U.S. GOVERNMENT ACCOUNTABILITY OFFICE

INFORMATION TECHNOLOGY

Key Attributes of Essential Federal Mission-Critical Acquisitions

Report to Congressional Requesters

September 2020
GAO-20-249SP

Accessible Version

Contents

Letter 1

Background 5
Key Attributes of Selected Mission-Critical IT Acquisitions 13
Agency Comments and Our Evaluation 51

Appendix I: Objective, Scope, and Methodology 54

Appendix II: Copy of the Questionnaire that GAO Administered to the 24 Agencies Covered by the Chief Financial Officers Act 63

Appendix III: Comments from the Social Security Administration 70

Agency Comment Letter 71

Appendix IV: GAO Contact and Staff Acknowledgments 72

GAO Contact 72
Staff Acknowledgments 72

Tables

Table 1: Federal Agency Mission-Critical Information Technology Acquisitions 14
Table 2: GAO Selection Criteria Categories and their Point Values 57

Figure

Figure 1: Illustration of Acquisition Profile 19

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

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

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

[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.

lack of disciplined and effective management, such as in planning projects, defining requirements, and overseeing and governing programs.

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

[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.

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 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.

[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).

[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.

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 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

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

[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.

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:

- **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

[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.

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-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

[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).

[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).

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 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]

[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).

[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.

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.
- **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.

[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).

- **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

[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.

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 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

[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.

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 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

[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.

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 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

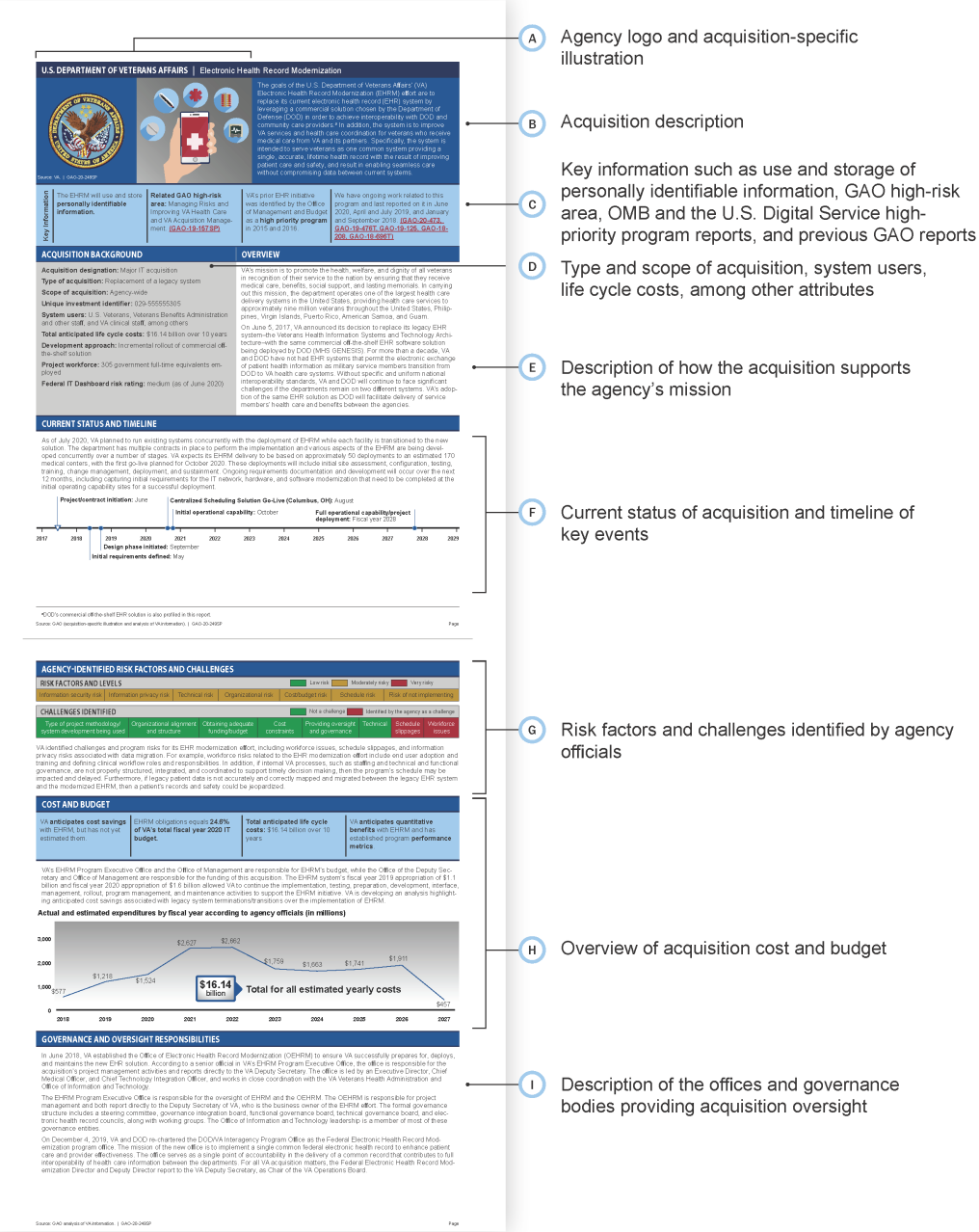
[35]Commercial off-the-shelf software is sold in substantial quantities in the commercial marketplace and is purchased without modification, or with minimal modification, to its original form.

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

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

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

[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.

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 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

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

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 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

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

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.

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.

3

☐ 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.

6

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

Agency Comment Letter

Text of Appendix III: Comments from the Social Security Administration

Page 1

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
Chief of Staff

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

Please Print on Recycled Paper.

U.S. GOVERNMENT
ACCOUNTABILITY
OFFICE