnaire results.[5]

The criteria were arranged into 14 categories: National Essential Functions, Agency Office of Inspector General, IT Dashboard, President's Management Agenda, OMB High Priority Program Reports to Congress, Government Accountability Office, Critical Infrastructure Sectors, Scope of End Users, Designation of Mission-Critical, Cost, Agency Oversight, OMB Oversight, Capabilities and Acquisition Type, and Potential Risks to the Agency and Nation. Each category is then made up of a number of more detailed attributes that were assigned point values ranging from zero to 16. These point values were assigned 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 2 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* (January 17, 2017); Office of Management and Budget, *Quarterly Report to Congress: 10 High Priority Programs Quarterly Report* (Washington, D.C.: June 25, 2015) and *Report to Congress: 10 High Priority Programs* (Washington, D.C.: June 9, 2016); United States Digital Service, *The U.S. Digital Service Report to Congress*, December 2016 and *The U.S. Digital Service Report to Congress*, July 2017; GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C. Feb. 11, 2015); *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017); *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018); *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019); *Presidential Policy Directive 21:Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013); and President's Management Council and Executive Office of the President, *President's Management Agenda* (Washington, D.C.: Mar. 20, 2018).

Table 2: 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 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, two 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, two 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, two points
Does the goal of the acquisition relate to providing critical Federal Government services that address the national health, safety, and welfare needs of the United States?	0 or 2	If yes, two points
Agency Office of Inspector General (OIG)		
Has the acquisition been audited by its agency OIG?	0 or 2	If yes, two points
Does the OIG consider the acquisition mission-critical?	0 or 2	If yes, two points
IT Dashboard		
Federal IT Dashboard's CIO risk rating[b]	0 to 3	3 points if the risk rating was 'high', 2 points if the rating was 'medium', and 1 point if the rating was 'low'
President's Management Agenda[c]		
Does the acquisition relate to goals in President's Management Agenda?	0 or 2	If yes, two points
Is the acquisition's purpose to:		
increase productivity and security through modernization	0 or 2	If yes, two points
leverage data as a strategic asset	0 or 2	If yes, two points
assist in developing a workforce for the 21st century	0 or 2	If yes, two points
improve the customer experience with federal services	0 or 2	If yes, two points
Improve the effectiveness and efficiency of administrative services	0 or 2	If yes, two points
share core mission support services	0 or 2	If yes, two points
help shift from low-value to high-value work	0 or 2	If yes, two points
leverage common contracts and best practices to drive savings and efficiencies	0 or 2	If yes, two points
use results-oriented accountability for grants	0 or 2	If yes, two points
improve payments made by the agency	0 or 2	If yes, two points
improve outcomes through federal IT spending transparency	0 or 2	If yes, two points
improve management of major acquisitions	0 or 2	If yes, two points
modernize infrastructure permitting process	0 or 2	If yes, two points
improve security clearance, suitability, and credentialing	0 or 2	If yes, two points
improve transfer of federally-funded technologies from lab-to-market	0 or 2	If yes, two points

Criteria categories and attributes	Points	Point value description
Office of Management and Budget (OMB) High Priority Program Reports to Congress[d]		
Was the acquisition identified in June 2015 report?	0 or 3	If yes, three points
Was the acquisition identified in June 2016 report?	0 or 3	If yes, three points
Was the acquisition identified in December 2016 report?	0 or 3	If yes, three points
Was the acquisition identified in July 2017 report?	0 or 3	If yes, three points
Government Accountability Office (GAO)		
Did GAO's high-risk list include the acquisition?[e]	0 or 3	If yes, three points
Was the overall purpose of the acquisition included within GAO's high-risk list?	0 or 2	If yes, two points
Was the acquisition included in the scope of past/current/planned GAO audits?	0 or 1	If yes, one point
Was the acquisition identified as high-priority by GAO subject matter experts?	0 or 3	If yes, three points
Was the acquisition reported by the agency as one of their critical legacy systems most in need of modernization?[f]	0 or 1	If yes, one point
Was the acquisition selected by GAO as one of the most critical legacy systems in need of modernization?	0 or 2	If yes, two points
Critical Infrastructure Sectors[g]		
Is the acquisition related to one of the 16 critical infrastructure sectors?	0 to 16	One point for each critical infrastructure sector for a total of 16 possible points
Scope of End Users		
What type of end users will use the acquisition (e.g., agency-wide, component-specific, public, specific public users, military, other agencies, and/or international)?	1 or 2	2 points if the public is the end user and 1 point for any other group of end users
Designation of Mission-Critical		
Does the acquisition meet the definition provided in the questionnaire of "mission-critical?"[h]	1 to 3	3 points if definition met and 1 point if definition not met
Was the acquisition formally designated as 'mission-critical' by the agency?	0 or 2	If yes, two points
Cost		
What is the acquisition's total life cycle cost?	1 to 3	Acquisitions with total life cycle cost of $100 million or higher were given 3 points, $100 to $50 million were given 2 points, and below $50 million were given 1 point
What percentage of the agency's yearly 2019 IT budget has been allotted to this acquisition?	1 to 3	Acquisitions with a larger percentage of the budget earn more points
Is the agency sharing the development costs and/or management of this acquisition with another federal agency?	0 or 1	If yes, one point
Agency Oversight		
Which department(s) within the agency is/are responsible for the oversight of this acquisition?	1 to 3	Acquisitions with an established governance structure received higher points.

Criteria categories and attributes	Points	Point value description
Does the CIO provide any level of oversight of this acquisition?	1 to 3	Point value was based on the impact of the CIO's roles and responsibilities on the acquisition. An acquisition received more points if the CIO had a large impact.
OMB Oversight		
Has the agency conducted a TechStat session related to the acquisition that it supports?[i]	0 or 2	If yes, two points
GAO determination of the significance of the TechStat session.	1 to 3	Points based on professional judgment. 3 points if very significant, 2 points if moderately significant, and 1 point if not very significant
Has the agency met with officials from OMB regarding oversight of the acquisition that it supports?	0 or 2	If yes, two points
How often did the meetings with OMB occur?	1 to 3	Meetings that occurred at a greater frequency earn more points
GAO determination of the significance of OMB meetings.	1 to 3	Points based on professional judgment. 3 points if very significant, 2 points if moderately significant, and 1 point if not very significant
Has OMB conducted a PortfolioStat for the acquisition that it supports?	0 or 2	If yes, two points
GAO determination of the significance of the PortfolioStat.	1 to 3	Points based on professional judgment. 3 points if very significant, 2 points if moderately significant, and 1 point if not very significant
Does the agency expect to identify this acquisition as a high value asset?[j]	0 or 6	If yes, six points
Capabilities and Acquisition Type		
What services and capabilities are to be provided by the asset under this acquisition?	1 to 3	One point if the acquisition's services affect the agency's mission and three points if it has national implications
Was the acquisition designated as a major acquisition?[k]	0 or 2	If yes, two points
What type of acquisition was this?	1 to 3	3 points if the acquisition is a new asset with new capabilities, 2 points if it is a replacement of a legacy system, and 1 point if it is an enhancement or component to an existing system
Potential Risks to the Agency and Nation[l]		
Did the agency report that there would be an adverse impact on the agency and its mission if it were terminated before the work was completed?	0 or 1	If yes, one point
Level of impact to the agency based on GAO analysis	1 to 3	3 points if the impact was high, 2 points if the impact was medium, and 1 point if it was low
Did the agency report that the acquisition would have an impact on the nation's public health and safety once deployed/placed in production?	0 or 3	If yes, three points

Criteria categories and attributes	Points	Point value description
Impact on the nation's public health and safety based on GAO analysis	1 to 3	3 points if the impact was high, 2 points if the impact was medium, and 1 point if it was low
How did the agency report the organizational risk associated with this acquisition?	0 to 6	6 points if very risky, 4 points if moderately risky, 2 points if low risk, and 0 points for not risky or not applicable/no basis to judge
How did the agency report the information security risk associated with this acquisition?	0 to 3	3 points if very risky, 2 points if moderately risky, 1 point if low risk, and 0 points for not risky or not applicable/no basis to judge
How did the agency report the information privacy risk associated with this acquisition?	0 to 3	3 points if very risky, 2 points if moderately risky, 1 point if low risk, and 0 points for not risky or not applicable/no basis to judge
How did the agency report the technical risk associated with this acquisition?	0 to 3	3 points if very risky, 2 points if moderately risky, 1 point if low risk, and 0 points for not risky or not applicable/no basis to judge
How did the agency report the cost/budget risk associated with this acquisition?	0 to 3	3 points if very risky, 2 points if moderately risky, 1 point if low risk, and 0 points for not risky or not applicable/no basis to judge
How did the agency report the scheduling risk associated with this acquisition?	0 to 3	3 points if very risky, 2 points if moderately risky, 1 point if low risk, and 0 points for not risky or not applicable/no basis to judge
How did the agency report the risk of not implementing this acquisition?	0 to 6	6 points if very risky, 4 points if moderately risky, 2 points if low risk, and 0 points for not risky or not applicable/no basis to judge

Source: GAO analysis | GAO-20-249SP

[a]The National Essential Functions used for these criteria can be found in 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 IT investments to further improve the transparency into and oversight of federal agencies' IT investments.

[c]President's Management Council and Executive Office of the President, President's Management Agenda (Washington, D.C.: Mar. 20, 2018).

[d]OMB, Quarterly Report to Congress: 10 High Priority Programs Quarterly Report (Washington, D.C.: June 25, 2015) and Report to Congress: 10 High Priority Programs (Washington, D.C.: June 9, 2016); United States Digital Service, The U.S. Digital Service Report to Congress, December 2016 and The U.S. Digital Service Report to Congress, July 2017.

[e]See GAO, High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019); High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation, GAO-18-622 (Washington, D.C.: Sept. 6, 2018); High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others, (Washington, D.C.: Feb. 15, 2017); and High-Risk Series: An Update, GAO-15-290 (Washington, D.C. Feb. 11, 2015).

[f]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 in most need of modernization.

[g]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 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.

[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]At the time of our analysis, the Office of Management and Budget's memorandum M-17-09 was in place and defined High Value Assets as those assets, federal information systems, information and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause 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. This memorandum and definition has been rescinded and replaced by M-19-03.

[k]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.

[l]GAO, Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-Making, GAO/AIMD-10.1.13 (Washington, D.C.: Feb. 3, 1997.

To apply the selection criteria to each acquisition, we analyzed information regarding the acquisitions from agency-provided questionnaire responses, the IT Dashboard, and prior reports that OMB, the Inspectors General, and we have issued. For each acquisition, we used this information to assign the associated point values for the criteria we developed.

To refine the list of acquisitions to be highlighted in the report, we calculated the total point values associated with the criteria for each identified acquisition. We then selected acquisitions with a total point value of at least 75 points (20 total acquisitions) based on a natural breaking point provided by our analysis for this report. To further refine the list and provide a larger representation of agencies' acquisitions across the federal government, we selected to the two highest-rated IT

acquisitions per agency.[6] This resulted in a final list of 16 GAO-selected mission-critical IT acquisitions. These acquisitions are being undertaken by 12 of the 24 agencies covered under the *Chief Financial Officers Act of 1990*. We consulted with the former Federal CIO on the final list to confirm that the acquisitions we selected were critical to federal government operations.

To obtain more detailed information on the selected acquisitions and their current implementation status, we provided the relevant agencies with a second questionnaire based on our analysis of the agency's initial responses. This questionnaire included inquiries on the basis for initiating the acquisition, including the current implementation status with a timeline of key milestones; the acquisition's governance structure; cost and budget data; project performance measures; acquisition workforce data; and risk factors and challenges. We also requested that the agencies provide supporting documentation, which included project plans and schedules, acquisition and risk plans, governance charters, and cost estimates. We then analyzed the information provided by the agency along with the supporting documentation to describe the IT acquisitions and their key attributes.

The profiles and the data presented in this report reflect key attributes of the selected federal IT acquisitions as of August 2020, unless otherwise noted. We conducted this performance audit from February 2018 to September 2020 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.

[6]We also excluded acquisitions that no longer had planned development work at the time of our review.

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' information technology (IT) acquisitions, we administered a questionnaire to the 24 major agencies covered by the Chief Financial Officers Act of 1990, from May 2018 through August 2018.[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 Questionnaire: Nation's Top Mission Critical Acquisitions Supported by Information Technology

The Government Accountability Office (GAO) is conducting this questionnaire 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 102614. We need your help in identifying the top five acquisitions that are supported by IT in your agency that are considered to be mission critical.

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 a "mission critical acquisition supported by IT" 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.

Acquisition: According to the Federal Acquisition Regulation (FAR), 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.

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

1. What is the total number of acquisitions your agency currently has in process that are supported by IT (initiation/need to pre-deployment/pre-production (before an acquisition is delivered and goes live), as of May 2018)? Click here to enter text.
   a. How many are new acquisitions (i.e., new systems or other assets with new capabilities—not replacing old systems)? Click here to enter text.
   b. How many are acquisitions that are replacing legacy/outdated systems? Click here to enter text.
   c. How many are enhancements or components of already existing systems? Click here to enter text.

2. What are your top 5 mission critical acquisitions (include only those acquisitions that are in the pre-deployment/pre-production phase) supported by IT? (Please complete Section B for each acquisition listed below):
   a. Name of mission critical acquisition #1 and its associated unique investment identifier[1]: Click here to enter text.

[1]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.

1

b. Name of mission critical acquisition #2 and its associated unique investment identifier: Click here to enter text.
c. Name of mission critical acquisition #3 and its associated unique investment identifier: Click here to enter text.
d. Name of mission critical acquisition #4 and its associated unique investment identifier: Click here to enter text.
e. Name of mission critical acquisition #5 and its associated unique investment identifier: Click here to enter text.

Section B. Profile of Mission Critical Acquisition Number Click here to enter text. **of 5:**
Name of Acquisition: Click here to enter text.

Background and Systems Development

Please provide your responses and corresponding documentation, if any, to the questions below for each acquisition listed in question #2:

1. Who is/are the point(s) of contact responsible for filling out this acquisitions profile?
   a. Name: Click here to enter text.
   b. Title: Click here to enter text.
   c. Office/team: Click here to enter text.
   d. Telephone: Click here to enter text.
   e. Email: Click here to enter text.

2. How does this acquisition fit into the definition provided for "mission critical?" Click here to enter text.
   a. Before this survey, was this acquisition formally designated as 'mission critical' by the agency? ☐ Yes ☐ No ☐ Other: Click here to enter text. ☐ Don't know

3. What are the total anticipated life cycle costs[2] for this acquisition? Click here to enter text.

4. Is your agency sharing the development costs and/or management of this acquisition with another federal agency? ☐ Yes ☐ No ☐ Other: Click here to enter text.
   a. If yes, please describe this relationship: Click here to enter text.

5. What is the scope of this acquisition?
   ☐ Agencywide
   ☐ Component/bureau specific — please list all applicable components/bureaus: Click here to enter text.
   ☐ Other: Click here to enter text.

6. When was the contract for this acquisition initiated? Click here to enter text.

7. When does your agency expect the work under this acquisition to be placed into deployment/production? Click here to enter text.

8. What department(s) within your agency is/are responsible for the oversight of this acquisition? Click here to enter text.

[2]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.

2

9. Has your agency conducted a TechStat[3] session related to this asset 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: Click here to enter text.

10. 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? Click here to enter text.
    b. If yes, please describe the nature and purpose of these meetings: Click here to enter text.

11. Has OMB conducted a PortfolioStat[4] 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: Click here to enter text.

12. Has OMB identified this acquisition, or the investment that it supports, as a "High Impact Program?" ☐ Yes ☐ No ☐ Don't know

13. Does your agency expect to identify this asset as a high value asset?[5] ☐ Yes ☐ No ☐ Don't know

14. What department(s) within your agency is/are responsible for the budget of this acquisition? Click here to enter text.

15. What department(s) within your agency is/are responsible for funding this acquisition? Click here to enter text.

16. What services and capabilities are to be provided by the asset under this acquisition? Click here to enter text.

17. Is this acquisition designated as:
    ☐ a major acquisition?[6]
    ☐ a non-major acquisition?
    ☐ Other: Click here to enter text.
    a. Please describe how your agency defines the acquisition type selected above: Click here to enter text.

18. Is this acquisition:
    ☐ a new asset with new capabilities?
    ☐ a replacement of a legacy system?
    ☐ an enhancement or component to an existing system?
    ☐ Other: Click here to enter text.

19. Which of the following under this acquisition were used to develop this asset? (select all that apply):
    ☐ Customized development by agency personnel
    ☐ Contractor developed

[3]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.
[4]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.
[5]"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.
[6]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.

☐ Commercial off-the-shelf (COTS)
☐ Open source software
☐ Other: Click here to enter text.

20. Which of the following type(s) of system development life cycle methodologies under this acquisition is/are being used to develop this asset (select all that apply)?
☐ Waterfall[7]
☐ Spiral[8]
☐ Agile software development[9]
☐ Rapid prototyping[10]
☐ Other incremental[11]
☐ Not applicable/no basis to judge
☐ Other: Click here to enter text.

Potential risks

Questions in this section are intended to collect information regarding the agency's perceived and potential risk for each attribute listed below regarding the mission critical acquisition(s) identified above (Question 2). Provide your responses and corresponding documentation, if any, to the following questions:

21. What impact would this acquisition have on your agency and its mission if it were terminated before the work was completed? Click here to enter text.

22. What impact, if any, will this acquisition have on the nation's public health and safety once deployed/placed in production? Click here to enter text.

23. 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	☐	☐	☐	☐	☐
Information security risk	☐	☐	☐	☐	☐
Information privacy risk	☐	☐	☐	☐	☐
Technical risk	☐	☐	☐	☐	☐
Cost/budget risk	☐	☐	☐	☐	☐

[7]A traditional waterfall development approach effort is usually broadly scoped, multiyear, and produces a product at the end of a sequence of phases.
[8]A spiral development approach is characterized by repeatedly iterating a set of elemental development processes and managing risk so it is actively being reduced. As part of this model, a prototype is developed or revised whenever a risk analysis shows that significant areas of uncertainty remain that pose substantial risks to project success.
[9]Agile software development calls for the delivery of software in small, short increments rather than in the typically long, sequential phases of a traditional waterfall approach. Agile emphasizes this early and continuous software delivery, as well as using collaborative teams, and measuring progress with working software.
[10]Rapid prototyping is based on prototyping and iterative development with no specific planning involved. It is a merger of various structured techniques, with prototyping techniques to accelerate software systems development.
[11]An incremental development approach delivers software products in smaller modules with shorter time frames.

Schedule risk	☐	☐	☐	☐	☐
Risk of not implementing this acquisition	☐	☐	☐	☐	☐
Other (specify): Click here to enter text.	☐	☐	☐	☐	☐

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.

Information security 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 information 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 information 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 information 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.
- 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 can 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.

5

- 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.

Appendix III: Comments from the Social Security Administration

SOCIAL SECURITY
Office of the Commissioner

August 5, 2020

Ms. Carol C. Harris
Director, Information Technology
Acquisition Management Issues
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Director Harris:

Thank you for the opportunity to review the draft report, "INFORMATION TECHNOLOGY: Key Attributes of Essential Federal Mission-Critical Acquisitions" (GAO-20-249SP).

The Disability Case Processing System 2 (DCPS2) is part of an enterprise-wide integration of an electronic case processing system across Social Security Administration (SSA) offices and disability determination services (DDS) sites. In looking to the future and maximizing the benefits of a common, national system, on July 14, 2020, the Commissioner of Social Security finalized the determination that DCPS2 will be the disability case processing system used by all DDSs to adjudicate SSA's disability determinations. Implementing DCPS2 as the national, common case processing system will improve public service, modernize disability determination processes, and increase information security.

If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Stephanie Hall

Stephanie Hall
Chief of Staff

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Appendix IV: 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: Nicole Jarvis (assistant director), Ashfaq Huda (analyst in charge), Amy Apostol, Chris Businsky, Sharhonda Deloach, Kristi Dorsey, Nancy Glover, Lee Hinga, Franklin Jackson, Scott Pettis, David Powner, Kelly Rubin, Roger Smith, Whitney Starr, Andrew Stavisky, and Jessica Waselkow.

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, Twitter, 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/fraudnet/fraudnet.htm

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

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

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