United States Government Accountability Office

Report to Congressional Requesters

June 2019

INFORMATION TECHNOLOGY

Agencies Need to Develop Modernization Plans for Critical Legacy Systems

GAO-19-471

June 2019

INFORMATION TECHNOLOGY

Agencies Need to Develop Modernization Plans for Critical Legacy Systems

GAO Highlights

Highlights of GAO-19-471, a report to congressional requesters

Why GAO Did This Study

The federal government plans to spend over $90 billion in fiscal year 2019 on IT. About 80 percent of this amount is used to operate and maintain existing IT investments, including aging (also called legacy) systems. As they age, legacy systems can be more costly to maintain, more exposed to cybersecurity risks, and less effective in meeting their intended purpose.

GAO was asked to review federal agencies' legacy systems. This report (1) identifies the most critical federal legacy systems in need of modernization and evaluates agency plans for modernizing them, and (2) identifies examples of legacy system modernization initiatives that agencies considered successful.

To do so, GAO analyzed a total of 65 legacy systems in need of modernization that 24 agencies had identified. Of these 65, GAO identified the 10 most in need of modernization based on attributes such as age, criticality, and risk. GAO then analyzed agencies' modernization plans for the 10 selected legacy systems against key IT modernization best practices.

The 24 agencies also provided 94 examples of successful IT modernizations from the last 5 years. In addition, GAO identified other examples of modernization successes at these agencies. GAO then selected a total of five examples to highlight a mix of system modernization types and a range of benefits realized.

This is a public version of a sensitive report that is being issued concurrently. Information that agencies deemed sensitive has been omitted.

View GAO-19-471. For more information, contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov.

What GAO Found

Among the 10 most critical legacy systems that GAO identified as in need of modernization (see table 1), several use outdated languages, have unsupported hardware and software, and are operating with known security vulnerabilities. For example, the selected legacy system at the Department of Education runs on Common Business Oriented Language (COBOL)—a programming language that has a dwindling number of people available with the skills needed to support it. In addition, the Department of the Interior's system contains obsolete hardware that is not supported by the manufacturers. Regarding cybersecurity, the Department of Homeland Security's system had a large number of reported vulnerabilities, of which 168 were considered high or critical risk to the network as of September 2018.

Table 1: The 10 Most Critical Federal Legacy Systems in Need of Modernization

Agency	System name[a]	Age of system, in years	Age of oldest hardware, in years	System criticality (according to agency)	Security risk (according to agency)
Department of Defense	System 1	14	3	Moderately high	Moderate
Department of Education	System 2	46	3	High	High
Department of Health and Human Services	System 3	50	Unknown[b]	High	High
Department of Homeland Security	System 4	8 – 11[c]	11	High	High
Department of the Interior	System 5	18	18	High	Moderately high
Department of the Treasury	System 6	51	4	High	Moderately low
Department of Transportation	System 7	35	7	High	Moderately high
Office of Personnel Management	System 8	34	14	High	Moderately low
Small Business Administration	System 9	17	10	High	Moderately high
Social Security Administration	System 10	45	5	High	Moderate

Source: GAO analysis of agency data. | GAO-19-471

[a]Due to sensitivity concerns, GAO substituted a numeric identifier for the system names.

[b]The agency stated that the system's hardware had various refresh dates and was not able to identify the oldest hardware.

[c]The agency stated that the majority of the network's hardware was purchased between 2008 and 2011.

Of the 10 agencies responsible for these legacy systems, seven agencies (the Departments of Defense, Homeland Security, the Interior, the Treasury; as well as the Office of Personnel Management; Small Business Administration; and Social Security Administration) had documented plans for modernizing the systems (see table 2). The Departments of Education, Health and Human Services, and Transportation did not have documented modernization plans. Of the seven agencies with plans, only the Departments of the Interior and Defense's modernization plans included the key elements identified in best practices (milestones, a description of the work necessary to complete the modernization, and a plan for the disposition of the legacy system). Until the

What GAO Recommends

In the sensitive report, GAO is making a total of eight recommendations—one to each of eight agencies—to ensure that they document modernization plans for the selected legacy systems.

The eight agencies agreed with GAO's findings and recommendations, and seven of the agencies described plans to address the recommendations.

other eight agencies establish complete modernization plans, they will have an increased risk of cost overruns, schedule delays, and project failure.

Table 2: Extent to Which Agencies' Legacy System Documented Modernization Plans Included Key Elements

Agency	System name[a]	Includes milestones to complete the modernization	Describes work necessary to modernize system	Summarizes planned disposition of legacy system
Department of Defense	System 1	Yes	Yes	Yes
Department of Education	System 2	No modernization plan		
Department of Health and Human Services	System 3	No modernization plan		
Department of Homeland Security	System 4	No	Yes	No
Department of the Interior	System 5	Yes	Yes	Yes
Department of the Treasury	System 6	Partial	Yes	No
Department of Transportation	System 7	No modernization plan		
Office of Personnel Management	System 8	Partial	Partial	No
Small Business Administration	System 9	Yes	No	Yes
Social Security Administration	System 10	Partial	Partial	No

Source: GAO analysis of agency data. | GAO-19-471

Agencies received a "partial" if the element was completed for a portion of the modernization.

[a]Due to sensitivity concerns, GAO substituted a numeric identifier for the system names.

The five examples that GAO selected of successful information technology (IT) modernization initiatives included transforming legacy code into a more modern programming language and moving legacy software to the cloud. Doing so allowed the agencies to reportedly leverage IT to successfully address their missions and achieve a wide range of benefits, including cost savings.

Contents

Tables

Figures

Abbreviations

CIO	Chief Information Officer
COBOL	Common Business Oriented Language
DHS	Department of Homeland Security
DOD	Department of Defense
Education	Department of Education
Energy	Department of Energy
FAA	Federal Aviation Administration
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
ICS	Industrial Control System
IRS	Internal Revenue Service
IT	information technology
Interior	Department of the Interior
Justice	Department of Justice
LOUO	limited official use only
MGT	Modernizing Government Technology
NRC	Nuclear Regulatory Commission
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
SCADA	Supervisory Control and Data Acquisition
SBA	Small Business Administration
SSA	Social Security Administration
State	Department of State
Transportation	Department of Transportation
Treasury	Department of the Treasury
VA	Department of Veterans Affairs

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

June 11, 2019

Congressional Requesters

According to the President's Budget, the federal government plans to spend over $90 billion in fiscal year 2019 on information technology (IT).[1] Of this amount, the government plans to spend about 80 percent on the operations and maintenance of existing IT investments, including aging (also called legacy) systems.[2]

However, federal legacy systems are becoming increasingly obsolete. In May 2016, we reported that many of the government's IT investments used outdated software languages and hardware parts that were unsupported.[3] We also reported instances where agencies were using systems that had components that were at least 50 years old or the vendors were no longer providing support for hardware or software. As they age, legacy systems can become more expensive to maintain, more exposed to cybersecurity risks, and less effective in accomplishing their intended purpose.

Accordingly, you asked us to review federal agencies' legacy systems. Our specific objectives were to (1) identify the most critical federal legacy systems in need of modernization and evaluate plans for modernizing them, and (2) identify examples of legacy system modernization initiatives in the last 5 years that agencies considered successful.

This report presents a public version of a "limited official use only" (LOUO) report that we are also issuing today.[4] The Department of Homeland Security (DHS) and the Department of the Interior (Interior)

[1]Office of Management and Budget, *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2019* (Washington, D.C.: 2018) and Department of Defense, *Information Technology and Cyberspace Activities Budget Overview, Fiscal Year 2019 President's Budget Request*, (March 2018).

[2]The Modernizing Government Technology (MGT) Act defines a legacy IT system as a system that is outdated or obsolete. *National Defense Authorization Act for Fiscal Year 2018*, Pub. L. No. 115-91, Div. A, Title X, Subtitle G (2017).

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

[4]GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-351SU (Washington, D.C.: June 11, 2019).

determined that certain information in our original report should be protected from public disclosure. Therefore, we will not release the LOUO report to the general public because of the sensitive information it contains.

The LOUO report includes eight recommendations that we made to eight agencies to identify and document modernization plans for particular legacy systems, including milestones, a description of the work necessary, and details on the disposition of the legacy system.[5] In this public version of the report, we have omitted sensitive information regarding particular legacy systems, including the systems' names and other information that would identify the systems.

Although the information provided in this report is more limited, this report addresses the same objectives as the LOUO report and is based on the same audit methodology. We provided a draft of this report to agency officials to obtain their review and comments on the sensitivity of the information contained herein. We confirmed with the agency officials that this report can be made available to the public without jeopardizing the security of federal agencies' legacy systems.

To identify the most critical legacy systems in need of modernization, we followed up with each of the 24 federal agencies' covered by the Chief Financial Officers Act of 1990 regarding their legacy systems that they had identified in 2017 as most in need of modernization.[6] All 24 agencies either confirmed or updated their lists of these systems most in need of modernization. This resulted in a collective list of 65 systems.

[5]We made recommendations to the Departments of Education, Health and Human Services, Homeland Security, Transportation, the Treasury; the Office of Personnel Management; Small Business Administration; and Social Security Administration.

[6]The 24 major federal agencies covered by the Chief Financial Officers Act of 1990 are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development. 31 U.S.C. §90l(b).

We then reviewed available technical literature[7] and consulted with system development experts within GAO to develop a set of attributes for determining system obsolescence and their need for modernization. These attributes included a system's age, hardware age, operating and labor costs, vendor warranty and support status, and security risk.[8] We assigned point values to each system based on the systems' agency-reported attributes. We totaled each system's assigned point values and used the results to rank the 65 legacy systems. We then designated the 10 systems with the highest scores as those legacy systems most in need of modernization.[9] However, due to sensitivity concerns, in this report we substituted a numeric identifier for the system names and are not providing detailed descriptions.

To evaluate agencies' plans for modernizing the 10 federal legacy systems most in need of modernization, we requested that the relevant agencies provide us with their documented plans for modernizing the selected systems. We reviewed government and industry best practices related to the modernization of legacy systems.[10] Based on our reviews of these documents, we determined that agencies' documented plans for system modernization should include, at a minimum, (1) milestones to

[7]Our review of literature included General Services Administration, Unified Shared Services Management, *Modernization and Migration Management (M3) Playbook* (Aug. 3, 2016); *M3 Playbook Guidance* (Aug. 3, 2016); American Technology Council, *Report to the President on Federal IT Modernization* (Dec. 13, 2017); Office of Management and Budget, *Management of Federal High Value Assets*, M-17-09 (Washington, D.C.: Dec. 9, 2016); American Council for Technology-Industry Advisory Council, *Legacy System Modernization: Addressing Challenges on the Path to Success* (Fairfax, VA: Oct. 7, 2016); and Dr. Gregory S. Dawson, Arizona State University, IBM Center for The Business of Government, *A Roadmap for IT Modernization in Government* (Washington, D.C.: 2018).

[8]A legacy system may run on updated hardware, and thus, the system's age and hardware age may not be the same.

[9]The 10 agencies with the most critical legacy systems in need of modernization are the Departments of Defense, Education, Health and Human Services, Homeland Security, the Interior, the Treasury, and Transportation; the Office of Personnel Management; the Small Business Administration; and the Social Security Administration.

[10]General Services Administration, Unified Shared Services Management, *Modernization and Migration Management (M3) Playbook* (Aug. 3, 2016); *M3 Playbook Guidance* (Aug. 3, 2016); American Technology Council, *Report to the President on Federal IT Modernization* (Dec. 13, 2017); Office of Management and Budget, *Management of Federal High Value Assets*, M-17-09 (Washington, D.C.: Dec. 9, 2016); American Council for Technology-Industry Advisory Council, *Legacy System Modernization: Addressing Challenges on the Path to Success* (Fairfax, VA: Oct. 7, 2016); and Dr. Gregory S. Dawson, Arizona State University, IBM Center for The Business of Government, *A Roadmap for IT Modernization in Government* (Washington, D.C.: 2018).

complete the modernization, (2) a description of the work necessary to modernize the system, and (3) details regarding the disposition of the legacy system. We then analyzed agencies' documented modernization plans for the selected legacy systems to determine whether the plans included these elements. We supplemented our work with interviews of officials in the agencies' offices of the Chief Information Officer (CIO) and program offices for the selected legacy systems.

To identify legacy system modernization initiatives that agencies indicated were successful, we asked each of the 24 agencies to provide us with examples of those modernization initiatives that they completed between 2014 and 2018 and deemed to be successful. In addition, we identified other examples of modernization successes at these agencies. We also coordinated with the selected agencies' Offices of Inspector General (OIG) to determine whether those offices had any past or current audit work that would contradict the agencies' determination that the initiatives were successful. We then selected initiatives that reflected a mix of different agencies, types of system modernizations undertaken, and types of benefits realized from the initiatives. A full description of our objectives, scope, and methodology can be found in appendix I.

We conducted this performance audit from January 2018 to June 2019 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

Historically, the federal government has had difficulties acquiring, developing, and managing IT investments.[11] Further, federal agencies have struggled with appropriately planning and budgeting for modernizing legacy systems; upgrading underlying infrastructure; and investing in high quality, lower cost service delivery technology. The consequences of not updating legacy systems has contributed to, among other things, security risks, unmet mission needs, staffing issues, and increased costs.

[11]As a result of the many issues the federal government has experienced, we identified "Improving the Management of IT Acquisitions and Operations" as a high-risk area in February 2015. GAO, *High-Risk Series: An Update,* GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

- **Security risks.** Legacy systems may operate with known security vulnerabilities that are either technically difficult or prohibitively expensive to address. In some cases, vendors no longer provide support for hardware or software, creating security vulnerabilities and additional costs. For example, in November 2017, the Department of Education's (Education) Inspector General identified security weaknesses that included the department's use of unsupported operating systems, databases, and applications.[12] By using unsupported software, the department put its sensitive information at risk, including the personal records and financial information of millions of federal student aid applicants.[13]
- **Unmet mission needs.** Legacy systems may not be able to reliably meet mission needs because they are outdated or obsolete. For instance, in 2016, the Department of State's (State) Inspector General reported on the unreliability of the Bureau of Consular Affairs' legacy systems.[14] Specifically, during the summers of 2014 and 2015, outages in the legacy systems slowed and, at times, stopped the processing of routine consular services such as visa processing. For example, in June 2015, system outages caused by a hardware failure halted visa processing for 13 days, creating a backlog of 650,000 visas.
- **Staffing issues.** In order to operate and maintain legacy systems, staff may need experience with older technology and programming languages, such as the Common Business Oriented Language (COBOL).[15] Agencies have had difficulty finding employees with such knowledge and may have to pay a premium to hire specialized staff or contractors. For example, we reported in May 2016 that the Social Security Administration (SSA) had to rehire retired employees to

[12]Department of Education, Office of Inspector General, *FY 2018 Management Challenges*, (Washington, D.C.: November 2017).

[13]According to Education's Office of General Counsel, Education has developed corrective action plans to address the Inspector General's recommendation.

[14]U.S. Department of State, Office of Inspector General, *Inspection of the Bureau of Consular Affairs, Office of Consular Systems and Technology*, ISP-I-17-04, (Arlington, VA: December 2016).

[15]COBOL, which was introduced in 1959, became the first widely used, high-level programming language for business applications. The Gartner Group, a leading IT research and advisory company, has reported that organizations using COBOL should consider replacing the language, as procurement and operating costs are expected to steadily rise, and because there is a decrease in people available with the proper skill sets to support the language.

maintain its COBOL systems.[16] Further, having a shortage of expert personnel available to maintain a critical system creates significant risk to an agency's mission. For instance, we reported in June 2018 that the Internal Revenue Service (IRS) was experiencing shortages of staff with the skills to support key tax processing systems that used legacy programming languages.[17] These staff shortages not only posed risks to the operation of the key tax processing systems, but they also hindered the agency's efforts to modernize its core tax processing system.

- **Increased costs.** The cost of operating and maintaining legacy systems increases over time. The issue of cost is linked to the three previously described consequences—either because the other issues directly raise costs or, as in the case of not meeting mission needs, the agency is not receiving a favorable return on investment. Further, in an era of constrained budgets, the high costs of maintaining legacy systems could limit agencies' ability to modernize and develop new or replacement systems.

During the course of our review, agencies reported that they consider several factors prior to deciding whether to modernize a legacy system. In particular, agencies evaluate factors, such as the inherent risks, the criticality of the system, the associated costs, and the system's operational performance.

- **Risks.** Agencies consider the risks associated with maintaining the legacy system as well as modernizing the legacy system. For instance, agencies may prioritize the modernization of legacy systems that have security vulnerabilities or software that is unsupported by the vendor.[18] However, limited system accessibility may also reduce the need to modernize a legacy system. For example, air-gapped systems, which are systems that are isolated from the internet, may

[16]GAO-16-468.

[17]GAO, *Information Technology: IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing,* GAO-18-298 (Washington, D.C.: June 28, 2018).

[18]When computer systems or software are no longer supported, the vendor of the product ceases to provide patches, security fixes, or updates, leaving system vulnerabilities open to exploitation.

mitigate a legacy system's cybersecurity risk by preventing remote hackers from having system access.[19]

Conversely, we have also reported that air-gapped systems are not necessarily secure: they could potentially be accessed by other means than the internet, such as through Universal Serial Bus devices.[20] Even so, removing the threat of remote access is a mitigation technique used by agencies such as the Nuclear Regulatory Commission (NRC). According to NRC, the agency reduced the riskiness of using computers with unsupported operating systems by putting these computers on isolated networks or by disconnecting them from networks entirely.

- **Criticality.** Agencies consider how critical the system is to the agency's mission. Several agencies stated that they would consider how essential a legacy system is to their agencies' missions before deciding to modernize it. For example, the Department of Health and Human Services (HHS) stated that, when deciding to modernize a legacy system, it considers the degree to which core mission functions of the agency or other agencies are dependent on the system. Similarly, Department of Energy (Energy) officials noted that the department is required to maintain several legacy systems associated with the storage of its nuclear waste.
- **Costs.** Agencies consider the costs of maintaining a legacy system and modernizing the system. For example, according to the Department of Veterans Affairs (VA), there are systems for which a life-cycle cost analysis of the legacy system may show that the cost to modernize exceeds the projected costs to maintain the system. Similarly, the Department of Defense (DOD) noted that, before deciding on a modernization solution, it is important to assess the costs of the transition to a new or replacement solution.

  An agency also may decide to modernize a system when there is potential for cost savings to be realized with a modernization effort. For example, HHS stated that it may pursue the modernization of a legacy system if the department anticipates reductions in operations

[19]Michael DePhillips and Susan Pepper, "Computer Security – Indirect Vulnerabilities and Threat Vectors (Air-Gap In-depth)" (paper presented at the International Conference on Physical Protection of Nuclear Material and Nuclear Facilities, Vienna, Austria: November 2017).

[20]GAO, *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities,* GAO-19-128 (Washington, D.C.: Oct. 9, 2018).

and maintenance costs due to efficiencies gained through the modernization.

- **Performance.** Before making the decision to modernize, agencies consider the legacy system's operational performance. Specifically, if the legacy system is performing poorly, the agency may decide to modernize it. For example, the Department of Transportation (Transportation) stated that, if a legacy system is no longer functioning properly, it should be modernized. In addition, HHS noted that the ability to improve the functionality of the legacy system could be a reason to modernize it.

GAO Has Reported on the Need to Improve Oversight of Legacy IT

As previously mentioned, in May 2016, we reported that federal legacy IT investments were becoming increasingly obsolete.[21] In this regard, agencies had reported operating systems that used outdated languages and old parts, which were difficult to replace. Further, we noted that each of the 12 selected agencies had reported using unsupported operating systems and components, which could create security vulnerabilities and additional costs.[22] At the time, five of the selected agencies reported using 1980s and 1990s Microsoft operating systems that stopped being supported by the vendor more than a decade ago. We concluded that agencies were, in part, maintaining obsolete investments because they were not required to identify, evaluate, and prioritize investments to determine whether the investments should be kept as-is, modernized, replaced, or retired. We pointed out that the Office of Management and Budget (OMB) had created draft guidance that would require agencies to do so, but OMB had not committed to a firm time frame for when the guidance would be issued.

As such, we made 16 recommendations to OMB and the selected federal agencies to better manage legacy systems and investments. Most agencies agreed with the recommendations or had no comment. However, as of May 2019, 13 recommendations had not been implemented. In particular, OMB has not finalized and issued its draft guidance on legacy systems. Until this guidance is finalized and issued,

[21]GAO-16-468.

[22]The agencies in our 2016 review were the 12 that reported the highest planned IT spending for fiscal year 2015. These agencies were the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Homeland Security, Justice, State, Transportation, the Treasury, and Veterans Affairs; and the Social Security Administration.

the federal government will continue to run the risk of maintaining investments that have outlived their effectiveness and are increasingly difficult to protect from cybersecurity vulnerabilities.

Congress and the Executive Branch Have Made Efforts to Modernize Federal IT

Congress and the executive branch have initiated several efforts to modernize federal IT, including:

- **Identification of High Value Assets.** In a December 2016 memorandum, OMB observed that continued increases in computing power combined with declining computing and storage costs and increased network connectivity had expanded the government's capacity to store and process data.[23] However, OMB noted that this rise in technology and interconnectivity also meant that the federal government's critical networks, systems, and data were more exposed to cyber risks. As a result, OMB issued guidance to assist federal agencies covered by the Chief Financial Officers Act in managing the risks to these assets, which it designated as High Value Assets.[24]

  Subsequently, in December 2018, OMB issued a memorandum that provided further guidance regarding the establishment and enhancement of the High Value Asset program.[25] It stated that the program is to be operated by DHS in coordination with OMB. Further, the new guidance expanded the program to apply to all agencies (i.e., agencies covered by the Chief Financial Officers Act, as well as those not covered by the act) and expanded the definition of High Value

[23]OMB, *Management of Federal High Value Assets*, M-17-09 (Washington, D.C.: Dec. 9, 2016).

[24]OMB's December 2016 memorandum 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 definition replaced a previous definition from OMB Memorandum M-16-04.

[25]OMB, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018). This memorandum rescinded the previous guidance on High Value Assets, M-16-04 and M-17-09.

Assets.[26] The guidance required agencies to identify and report these assets (which may include legacy systems), assess them for security risks, and remediate any weaknesses identified, including those associated with obsolete or unsupported technology.

- **Assessment of federal IT modernization.** On May 11, 2017, the President signed Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.[27] This executive order outlined actions to enhance cybersecurity across federal agencies and critical infrastructure to improve the nation's cyber posture and capabilities against cybersecurity threats. Among other things, the order tasked the Director of the American Technology Council to coordinate a report to the President from the Secretary of DHS, the Director of OMB, and the Administrator of the General Services Administration (GSA), in consultation with the Secretary of Commerce, regarding modernizing federal IT.[28]

  As a result, the *Report to the President on Federal IT Modernization* was issued on December 13, 2017, and outlined the current and envisioned state of federal IT.[29] The report focused on modernization efforts to improve the security posture of federal IT and recognized that agencies have attempted to modernize systems but have been stymied by a variety of factors, including resource prioritization, ability to procure services quickly, and technical issues. The report provided multiple recommendations intended to address these issues through the modernization and consolidation of networks and the use of shared services. In particular, the report recommended that the

[26]According to OMB's December 2018 guidance, an agency may designate federal information or an information system as a High Value Asset when one or more of these categories apply to it: (1) the information or information system that processes, stores, or transmits the information is of high value to the federal government or its adversaries; (2) the agency that owns the information or information system cannot accomplish its primary mission essential functions within expected timelines without the information or information system; and (3) the information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise.

[27]Exec. Order No. 13800, 82 Fed Reg. 22391 (2017).

[28]The American Technology Council was established in May 2017, and has the goal of helping to transform and modernize federal agency IT and how the federal government uses and delivers digital services. The President is the chairman of this council, and the Federal CIO and the United States Digital Service Administrator are among the members.

[29]American Technology Council, *Report to the President on Federal IT Modernization*, (Washington, D.C.: Dec. 13, 2017).

federal government prioritize the modernization of legacy IT by focusing on enhancing security and privacy controls for those assets that are essential for agencies to serve the American people and whose security posture is most vulnerable (i.e., High Value Assets).

- **Enactment of the Modernizing Government Technology (MGT) Act.** To help further agencies' efforts to modernize IT, in December 2017, Congress and the President enacted a law to authorize the availability of funding mechanisms to improve, retire, or replace existing IT systems to enhance cybersecurity and to improve efficiency and effectiveness. The law, known as the MGT Act, authorizes agencies to establish working capital funds for use in transitioning from legacy systems, as well as for addressing evolving threats to information security.[30] The law also created the Technology Modernization Fund, within the Department of the Treasury (Treasury), from which agencies can "borrow" money to retire and replace legacy systems, as well as acquire or develop systems.

  Subsequently, in February 2018, OMB issued guidance for agencies to implement the MGT Act.[31] The guidance was intended to provide agencies additional information regarding the Technology Modernization Fund, and the administration and funding of the related IT working capital funds.[32] Specifically, the guidance allowed agencies to begin submitting initial project proposals for modernization on February 27, 2018.

  In addition, in accordance with the MGT Act, the guidance provides details regarding a Technology Modernization Board, which is to consist of (1) the Federal CIO; (2) a senior official with IT technical expertise from GSA; (3) a member of DHS's National Protection and

[30]*National Defense Authorization Act for Fiscal Year 2018*, Pub. L. No. 115-91, Div. A, Title X, Subtitle G (2017).

[31]OMB, *Implementation of the Modernizing Government Technology Act*, M-18-12 (Washington, D.C.: Feb. 27, 2018).

[32]OMB staff stated that, while the MGT Act authorizes agencies to establish working capital funds, the Act does not confer the transfer authority necessary to operate an IT working capital fund.

Program Directorate;[33] and (4) four federal employees with technical expertise in IT development, financial management, cybersecurity and privacy, and acquisition, appointed by the Director of OMB.[34]

As of February 2019, the Technology Management Fund Board had approved funds for seven IT modernization projects across five agencies: the Department of Agriculture, Energy, the Department of Housing and Urban Development (HUD), the Department of Labor, and GSA. For example, the board approved $20 million for HUD to modernize a mainframe and five COBOL-based applications that are expensive to maintain. According to the board's website, without these funds, HUD would not have been able to pursue this project for several years.

- **Issuance of the President's Management Agenda.** In March 2018, the Administration issued the *President's Management Agenda*, which lays out a long-term vision for modernizing the federal government.[35] The agenda identifies three related drivers of transformation—IT modernization; data, accountability, and transparency; and the workforce of the future—that are intended to push change across the federal government.

  The *President's Management Agenda* identifies 14 related Cross-Agency Priority goals, many of which have elements that involve IT.[36] In particular, the Cross-Agency Priority goal on IT modernization states that modern technology must function as the backbone of how government serves the public in the digital age. Further, the goal on IT modernization provides three priorities that are to guide the Administration's efforts to modernize federal IT: (1) enhancing mission effectiveness by improving the quality and efficiency of critical

[33]The National Protection and Program Directorate was the DHS component responsible for addressing physical and cyber infrastructure protection. The Cybersecurity and Infrastructure Security Agency Act of 2018 renamed the National Protection and Program Directorate to be the Cybersecurity and Infrastructure Security Agency and established a director and responsibilities for the agency.

[34]As of February 2019, these four employees were the Acting Administrator of OMB's U.S. Digital Service, the Small Business Administration's CIO, SSA's CIO, and VA's Chief Technology Officer.

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

[36]Cross-Agency Priority goals were established in response to the GPRA Modernization Act of 2010, Pub. L. No. 111-352, Sec. 5 (Jan. 4, 2011); 124 Stat. 3866, 3873; 31 U.S.C. § 1120(a)(1)(B).

services, including the increased utilization of cloud-based solutions;[37] (2) reducing cybersecurity risks to the federal mission by leveraging current commercial capabilities and implementing cutting edge cybersecurity capabilities; and (3) building a modern IT workforce by recruiting, reskilling, and retaining professionals able to help drive modernization with up-to-date technology.

GAO Identified 10 Critical Federal Legacy Systems; Agencies Often Lack Complete Plans for Their Modernization

As determined by our review of 65 critical federal legacy systems (see appendix II), the 10 most critical legacy systems in need of modernization are maintained by 10 different federal agencies whose missions are essential to government operations, such as emergency management, health care, and wartime readiness.[38] These legacy systems provide vital support to the agencies' missions.

According to the agencies, these legacy systems range from about 8 to 51 years old and, collectively, cost approximately $337 million annually to operate and maintain.[39] Several of the systems use older languages, such as COBOL and assembly language code.[40] However, as we reported in June 2018, reliance on assembly language code and COBOL has risks, such as a rise in procurement and operating costs, and a decrease in the availability of individuals with the proper skill sets.[41]

[37]Cloud computing is a means for delivering computing services via IT networks. When executed effectively, cloud-based solutions can allow agencies to pay for only the IT services used, thus paying less for more services.

[38]To identify the 10 most critical legacy systems in need of modernization, we collected information on 65 of the most critical federal legacy systems and assigned point values based on system attributes, including a system's age, hardware's age, system criticality, and security risk (see appendix II for the full list of 65 systems). We then selected the 10 systems with the highest scores as the most critical legacy systems in need of modernization.

[39]SSA was unable to isolate the costs for just System 10 and, as a result, this number includes the cost of operating some of SSA's other mainframe systems.

[40]As we reported in May 2016, assembly language code is a low-level computer language initially used in the 1950s. Programs written in assembly language are conservative of machine resources and quite fast; however, they are much more difficult to write and maintain than other languages. Programs written in assembly language may only run on the type of computer for which they were originally developed.

[41]GAO, *Information Technology: IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing,* GAO-18-298 (Washington, D.C.: June 28, 2018).

Further, several of these legacy systems are also operating with known security vulnerabilities and unsupported hardware and software. For example, DHS's Federal Emergency Management Agency performed a security assessment on its selected legacy system in September 2018. This review found 249 reported vulnerabilities, of which 168 were considered high or critical risk to the network.

With regard to unsupported hardware and software, Interior's system contains obsolete hardware that is not supported by the manufacturers. Moreover, the system's original hardware and software installation did not include any long-term vendor support. Thus, any original components that remain operational may have had long-term exposure to security and performance weaknesses.

Table 1 provides a generalized list of each of the 10 most critical legacy systems that we identified, as well as agency-reported system attributes, including the system's age, hardware's age, system criticality, and security risk. (Due to sensitivity concerns, we substituted a numeric identifier for the system names and are not providing detailed descriptions). Appendix III provides additional generalized agency-reported details on each of these 10 legacy systems.

Table 1: The 10 Most Critical Federal Legacy Systems in Need of Modernization

Agency	System name[a]	System description[a]	Age of system, in years	Age of oldest hardware, in years	System criticality (according to agency)	Security risk (according to agency)
Department of Defense	System 1	A maintenance system that supports wartime readiness, among other things	14	3	Moderately high	Moderate
Department of Education	System 2	A system that contains student information	46	3	High	High
Department of Health and Human Services	System 3	An information system that supports clinical and patient administrative activities	50	Unknown[b]	High	High
Department of Homeland Security	System 4	A network that consists of routers, switches, and other network appliances	Between 8 and 11[c]	11	High	High
Department of the Interior	System 5	A system that supports the operation of certain dams and power plants	18	18	High	Moderately high
Department of the Treasury	System 6	A system that contains taxpayer information	51	4	High	Moderately low
Department of Transportation	System 7	A system that contains information on aircraft	35	7	High	Moderately high
Office of Personnel Management	System 8	Hardware, software, and service components that support information technology applications and services	34	14	High	Moderately low
Small Business Administration	System 9	A system that controls access to applications	17	10	High	Moderately high
Social Security Administration	System 10	A group of systems that contain information on Social Security beneficiaries	45	5	High	Moderate

Key:

Agencies reported the system criticality and security risk on a scale of 1 to 5 (with 5 being the most critical and the highest risk).

Low-1: According to the agency, system has low security risk or criticality.

Moderately low-2: According to the agency, system has moderately low security risk or criticality.

Moderate-3: According to the agency, system has moderate security risk or criticality.

Moderately high-4: According to the agency, system has moderately high security risk or criticality.

High-5: According to the agency, system has high security risk or criticality.

Source: GAO analysis of agency data. | GAO-19-471

[a]Due to sensitivity concerns, we substituted a numeric identifier for the system names and only provided general details.

[b]The agency stated that the system's hardware had various refresh dates and that it was not able to identify the oldest hardware.

[c]The agency stated that the majority of the network's hardware was purchased between 2008 and 2011.

The Majority of Agencies Lack Complete Plans for Modernizing the Most Critical Legacy Systems

Given the age of the hardware and software in legacy systems, the systems' criticality to agency missions, and the security risks posed by operating aging systems, it is imperative that agencies carefully plan for their successful modernization. Documenting modernization plans in sufficient detail increases the likelihood that modernization initiatives will succeed. According to our review of government and industry best practices for the modernization of federal IT,[42] agencies should have documented modernization plans for legacy systems that, at a minimum, include three key elements: (1) milestones to complete the modernization, (2) a description of the work necessary to modernize the legacy system, and (3) details regarding the disposition of the legacy system.

Of the 10 identified agencies with critical systems most in need of modernization, seven (DOD, DHS, Interior, Treasury, the Office of Personnel Management (OPM), the Small Business Administration (SBA), and SSA) had documented modernization plans for their respective critical legacy systems and three did not have documented plans. The three agencies that did not have documented modernization plans for their critical legacy systems were: (1) Education, (2) HHS, and (3) Transportation.

Of the seven agencies with documented plans, DOD and Interior had modernization plans that addressed each of the three key elements. For example, Interior submitted documentation of both completed and forthcoming milestones leading to the deployment of the modernized system. The department also provided a list of the mandatory requirements for the updated system, as well as the work that needed to be performed at each stage of the project, including the disposition of the legacy system.

Likewise, DOD provided documentation of the milestones and the work needed to complete the modernization of its legacy system. In addition, the documentation discussed the department's plans for the disposition of the legacy system.

[42]GSA, Unified Shared Services Management, *Modernization and Migration Management (M3) Playbook* (Aug. 3, 2016); *M3 Playbook Guidance* (Aug. 3, 2016); American Technology Council, *Report to the President on Federal IT Modernization* (Dec. 13, 2017); OMB, *Management of Federal High Value Assets*, M-17-09 (Washington, D.C.: Dec. 9, 2016); American Council for Technology-Industry Advisory Council, *Legacy System Modernization: Addressing Challenges on the Path to Success* (Fairfax, VA: Oct. 7, 2016); and Dr. Gregory S. Dawson, Arizona State University, IBM Center for The Business of Government, *A Roadmap for IT Modernization in Government* (Washington, D.C.: 2018).

While the other five agencies—Treasury, DHS, OPM, SBA, and SSA—had developed modernization plans for their respective legacy systems, their plans did not fully address one or more of the three key elements. For instance, DHS's Federal Emergency Management Agency's modernization plan for its selected legacy system described the work that the department needed to accomplish, but did not include the associated milestones or the disposition of the legacy system. Similarly, SBA included milestones and a plan for the disposition of the legacy system, but did not include a description of the work necessary to accomplish the modernization.

Treasury, OPM, and SSA partially included one or more of the key elements in their modernization plans. For instance, OPM's and SSA's plans included upcoming milestones for one part of the initiative, but not the entire effort. Similarly, OPM's modernization plans only described a portion of the work necessary to complete each modernization initiative. Further, none of these four agencies' modernization plans included considerations for the disposition of legacy system components following the completion of the modernization initiatives. While agencies may be using development practices that minimize initial planning, such as agile,[43] agencies should have high-level information on cost, scope, and timing.[44]

Table 2 identifies the seven agencies with documented modernization plans for their critical systems, as well as the extent to which the plans were sufficiently detailed to include the three key elements. (Due to sensitivity concerns, we substituted a numeric identifier for the system names.)

[43]Agile development is a type of incremental development, which calls for the rapid delivery of software in small, short increments. Many organizations, especially in the federal government, are accustomed to using a waterfall software development model, which consists of long, sequential phases.

[44]GAO, *FEMA Grants Modernization: Improvements Needed to Strengthen Program Management and Cybersecurity,* GAO-19-164 (Washington, D.C.: Apr. 9, 2019).

Table 2: Extent to Which Agencies' Legacy System Documented Modernization Plans Included Key Elements

Agency	System name[a]	Includes milestones to complete the modernization	Describes work necessary to modernize system	Summarizes planned disposition of legacy system
Department of Defense	System 1	Yes	Yes	Yes
Department of Homeland Security	System 4	No	Yes	No
Department of the Interior	System 5	Yes	Yes	Yes
Department of the Treasury	System 6	Partial	Yes	No
Office of Personnel Management	System 8	Partial	Partial	No
Small Business Administration	System 9	Yes	No	Yes
Social Security Administration	System 10	Partial	Partial	No

Legend:

Yes – Agency included element in modernization plan.

Partial – Agency partially included the element in the modernization plan (e.g., the element was completed for only a portion of the modernization, rather than the entire modernization).

No – Agency did not include element in modernization plan.

Source: GAO analysis of agency modernization plans. | GAO-19-471

[a]Due to sensitivity concerns, we have substituted the systems' names with a numeric identifier.

The agencies provided a variety of explanations for the missing modernization plans. For example, according to the three agencies without documented modernization plans:

- Education's modernization plans were pending the results of a comprehensive IT visualization and engineering project that would determine which IT systems and services could be feasibly modernized, consolidated, or eliminated;
- HHS had entered into a contract to begin a modernization initiative but had not yet completed its plans; and
- Transportation had solicited information from industry to determine whether the agency's ideas for modernization were feasible.

Of the five agencies which had plans that lacked key elements, officials within SSA's office of the CIO stated that the agency has yet to complete its modernization planning, even though modernization efforts are currently underway. The officials said that they will update the planning documentation and make further decisions as the modernization effort progresses.

Officials within DHS's Federal Emergency Management Agency's Office of the CIO stated that its plans for modernizing the system we reviewed

(System 4) are contingent on receiving funding and being able to allocate staffing resources to planning activities. According to the officials, the agency is also integrating its plans for modernizing System 4 with the management of the rest of the agency's systems.

Similarly, Treasury officials stated that IRS's efforts to complete planning for the remaining modernization activities have been delayed due to budget constraints. In addition, officials within OPM's Office of the CIO stated that its modernization plan did not extend to fiscal year 2019 because there were changes in leadership during the creation of the plan, and because of uncertainty in funding amounts.

While we recognize that system modernizations are dependent on funding, it is important for agencies to prioritize funding for the modernization of these critical legacy systems. In addition, Congress provided increased authority for agencies to fund such modernization efforts through the MGT Act's Technology Modernization Fund and the related IT working capital funds.

Until the agencies establish complete legacy system modernization plans that include milestones, describe the work necessary to modernize the system, and detail the disposition of the legacy system, the agencies' modernization initiatives will have an increased likelihood of cost overruns, schedule delays, and overall project failure. Project failure would be particularly detrimental in these 10 cases, not only because of wasted resources, but also because it would prolong the lifespan of increasingly vulnerable and obsolete systems, exposing the agency and system clients to security threats and potentially significant performance issues.

Further, agencies may not be effectively planning for the modernization of legacy systems, in part, because they are not required to. As we reported in May 2016, agencies are not required to identify, evaluate, and prioritize existing IT investments to determine whether they should be kept as-is, modernized, replaced, or retired.[45] We recommended that OMB direct agencies to identify legacy systems needing to be replaced or modernized. As of April 2019, OMB had not implemented this recommendation. OMB staff stated that agencies were directed to manage the risk to High Value Assets associated with legacy systems in

[45]GAO-16-468.

OMB's December 2018 guidance.[46] While OMB's guidance does direct agencies to identify, report, assess, and remediate issues associated with High Value Assets, it does not require agencies to do so for all legacy systems. Until OMB requires agencies to do so, the federal government will continue to run the risk of continuing to maintain investments that have outlived their effectiveness.

Agencies Reported a Variety of IT Modernization Successes

The 24 Chief Financial Officers Act agencies in our review identified a total of 94 examples of successful modernizations of legacy systems undertaken in the last 5 years. The initiatives were of several types, including those aimed at transforming legacy code into a more modern programming language, migrating legacy services (e.g., email) to the cloud, and re-designing a legacy mainframe to a cloud-based application. Among these examples, the five that we selected reflect a mix of different agencies, types of system modernization initiatives, and types of benefits realized from the initiatives.

Table 3 provides details on the five examples of successful IT modernization initiatives, as reported by their respective agencies, as well as the reported benefits related to those initiatives.

Table 3: Agency-Reported Examples of Successful Information Technology (IT) Modernization Initiatives in the Last 5 Years and Associated Benefits

Agency	Initiative description	Benefits reported by agencies
Department of Defense (DOD)	**Standard Base Supply System and Enterprise Solution-Supply.** In April 2015, the Air Force, a component of DOD, began an initiative to modernize its Standard Base Supply System and Enterprise Solution-Supply (legacy systems responsible for the management of supplies and equipment for warfighting missions). To do so, among other things, the component transformed millions of lines of Common Business Oriented Language (COBOL) code to Java code. In February 2018, the Air Force completed the migration to the modernized version of the Integrated Logistics Systems-Supply system.	• Avoided spending $11 million on costs associated with hosting the system due to decommissioning the legacy system earlier than anticipated • Avoided spending $25 million annually on hosting costs • Minimized the use of legacy code, which can be costly and difficult to maintain

[46]OMB, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018).

Agency	Initiative description	Benefits reported by agencies
Department of Education (Education)	**Direct Loan Consolidation System.** In 2012, Education began its initiative to modernize the Direct Loan Consolidation System, its system that allows students to apply for, receive, and consolidate federal education loans. Among other things, this modernization allowed loans to be assigned to multiple servicers, corrected information security findings, and provided better customer service. In June 2016, Education decommissioned the legacy system. Functions that were performed by the legacy system are now performed by another existing system, which has an application process in place for borrowers and a real-time interface to help prepopulate the application.	• Improved customer experience through website consolidation • Consolidated customer call centers • Reduced applicant data entry errors by prepopulating data from another system • Reduced the amount of oversight required by lowering the number of contractors and systems • Closed multiple critical security vulnerabilities • Improved customer service
Department of Homeland Security (DHS)	**Employing Shared Services/ Cloud.** In August 2012, DHS initiated the modernization of multiple IT infrastructure systems. This included an agency-wide transition to a DHS private cloud email system and migrating legacy services to 13 DHS private cloud offerings.[a] In particular, all eight of DHS's operational components migrated applicable legacy services to 13 DHS private cloud offerings by the end of fiscal year 2016. As a result, DHS components were able to retire legacy systems and replace legacy software application procurement requirements. For example, U.S. Citizenship and Immigration Services migrated several legacy services to the cloud, including email, which ultimately saved the agency $42,000.	• Realized cumulative $1.6 billion in cost savings • Streamlined the supply chain for IT services • Reduced the amount of labor needed to maintain legacy systems and software • Enhanced security
Department of the Treasury (Treasury)	**Treasury Offset Program.** Treasury began the modernization initiative for this system in July 2011 using Agile development principles.[b] In November 2014, Treasury migrated its legacy COBOL- and Java-based Treasury Offset Program system to its new Java-based Treasury Offset Program Next Generation. The new system easily supported adding new debt collections from federal and state agencies, along with new payment streams.	• Enhanced revenue by $759 million by collecting delinquent debts • Increased efficiency of the system • Reduced time spent on manual interventions to keep the system from failing • Automated testing and deployment pipeline, reducing risk and cost
Social Security Administration (SSA)	**Representative Payee System.** SSA began the modernization initiative in December 2011. The agency needed to have the ability to continually add new representative payee records and expand the number of records stored in the database. In April 2016, SSA completed its redesign of the system, changing it from a mainframe-based system that used Assembler Language Code and COBOL to a web-based application, and decommissioned the legacy system.	• Improved users' ability to find data related to criminal history and fraud • Increased security by becoming compliant with current agency standards and federal guidelines • Improved business processes, such as search capability • Improved ability to identify criminal and fraudulent data • Improved system performance and incorporated user requested features

Source: GAO analysis of agency data. | GAO-19-471

[a]A private cloud is set up specifically for one organization, although there may be multiple customers within that organization and the cloud may exist on or off the customer's premises.

[b]Agile development is an incremental approach that delivers software functionality in short increments before the system is fully deployed.

The five agencies attributed the success of their modernization initiatives to various factors, including:

- using automated technologies to examine programming code and perform testing (DOD and Treasury);
- testing the system thoroughly (SSA and Treasury);
- actively engaging the end users and stakeholders throughout the modernization process (SSA and Treasury);
- cultivating a partnership between industry and government (DOD);
- following management practices on change and life cycle management (Education);
- developing and implementing an enterprise-wide cost collection and data analysis process for commodity IT to track and measure progress against consolidation, optimization, and savings targets (DHS);
- creating an interface that was consistent across systems (SSA);
- having strong executive leadership and support (Treasury); and
- using agile principles to facilitate the team's ownership of the project (Treasury).

These factors are largely consistent with government and industry best practices. For example, we reported in 2011 on critical success factors associated with major acquisitions, including engaging stakeholders and having the support of senior executives.[47] Similarly, OMB's guidance on High Value Assets calls for agencies' plans to address change management and life cycle management.[48] Likewise, the Software Engineering Institute's Capability Maturity Model® Integration for Development recommends that organizations engage stakeholders, practice effective change and life cycle management, and thoroughly test systems, among other practices.[49] Further, our Information Technology Investment Management framework recommends involving end users,

[47]GAO, *Information Technology: Critical Factors Underlying Successful Major Acquisitions,* GAO-12-7 (Washington, D.C.: Oct. 21, 2011).

[48]OMB, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018).

[49]Carnegie Mellon University's Software Engineering Institute, *Capability Maturity Model® Integration for Development, Version 1.3* (CMMI-Dev V1.3) (Pittsburgh, PA: Nov. 2010).

implementing change and life cycle management processes, and obtaining the support of executive leadership.[50]

Agencies that follow such practices are better positioned to modernize their legacy systems. Doing so will also allow the agencies to leverage IT to successfully address their missions.

Conclusions

The 10 most critical federal legacy systems in need of modernization are becoming increasingly obsolete. Several agencies are using outdated computer languages, which can be difficult to maintain and increase costs. Further, several of these legacy systems are also operating with unsupported hardware and software and known security vulnerabilities.

Most agencies did not have complete plans to modernize these legacy systems. Due to the criticality and possible cybersecurity risks posed by operating aging systems, having a plan that includes how and when the agency plans to modernize is vital. In the absence of such plans, the agencies increase the likelihood of cost overruns, schedule delays, and overall project failure. Such outcomes would be particularly detrimental because of the importance of these systems to agency missions.

Successfully modernizing legacy systems is possible, as demonstrated by the five highlighted examples. Agencies attributed the success of their modernization initiatives to a variety of management and technical factors that were consistent with best practices.

Recommendations for Executive Action

In the LOUO report that we are issuing concurrently with this report, we are making a total of eight recommendations to eight federal agencies to identify and document modernization plans for their respective legacy systems, including milestones, a description of the work necessary, and details on the disposition of the legacy system.

Agency Comments and Our Evaluation

We requested comments on a draft of this report from OMB and the 24 agencies included in our review. The eight agencies to which we made recommendations in the LOUO report agreed with our findings and

[50]GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity,* GAO-04-394G (Washington, D.C.: March 2004).

recommendations. In addition, OMB and the 16 agencies to which we did not make recommendations either agreed with our findings, did not agree or disagree with the findings, or stated that they had no comments. Further, multiple agencies provided technical comments, which we have incorporated, as appropriate.

The following eight agencies agreed with our recommendations:

- In written comments from Education, the agency stated that it concurred with the recommendation and indicated its intent to address it. Education's comments are reprinted in appendix IV.
- In written comments from HHS on the LOUO version of this report, the agency stated that it concurred with the recommendation and intends to evaluate ways to provide its modernization plan, including milestones and a description of the work necessary to modernize the system. HHS also provided technical comments that we incorporated, as appropriate.

  HHS deemed some of the information in its original agency comment letter pertaining to particular legacy systems to be sensitive, which must be protected from public disclosure. Therefore, we have omitted the sensitive information from the version of the agency comment letter that is reprinted in appendix V of this report.
- In written comments, DHS stated that it concurred with our recommendation. DHS's comments are reprinted in appendix VI.
- In comments received via email from Transportation's Director of Audit Relations and Program Improvement on May 9, 2019, the agency stated that it agreed with our recommendation.
- In comments from Treasury's Supervisory IT Specialist/Performance and Governance Analyst, received via email on May 17, 2019, the department stated that it agreed with our recommendation. In addition, Treasury's component agency, IRS, provided written comments which stated that it agreed with the recommendation. The agency said it intends to develop a multiyear retirement strategy for its system to address the recommendation.

  In its written comments, IRS also stated that our draft report did not accurately convey that the legacy system replacement project is intended to only replace core components of its selected legacy system. The agency said that, even when the entire replacement project is completed, it will only address a portion of the work required to retire the legacy system. In response, we modified our discussion

of this project in the report. IRS's comments are reprinted in appendix VII.

- In written comments from OPM on the LOUO version of this report, the agency stated that it concurred with the recommendation and indicated its plans to address the recommendation. OPM also provided technical comments that we incorporated, as appropriate.

  OPM deemed some of the information in its original agency comment letter pertaining to particular legacy systems to be sensitive, which must be protected from public disclosure. Therefore, we have omitted the sensitive information in the version of the agency comment letter that is reprinted in appendix VIII.

- In written comments, SBA concurred with our recommendation and stated that it intends to include a description of the work necessary to modernize the legacy system in the initiative's project plan. The agency estimated that it will address the recommendation by July 31, 2019.

  SBA deemed some of the information in its original agency comment letter pertaining to particular legacy systems to be sensitive, which must be protected from public disclosure. Therefore, we have omitted the sensitive information from the version of the agency comment letter that is reprinted in appendix IX.

- In written comments from SSA, the agency stated that it agreed with our recommendation. The agency added that it is modernizing its legacy system using agile software methods and a multiyear roadmap of development activities. The agency further stated that, as it completes its modernization work, it expects to retire most of the legacy software associated with System 10. SSA also provided technical comments that we incorporated, as appropriate. SSA's comments are reprinted in appendix X.

In addition, we received responses via email from 14 agencies to which we did not make recommendations. Of these agencies, three agreed with our findings and 11 stated that they did not have comments on the report. Two other agencies—HUD and the U.S. Agency for International Development—provided written comments in which they expressed appreciation for the opportunity to review the report, but did not state whether they agreed or disagreed with our findings. These agencies' comments are reprinted in appendixes XI and XII, respectively.

Further, in an email from OMB staff on May 22, 2019, the agency did not state whether it agreed or disagreed with our findings, but provided technical comments that we incorporated, as appropriate.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Labor, State, the Interior, the Treasury, Transportation, and Veterans Affairs; the U.S. Attorney General (Department of Justice); the Administrators of the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, Small Business Administration, and the U.S. Agency for International Development; the Commissioner of the Social Security Administration; the Directors of the National Science Foundation and the Office of Personnel Management; and the Chairman of the Nuclear Regulatory Commission; and other interested parties. This report is also available at no charge on the GAO website at http://www.gao.gov.

Should you or your staffs have any questions on information discussed in 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 major contributions to this report are listed in appendix XIII.

Carol C. Harris
Director
Information Technology Management Issues

List of Requesters

The Honorable Elijah E. Cummings
Chairman
The Honorable Jim Jordan
Ranking Member
Committee on Oversight and Reform
House of Representatives

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

The Honorable Will Hurd
House of Representatives

The Honorable Robin L. Kelly
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) identify the most critical federal legacy systems in need of modernization and evaluate plans for modernizing them, and (2) identify examples of information technology (IT) legacy system modernization initiatives in the last 5 years that agencies considered successful. The scope of our review included the 24 agencies covered by the Chief Financial Officers Act of 1990.[1]

This report presents a public version of a "limited official use only" (LOUO) report that we are also issuing today.[2] The Department of Homeland Security and the Department of the Interior determined that certain information in our original report should be protected from public disclosure. Therefore, we will not release the LOUO report to the general public because of the sensitive information it contains.

The LOUO report includes eight recommendations that we made to eight agencies to document modernization plans for particular legacy systems, including milestones, a description of the work necessary, and details on the disposition of the legacy system.[3] In this public version of the report, we have omitted sensitive information regarding particular legacy systems. Specifically, we have deleted systems' names and other information that would identify the particular system, such as specific descriptions of the systems' purposes and vulnerabilities.

Although the information provided in this report is more limited, the report addresses the same objectives as the LOUO report and is based on the same audit methodology. We provided a draft of this report to agency officials to obtain their review and comments on the sensitivity of the information contained herein. We confirmed with the agency officials that

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

[2]GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-351SU (Washington, D.C.: June 11, 2019).

[3]We made recommendations to the Departments of Education, Health and Human Services, Homeland Security, Transportation, the Treasury; the Office of Personnel Management; Small Business Administration; and Social Security Administration.

this report can be made available to the public without jeopardizing the security of federal agencies' legacy systems.

To identify the most critical legacy systems in need of modernization, we first reviewed the agencies' 2017 responses to congressional committees' requests for information that identified the agencies' top three legacy systems in need of modernization. We then asked the agencies to either confirm that those systems were still considered their top systems in need of modernization or update their lists to include the three systems most in need of modernization. All 24 agencies either confirmed or updated their lists of legacy systems most in need of modernization. This resulted in a collective list of 65 systems.[4] However, due to sensitivity concerns, we are not disclosing the names of the systems in this report. Appendix II provides a generalized list of the systems.

To develop a set of attributes for determining systems' obsolescence and their need for modernization, we reviewed available technical literature, such as:

- General Services Administration's Unified Shared Services Management's[5] *Modernization and Migration Management (M3) Playbook* and *M3 Playbook Guidance*,[6]
- American Technology Council's[7] *Report to the President on Federal IT Modernization*,[8]

[4]Most agencies provided a list of three legacy systems in need of modernization. However, the Department of Education reported four legacy systems, the Department of Commerce reported two legacy systems, and the Departments of Agriculture and Energy each reported one legacy system. The U.S. Agency for International Development stated that it did not have any legacy systems.

[5]The Unified Shared Services Management office resides within the General Services Administration and is to provide the strategy and leadership to make mission-enabling services better, faster, and more affordable.

[6]General Services Administration, Unified Shared Services Management, *Modernization and Migration Management (M3) Playbook* (Aug. 3, 2016); *M3 Playbook Guidance* (Aug. 3, 2016).

[7]The American Technology Council was established in May 2017, and has the goal of helping to transform and modernize federal agency IT and how the federal government uses and delivers digital services. The President is the chairman of this council, and the Federal CIO and the United States Digital Service Administrator are among the members.

[8]American Technology Council, *Report to the President on Federal IT Modernization* (Dec. 13, 2017).

- Office of Management and Budget's *Management of Federal High Value Assets* Memorandum,[9]
- IBM Center for The Business of Government's *A Roadmap for IT Modernization in Government*,[10] and
- American Council for Technology-Industry Advisory Council's *Legacy System Modernization: Addressing Challenges on the Path to Success*.[11]

We also consulted with system development experts within GAO and reviewed our prior report on federal legacy systems.[12] Using these sources, we developed a set of 14 total attributes for determining systems' obsolescence and their need for modernization. We then asked the agencies in our review to provide the associated details for the selected systems. We considered these details to rank the systems against the attributes that we compiled. We assigned point values to each system based on the systems' agency-reported attributes. Table 4 details the nine attributes and associated point values and ranges we used to initially rank the legacy systems.

[9]Office of Management and Budget, *Management of Federal High Value Assets*, M-17-09 (Washington, D.C.: Dec. 9, 2016). This was the memorandum that was in place at the time of our analysis. It has since been rescinded and replaced by M-19-03.

[10]Dr. Gregory S. Dawson, Arizona State University, IBM Center for The Business of Government, *A Roadmap for IT Modernization in Government* (Washington, D.C.: 2018).

[11]American Council for Technology-Industry Advisory Council, *Legacy System Modernization: Addressing Challenges on the Path to Success* (Fairfax, VA: Oct. 7, 2016).

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

Table 4: Attributes and Associated Point Values Used to Rank Legacy Systems

System attribute	Point values
Initial year of implementation	0 points if the system had been implemented in the 2010s
	2 points if the system had been implemented in the 2000s
	4 points if the system had been implemented in the 1990s
	6 points if the system had been implemented in the 1980s
	8 points if the system had been implemented in the 1970s
	10 points if the system had been implemented before 1970
High Value Asset[a] status	10 points if system had been a High Value Asset; 0 points if not
Date of oldest hardware	0 points if the oldest hardware had been installed in the 2010s
	1 point if the oldest hardware had been installed in the 2000s
	2 points if the oldest hardware had been installed in the 1990s
	3 points if the oldest hardware had been installed in the 1980s
	4 points if the oldest hardware had been installed in the 1970s
	5 points if the oldest hardware had been installed before 1970
Hardware warranty status	5 points if the system's hardware was no longer under warranty; 0 points if the hardware was under warranty
Operating system support status	5 points if the system's operating system was no longer supported by the vendor; 0 points if the operating system was supported
Software support status	5 points if the system's software was no longer supported by the vendor; 0 points if the software was supported
Use of legacy programming language	5 points if the system used a programming language that the agency identified as a legacy language; 0 points if the system did not use legacy programming languages
System criticality (on a scale of 1 to 5, 5 being most critical)	1 – 5 points, as assessed by the agency
Security risk (on a scale of 1 to 5, 5 having the most risk)	1 – 5 points, as assessed by the agency

Source: GAO analysis. | GAO-19-471

[a]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 since been rescinded and replaced by M-19-03.

We then totaled the assigned points for each legacy system and ranked the results from highest to lowest number of assigned points. While we had planned to select the top 20 systems with the most points for more detailed analysis, three systems were ranked in nineteenth place. As a result, we selected 21 systems for our review.

We collected additional information on the 21 selected systems and performed a second round of analysis, scoring, and ranking. Based on the second set of scores, we identified the 10 systems with the highest scores as being the most critical legacy systems in need of modernization. We also supplemented our review with interviews of officials in the agencies' offices of the Chief Information Officer and program offices for the selected legacy systems. Table 5 details the five attributes and associated point values and ranges we used to rank the legacy systems in the subsequent round of analysis. Table 6 lists these 10 selected systems according to their designated identifiers. However, due to sensitivity concerns, we substituted a numeric identifier for the name of each system.

Table 5: Attributes and Associated Point Values Used to Rank Legacy Systems in the Subsequent Round of Analysis

System attribute	Point values
Status of modernization plans	5 points if the agency did not have plans to modernize the system; 0 points if the agency had plans to modernize the system
Number of users	0 points if the system had under 100 users
	1 point if the system had 100 to 5,000 users
	2 points if the system had 5,000 to 25,000 users
	3 points if the system had 25,000 to 100,000 users
	4 points if the system had 100,000 to 500,000 users
	5 points if the system had more than 500,000 users
Potential annual cost savings of system modernization	0 points if the modernization of the system could potentially result in cost savings of less than $100,000
	1 point if the modernization of the system could potentially result in cost savings of $100,000 to $500,000
	2 points if the modernization of the system could potentially result in cost savings of $500,000 to $2 million
	3 points if the modernization of the system could potentially result in cost savings of $2 million to $10 million
	4 points if the modernization of the system could potentially result in cost savings of $10 million to $20 million
	5 points if the modernization of the system could potentially result in cost savings of more than $20 million
Annual operating costs	0 points if the system's annual operating costs were under $100,000
	1 point if the system's annual operating costs were between $100,000 and $500,000
	2 points if the system's annual operating costs were between $500,000 and $2 million
	3 points if the system's annual operating costs were between $2 million and $10 million
	4 points if the system's annual operating costs were between $10 million and $20 million
	5 points if the system's annual operating costs were more than $20 million

System attribute	Point values
Annual labor costs	0 points if the system's annual labor costs were under $100,000
	1 point if the system's annual labor costs were between $100,000 and $500,000
	2 points if the system's annual labor costs were between $500,000 and $2 million
	3 points if the system's annual labor costs were between $2 million and $10 million
	4 points if the system's annual labor costs were between $10 million and $20 million
	5 points if the system's annual labor costs were more than $20 million

Source: GAO analysis. | GAO-19-471

Table 6: The 10 Selected Most Critical Legacy Systems in Need of Modernization

Agency	System name
Department of Defense	System 1
Department of Education	System 2
Department of Health and Human Services	System 3
Department of Homeland Security	System 4
Department of the Interior	System 5
Department of the Treasury	System 6
Department of Transportation	System 7
Office of Personnel Management	System 8
Small Business Administration	System 9
Social Security Administration	System 10

Source: GAO analysis of agency documentation. | GAO-19-471

To evaluate agencies' plans for modernizing the 10 federal legacy systems most in need of modernization, we requested that agencies provide us with the relevant plans. These modernization plans could have been contained within several types of documentation, since a system modernization could be a new system development, a system acquisition, or a renovation of the legacy system. For example, if an agency was acquiring a new system from a vendor, the plans for modernization could have been contained within an acquisition plan or a statement of work in a contract. Likewise, if an agency was developing a new system on its own, the modernization plans could have been within a project plan or design document.

We reviewed government and industry best practice documentation on the identification and modernization of legacy systems, including:

- General Services Administration's Unified Shared Services Management's[13] *Modernization and Migration Management (M3) Playbook* and *M3 Playbook Guidance*,[14]
- American Technology Council's[15] *Report to the President on Federal IT Modernization*,[16]
- Office of Management and Budget's Management of *Federal High Value Assets* memorandum,[17]
- IBM Center for The Business of Government's *A Roadmap for IT Modernization in Government*,[18] and
- American Council for Technology-Industry Advisory Council's *Legacy System Modernization: Addressing Challenges on the Path to Success*.[19]

Based on our reviews of these sources, we determined that agencies' documented plans for system modernization should include, at a minimum, (1) milestones to complete the modernization, (2) a description of the work necessary to modernize the system, and (3) details regarding the disposition of the legacy system. We then analyzed agencies' documented modernization plans for the selected systems to determine whether the plans included these elements. If an agency's plans included

[13]The Unified Shared Services Management office resides within the General Services Administration and is to provide the strategy and leadership to make mission-enabling services better, faster, and more affordable.

[14]General Services Administration, Unified Shared Services Management, *Modernization and Migration Management (M3) Playbook* (Aug. 3, 2016); *M3 Playbook Guidance* (Aug. 3, 2016).

[15]The American Technology Council was established in May 2017, and has the goal of helping to transform and modernize federal agency IT and how the federal government uses and delivers digital services. The President is the chairman of this council, and the Federal CIO and the United States Digital Service Administrator are among the members.

[16]American Technology Council, *Report to the President on Federal IT Modernization* (Dec. 13, 2017).

[17]Office of Management and Budget, *Management of Federal High Value Assets*, M-17-09 (Washington, D.C.: Dec. 9, 2016). This was the memorandum that was in place at the time of our analysis. It has since been rescinded and replaced by M-19-03.

[18]Dr. Gregory S. Dawson, Arizona State University, IBM Center for The Business of Government, *A Roadmap for IT Modernization in Government* (Washington, D.C.: 2018).

[19]American Council for Technology-Industry Advisory Council, *Legacy System Modernization: Addressing Challenges on the Path to Success* (Fairfax, VA: Oct. 7, 2016).

milestones for only a portion of the initiative or only described a portion of the work necessary to complete the modernization, we assigned the agency a partial rating. Appendix III provides details on each of the selected systems and the agencies' plans for modernizing them.

To identify examples of successful IT legacy system modernization initiatives, we first asked each of the 24 agencies to provide us with examples of their successful modernization initiatives completed between 2014 and 2018. The agencies reported 94 examples of successful modernization initiatives. We also reviewed the agencies' responses to congressional committees' requests for information to determine other possible successful modernization initiatives at these agencies. Using the examples discovered in this process and the agency-provided examples, we then collected and reviewed documentation describing the modernization initiatives, such as case studies and the agencies' written responses to our questions about the initiatives.

We used our professional judgment to select examples that reflected a mix of different agencies, types of system modernization initiatives, and types of benefits realized from the initiatives. We ultimately included in our review those modernization initiatives that two or more members of our audit team selected as examples that reflected a mix of different agencies, types of system modernization initiatives, and types of benefits realized from the initiatives. We also coordinated with the selected agencies' Offices of Inspector General to determine whether those offices had any past or current audit work that would contradict the agencies' determination that the selected initiatives were successful.

We conducted this performance audit from January 2018 to June 2019 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.

Appendix II: The 24 Chief Financial Officers Act Agencies' Most Critical Legacy Systems in Need of Modernization

Each of the 24 Chief Financial Officers Act agencies identified their agency's most critical legacy systems in need of modernization. The agencies identified a total of 65 such systems.[1] The agencies also identified various attributes of the legacy systems, including the systems' age, hardware age,[2] system criticality, and security risk. Table 7 provides a generalized list of the most critical legacy systems in need of modernization, as identified by the agencies, as well as selected factors related to each system's age and criticality. (Due to sensitivity concerns, we substituted alphanumeric identifiers for the names of the agencies' systems. Specifically, we assigned a number to identify each of the 10 most critical legacy systems in need of modernization that we discuss in this report and we assigned a letter or letters to identify the remaining 55 systems.)

Table 7: Combined List of Agencies' Most Critical Legacy Systems in Need of Modernization

Agency	System name[a]	Age of system, in years	Age of oldest hardware installed, in years	System criticality (as determined by agency)	Security risk (as determined by agency)
Department of Agriculture	System A	8	Unknown[b]	High	Moderately low
Department of Commerce	System B	16	5	High	High
	System C	25	7	High	Low
Department of Defense	System 1	14	3	Moderately high	Moderate
	System D	55	5	High	Low
	System E	33	12	High	Moderately low
Department of Education	System 2	46	3	High	High
	System F	13	12	High	Moderately high
	System G	25	5	High	High
	System H	24	17	Moderate	High
Department of Energy	System I	32	2	High	Low
Department of Health and Human Services	System 3	50	Various[c]	High	High
	System J	21	Unknown[b]	High	Moderate
	System K	7	8	High	Moderate

[1]Most agencies provided a list of three legacy systems in need of modernization. However, the Department of Education reported four legacy systems, the Department of Commerce reported two legacy systems, and the Departments of Agriculture and Energy each reported one legacy system. The U.S. Agency for International Development stated that it did not have any legacy systems.

[2]A legacy system may run on updated hardware, and, thus, the system's age and hardware age may not be the same.

Agency	System name[a]	Age of system, in years	Age of oldest hardware installed, in years	System criticality (as determined by agency)	Security risk (as determined by agency)
Department of Homeland Security	System 4	11	11	High	High
	System L	9	2	High	Moderately low
	System M	6	1	High	Low
Department of Housing and Urban Development	System N	42	2	High	Moderate
	System O	44	2	High	Moderate
	System P	44	2	High	Moderate
Department of Justice	System Q	21	10	High	High
	System R	38	7	High	Moderately low
	System S	49	6	Moderately high	Low
Department of Labor	System T	14	9	High	Low
	System U	21	10	High	Low
	System V	15	3	High	Moderate
Department of State	System W	24	5	High	Moderate
	System X	21	5	Moderately high	Moderate
	System Y	20	3	Moderately high	Moderate
Department of the Interior	System 5	18	18	High	Moderately high
	System Z	29	9	High	High
	System AA	23	23	Moderately high	Low
Department of the Treasury	System 6	51	4	High	Moderately low
	System AB	13	10	Moderate	Moderate
	System AC	10	8	High	Moderately low
Department of Transportation	System 7	35	7	High	Moderately high
	System AD	17	4	High	Moderately high
	System AE	19	n/a[b]	High	High
Department of Veterans Affairs	System AF	31	3	High	Low
	System AG	49	2	High	Moderately low
	System AH	31	4	High	Moderate
Environmental Protection Agency	System AI	24	1	High	Low
	System AJ	17	1	High	Low
	System AK	14	1	High	Low
General Services Administration	System AL	39	2	High	Low
	System AM	5	10	High	Moderate
	System AN	8	Unknown[b]	High	Moderate
National Aeronautics and Space Administration	System AO	10	13	High	High
	System AP	About 19	31	Moderately high	Moderately low
	System AQ	6	6	High	Low

Agency	System name[a]	Age of system, in years	Age of oldest hardware installed, in years	System criticality (as determined by agency)	Security risk (as determined by agency)
Nuclear Regulatory Commission	System AR[d]	11	7	Moderately high	Moderate
	System AS[d]	20	2	Moderately high	Moderate
	System AT	15	9	Moderately high	Moderately low
National Science Foundation	System AU	18	2	High	Moderately low
	System AV	18	2	Moderate	Moderately low
	System AW	22	2	Moderate	Moderate
Office of Personnel Management	System 8	34	6	High	Moderately low
	System AX	29	6	High	Moderately high
	System AY	21	6	High	Moderately low
Small Business Administration	System 9	17	10	High	Moderately high
	System AZ	13	10	Moderately high	Moderately high
	System BA	15	3	High	Moderately high
Social Security Administration	System 10	45	5	High	Moderate
	System BB	34	5	High	Moderate
	System BC	38	4	High	Moderate
U.S. Agency for International Development	n/a – Agency stated that it does not have any legacy systems.				

Key:

Agencies reported the system criticality and security risk on a scale of 1 to 5 (with 5 being the most critical or the highest risk). We assigned the following based on those numbers.

Low-1: According to the agency, system has low security risk or criticality.

Moderately low-2: According to the agency, system has moderately low security risk or criticality.

Moderate-3: According to the agency, system has moderate security risk or criticality.

Moderately high-4: According to the agency, system has moderately high security risk or criticality.

High-5: According to the agency, system has high security risk or criticality.

Source: GAO analysis of agency documentation. | GAO-19-471

[a]Due to sensitivity concerns, we substituted an alphanumeric identifier for the system names.

[b]The agency procures services from a vendor or another agency and was not able to get the information from the vendor.

[c]The agency stated that the system's hardware had various refresh dates and was not able to identify the oldest hardware.

[d]This system has been decommissioned since the agency reported it to us.

Appendix III: Profiles of the 10 Most Critical Legacy Systems in Need of Modernization

This appendix describes the 10 most critical legacy systems in need of modernization, as identified during our review. The profiles of each system describe (1) the system's purpose, (2) the reason that the system needs to be modernized, (3) the agency's plans for modernization, and (4) possible benefits to be realized once the system is modernized.

System 1

Department of Defense—U.S. Air Force

Reported number of users: Approximately 242,672

Initial year of implementation: 2005

System hardware under warranty? Agency did not know

Software vendor supported? No

Operating system(s) supported? Yes

Legacy programming language(s) used? Yes

System criticality (as determined by agency): Moderately high

System security risk (as determined by agency): Moderate

Reported annual operating costs: $21.8 million

Reported annual labor costs: $3.6 million

Reported cost of modernization: $12 million

Potential cost savings: $34 million annually

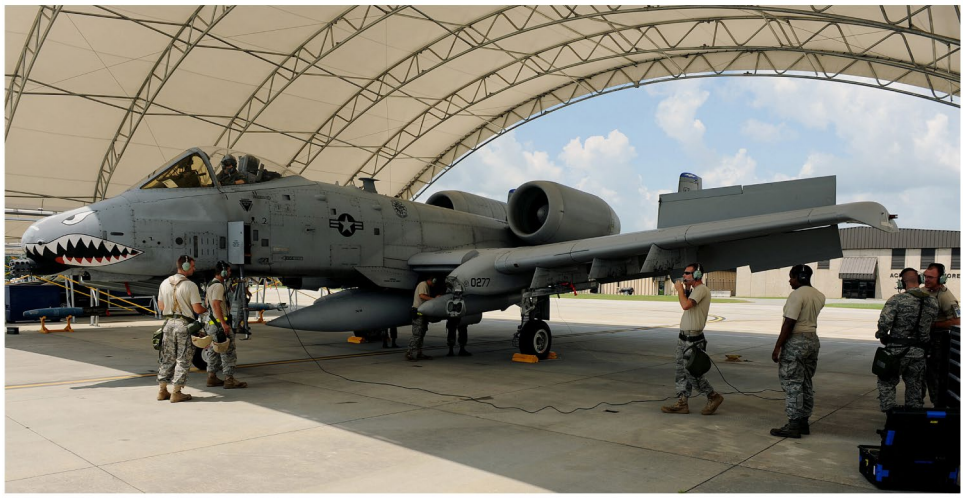
Other benefits: Increased functionality, increased aircraft touch time and availability

Status of modernization plans: Agency has documented modernization plans that include milestones to complete the modernization, descriptions of the work necessary to modernize the legacy system, and plans for the disposition of the legacy system

Source: GAO analysis of agency documentation and interviews. | GAO-19-471

The Department of Defense (DOD)—U.S. Air Force's System 1 provides configuration control and management to support wartime readiness and operational support of aircraft, among other things. See figure 1 for a photograph of airmen maintaining an aircraft.

Figure 1: Airmen Maintaining an Air Force Aircraft



Source: Photo U.S. Air Force, Airman 1st Class Joshua Green. | GAO-19-471

According to Air Force documentation, the cost to maintain and sustain the system has been steadily increasing due to several factors, including (1) costs associated with maintaining and operating the system's infrastructure and the manpower to maintain the legacy code; and (2) the difficulty and cost of experienced Common Business Oriented Language (COBOL)[1] programmers, poor legacy documentation, and an aging infrastructure and code. In addition, the system runs on a mainframe that is hosted by another agency. As a result of these issues, Air Force officials expect annual costs to rise from $21.8 million in 2018 to approximately $35 million beginning in 2020.

[1]COBOL, which was introduced in 1959, became the first widely used, high-level programming language for business applications. The Gartner Group, a leading information technology research and advisory company, has reported that organizations using COBOL should consider replacing the language, as procurement and operating costs are expected to steadily rise, and because there is a decrease in people available with the proper skill sets to support the language.

In September 2018, the Air Force awarded a contract to modernize and migrate the system to a cloud environment by September 2019. DOD contractors developed a project plan for the modernization that contains goals and outlines how the contractor plans to move through the modernization process, listing out sequential tasks leading to project completion. In addition, it outlines milestones from the starting point through implementation, and provides for the disposition of the legacy system. After the migration, as funding allows, the Air Force plans to incrementally transform the system's COBOL code to a more modern language.

Air Force program office officials stated that the modernized system will save the agency over $34 million a year, resulting in $356 million saved over a 10-year period. Officials also noted that, given the savings, the modernization would pay for itself in only 5 months. The Air Force also expects increased functionality with this modernization leading to increased aircraft touch time[2] and aircraft availability by enabling adoption of new technologies.

[2]Aircraft touch time is the time spent performing aircraft maintenance tasks.

System 2

Department of Education—Federal Student Aid

Reported number of users: Over 20 million student applications annually and thousands of other users

Initial year of implementation: 1973

System hardware under warranty? Yes

Software vendor supported? Yes

Operating system(s) supported? Yes

Legacy programming language(s) used? Yes

System criticality (as determined by agency): High

System security risk (as determined by agency): High

Reported annual operating costs: $43.9 million

Reported annual labor costs: $2.0 million

Reported cost of modernization: Agency has not determined costs

Potential cost savings: Agency has not calculated

Other benefits: Integration across the enterprise, improved cybersecurity and data protection, reduced system complexity, and increased efficiency

Status of modernization plans: Agency does not have a modernization plan

Source: GAO analysis of agency documentation and interviews. | GAO-19-471

The Department of Education's (Education) System 2 processes and stores student information and supports the processing of federal student aid applications.

Education first implemented System 2 in 1973.[3] Agency officials stated that the system runs approximately 1 million lines of Common Business Oriented Language (COBOL)[4] on an IBM mainframe. COBOL is a legacy language that can be costly to maintain. The department noted that 18 contractors are employed to maintain the COBOL programming language for this and another system. Education officials stated that the agency would like to modernize System 2 to eliminate reliance on COBOL, simplify user interactions, improve integration with other applications, respond to changing business requirements more quickly, and decrease development and operational costs.

Education officials stated that the agency intends to modernize System 2 as part of its Next Generation Financial Services Environment initiative. This initiative is to modernize Federal Student Aid's technical and operational architecture and improve the customer experience. The agency expects to consolidate all customer-facing websites and implement a new loan servicing platform to benefit federal student loans.

Education has not developed a plan for the modernization of System 2. According to agency officials, these plans are pending the results of a comprehensive information technology (IT) visualization and engineering project that will determine which IT systems and services could be feasibly modernized, consolidated, or eliminated.

While Education has not calculated the specific cost savings associated with modernizing System 2, the department anticipates potential cost savings, including decreased hardware and software licensing costs and decreased costs associated with changes to business rules. According to the agency, other potential benefits of modernizing this system include

[3]At the time, Education was part of the Department of Health, Education, and Welfare.

[4]COBOL, which was introduced in 1959, became the first widely used, high-level programming language for business applications. The Gartner Group, a leading information technology research and advisory company, has reported that organizations using COBOL should consider replacing the language, as procurement and operating costs are expected to steadily rise, and because there is a decrease in people available with the proper skill sets to support the language.

integration across the enterprise, improved cybersecurity and data protection, reduced system complexity, and improved system efficiency.

System 3

Department of Health and Human Services—Indian Health Service

Reported number of users: Approximately 20,000

Initial year of implementation: 1969

System hardware under warranty? Yes

Software vendor supported? Yes

Operating system(s) supported? Yes

Legacy programming language(s) used? Yes

System criticality (as determined by agency): High

System security risk (as determined by agency): High

Reported annual operating costs: $79.1 million

Reported annual labor costs: $26.7 million

Reported cost of modernization: Agency has not calculated

Potential cost savings: Agency has not calculated

Other benefits: Improves interoperability with other healthcare partners and enhances patient care

Status of modernization plans: Agency does not have a modernization plan

Source: GAO analysis of agency documentation and interviews. | GAO-19-471

The Department of Health and Human Services' (HHS) System 3 is a clinical and patient administrative information system. HHS's component, Indian Health Service's (IHS) uses the system to gather, store, and display clinical, administrative, and financial information on patients seen in a clinic, hospital, or remotely through the use of telehealth and home visit practices.

HHS officials stated that the modernization of System 3 is imperative. Specifically, the agency noted that the system's technical architecture and infrastructure were outdated. This has resulted in challenges in developing new capabilities in response to business and regulatory requirements. Further, System 3 is coded in C++ and MUMPS. MUMPS is a programming language that HHS considers to be a legacy language.[5] The agency noted that it has become increasingly difficult to find programmers proficient in writing code for MUMPS. Lastly, the system's more than 50 modules were added over time to address new business requirements. The software is installed on hundreds of separate computers, which has led to variations in the configurations at each site. According to IHS, this type of add-on development becomes detrimental over time and eventually requires a complete redesign to improve database design efficiency, process efficiency, workflow integration, and graphical user interfaces.

While the agency does not yet have modernization plans, in September 2018, HHS awarded a contract to conduct research for modernizing IHS's health information technology (IT) infrastructure, applications, and capabilities. According to the department, the research will be conducted in several stages over the next year, and a substantial part of the research will be an evaluation of the current state of health IT across IHS's health facilities. Once the research is conducted, in consultation with IHS and its stakeholders, the contractor will use the findings and recommendations to propose a prioritized roadmap for modernization. According to HHS, the agency will be completing the modernization initiative over the next 5 years, but anticipated that it may be able to begin to execute an implementation plan as early as 2020.

[5]MUMPS was originally known as the Massachusetts General Hospital Utility Multi-Programming System. It is a programming language developed originally for building medical systems. In January 2018, we reported that there is a dwindling supply of qualified software developers for MUMPS.

With regards to potential cost savings, HHS noted that the modernization will take significant capital investment to complete and it is unknown whether the modernization will lead to cost savings. HHS officials stated that this modernization could improve interoperability with its health care partners, the Department of Veterans Affairs and the Department of Defense, and significantly enhance direct patient care.

System 4

Department of Homeland Security—Federal Emergency Management Agency

Reported number of users: On average 30,000; more during a disaster

Initial year of implementation: Between 2008 and 2011

System hardware under warranty? No

Software vendor supported? No

Operating system(s) supported? No

Legacy programming language(s) used? No

System criticality (as determined by agency): High

System security risk (as determined by agency): High

Reported annual operating costs: $1.9 million

Reported annual labor costs: $0

Reported cost of modernization: Agency has not calculated

Potential cost savings: Agency has not calculated

Other benefits: Ability to meet mission requirements, reduction of network downtime, and increased network availability

Status of modernization plans: Agency has documented modernization plans that describe the work necessary to modernize the system; however, they do not contain milestones to complete the modernization or plans for the disposition of legacy system components following system modernization

Source: GAO analysis of agency documentation and interviews. | GAO-19-471

The Department of Homeland Security—Federal Emergency Management Agency's (FEMA) System 4 consists of routers, switches, firewalls, and other network appliances (all referred to as devices) to support the connectivity of FEMA sites.

According to the agency, System 4 needs to be modernized because there are significant cyber and network vulnerability risks associated with its end of life (i.e., no longer supported or manufactured by the vendor) devices. In particular, the system's devices typically require replacement every 3 to 5 years from the date of purchase. Despite this, the majority of the hardware was purchased between 8 and 11 years ago. As of December 2018, about 545 of these devices were at the end of life.

In a security assessment report performed in September 2018, System 4 received 249 security findings, of which 168 were high or critical risk to the system. Further compounding this issue, the agency is not certain exactly how many devices make up the system. In particular, FEMA officials stated that the vendor completed an inventory of devices in May 2018, but that inventory did not align with other inventory counts. As a result, the agency plans to develop an inventory reconciliation strategy and process to address this issue.

FEMA intends to replace System 4's devices in two phases. The first phase will target the agency's smaller facilities, while the second phase is to address the larger facilities, which may require more complex installations. FEMA's Office of the Chief Information Officer is conducting site surveys to better define requirements and cost estimates. While the agency has yet to develop finalized modernization plans for this initiative with milestones, DHS officials and contract information technology staff developed a list of future recommended activities that would help modernize the system as part of their November 2018 quarterly business review. Despite the lack of finalized plans, FEMA intends to replace 240 of the 545 devices that are at the end of support, if funds are available. The agency also intends to upgrade the remaining 305 devices in the future, if funds are available.

The agency has not calculated the exact amount of cost savings. Once the system is completely updated and a lifecycle replacement operations and maintenance support plan is in place and funded, FEMA and DHS expect to realize cost savings based on new technology and increased

throughput.[6] Further, the agency stated that with new equipment, it would be able to meet mission requirements and take advantage of new technologies. In addition, replacing these unsupported devices would significantly reduce downtime and increase network availability.

[6]Throughput refers to the performance of tasks by a computing service or device over a specific period. It measures the amount of completed work against time consumed and may be used to measure the performance of a process, memory, and/or network communications.

System 5

Department of the Interior—Bureau of Reclamation

Reported number of users: 49

Initial year of implementation: 2001

System hardware under warranty? No

Software vendor supported? No

Operating system(s) supported? No

Legacy programming language(s) used? Yes

System criticality (as determined by agency): High

System security risk (as determined by agency): Moderately high

Reported annual operating costs: $427,000

Reported annual labor costs: $448,000

Reported cost of modernization: $4.5 million

Potential cost savings: $152,000 per year

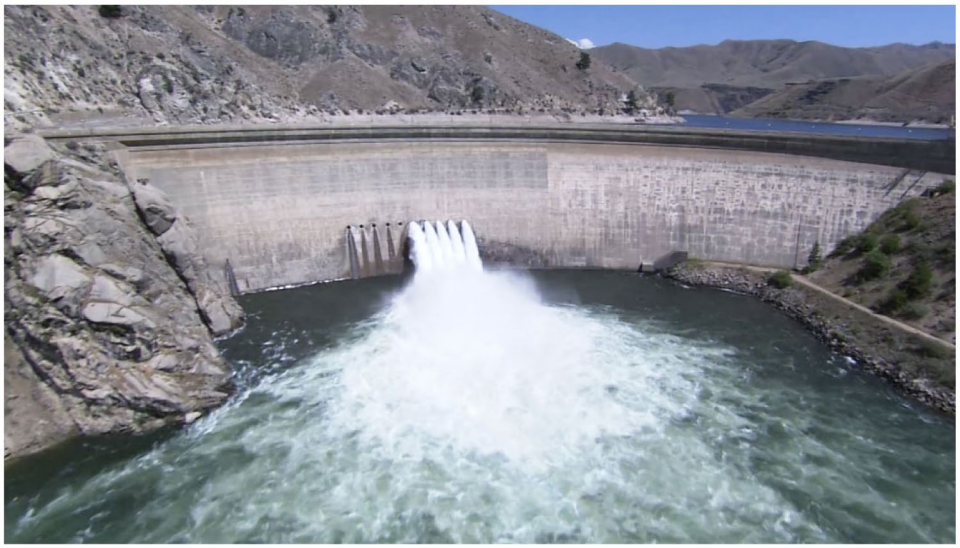
Other benefits: Increased capacity for new system requirements, elimination of obsolete hardware, increased system reliability

Status of modernization plans: Agency has documented modernization plans that include milestones to complete the modernization, descriptions of the work necessary to modernize the legacy system, and plans for the disposition of legacy system components following system modernization

Source: GAO analysis of agency documentation and interviews. | GAO-19-471

The Department of the Interior's (Interior) System 5 is an Industrial Control System (ICS) Supervisory Control and Data Acquisition (SCADA) System that supports the general operation of dams and power plants on a particular river and its tributaries. The system serves its customers by, among other things, starting and stopping the generators, adjusting the output of electricity to assure electric grid stability, and monitoring the operating conditions of dam and power plant equipment. Figure 2 shows an example of an Interior dam.

Figure 2: Photograph of a Dam



Source: U.S. Department of the Interior's Bureau of Reclamation; Creative Commons ShareAlike 2.0 Generic (https://creativecommons.org/licenses/by-sa/2.0/legalcode). | GAO-19-471

The system is approximately 18 years old and contains obsolete hardware that is not supported by the manufacturers. Further, according to a program official, the system's original hardware and software installation did not include any long-term vendor support. Thus, any original components that remain operational may have had long-term exposure to security and performance weaknesses. In January 2014, the Director of National Intelligence testified that ICS and SCADA systems used in electrical power distribution provided an enticing target to malicious actors and that, although newer architectures provide flexibility, functionality, and resilience, large segments of the systems remain vulnerable to attack, potentially causing significant economic or human impact. Further, according to Interior's system modernization plans, the agency needs to modernize the system in order to increase data

collection capabilities and security. Specifically, the system is expected to interface with more plant equipment and collect and report on more data than it has in the past.

According to Interior's plans, the modernized system is expected to accommodate future growth requirements. The plans also support the complete replacement of the system's obsolete hardware and software. The modernization plans also outline goals, milestones, and the work to be accomplished. The agency plans to complete the modernization by January 2020.

By replacing the legacy system, Interior plans to realize a number of potential benefits, including annual cost savings of $152,000. In addition, the system will no longer run on obsolete, unsupported hardware. Furthermore, newer software and hardware are expected to allow for the automation of compliance tasks, increase system security, and expand system availability. According to the system's fiscal year 2017 operational analysis, these benefits should create a more reliable system for both the agency and the customers of the networked hydroelectric dams.

System 6

Department of the Treasury—Internal Revenue Service

Reported number of users: 0[a]

Initial year of implementation: 1968

System hardware under warranty? No

Software vendor supported? Yes

Operating system(s) supported? Yes

Legacy programming language(s) used? Yes

System criticality (as determined by agency): High

System security risk (as determined by agency): Moderately low

Reported annual operating costs: $5.5 million

Reported annual labor costs: $10.4 million

Reported cost of modernization: $1.6 billion

Potential cost savings: None

Other benefits: Quick resolution of customer issues, reduced IT costs and complexity, and enhanced analytics and reporting

Status of modernization plans: Agency has documented modernization plans that describe the work necessary to modernize the legacy system; however, they only partially include milestones to complete the modernization and do not include details on the disposition of the legacy system

Note: [a]According to the agency, the system does not have users in the traditional sense and instead passes along data for applications to use. In 2018, the system assisted the agency in processing over 154 million tax returns.

Source: GAO analysis of agency documentation and interviews. | GAO-19-471

The Department of the Treasury's Internal Revenue Service's (IRS) System 6 contains taxpayer data. Many IRS processes depend on output, directly or indirectly, from this data source.

System 6 was written in a now outdated assembly language code[7] and Common Business Oriented Language (COBOL).[8] The department and we have raised a number of concerns related to this system's reliance on assembly language code and COBOL, the maintainability of the system, and staff attrition. For example, in May 2016, we reported that legacy systems using outdated languages may become increasingly more expensive and agencies may pay a premium to hire staff or contractors with the knowledge to maintain these systems.[9]

IRS plans to address these concerns by modernizing core components of System 6. The new system is intended to provide improved functionality. However, IRS is having trouble fully staffing the modernization effort, resulting in significant delays. While the agency has developed modernization plans, they are incomplete. For example, the plans' milestones do not go past the current project and their descriptions of the work necessary to complete the project are at a higher level when outlining the goals of future stages. In May 2019, the agency stated that even when the current modernization effort is fully implemented, only a portion of the work required to retire the legacy system will have been completed. The agency has not provided a target date for decommissioning the legacy system.

While IRS does not anticipate cost savings associated with the modernization of this system, it anticipates many internal and external benefits for both the taxpayer and the agency. In particular, according to

[7]As we reported in May 2016, assembly language code is a low-level computer language initially used in the 1950s. Programs written in assembly language are conservative of machine resources and quite fast; however, they are much more difficult to write and maintain than other languages. Programs written in assembly language may only run on the type of computer for which they were originally developed.

[8]COBOL, which was introduced in 1959, became the first widely used, high-level programming language for business applications. The Gartner Group, a leading IT research and advisory company, has reported that organizations using COBOL should consider replacing the language, as procurement and operating costs are expected to steadily rise, and because there is a decrease in people available with the proper skill sets to support the language.

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

the IRS's *Fiscal Year 2019 Capital Investment Plan*, the benefits of modernizing this system include: (1) increased agility of agency response to changing taxpayer priorities and legislation; (2) reduced IT costs and complexity; (3) enhanced analytics and reporting to greatly improve compliance and issue resolution; and (4) reduced burden of manually intensive processes on IRS employees, by enabling automated calculations that currently are not possible.

System 7

Department of Transportation—Federal Aviation Administration

Reported number of users: 160

Initial year of implementation: 1984

System hardware under warranty? Unknown

Software vendor supported? No

Operating system(s) supported? No

Legacy programming language(s) used? No

System criticality (as determined by agency): High

System security risk (as determined by agency): Moderately high

Reported annual operating costs: $3.8 million

Reported annual labor costs: $10.7 million

Reported cost of modernization: Agency has not calculated

Potential cost savings: Agency has not calculated

Other benefits: Enhanced security, compliance with law

Status of modernization plans: Agency does not have a modernization plan

Source: GAO analysis of agency documentation and interviews. | GAO-19-471

The Department of Transportation's (Transportation) Federal Aviation Administration's (FAA) System 7 contains information on aircraft and pilots. The system also provides information to other government agencies, including those responsible for homeland security and investigations of aviation accidents.

According to Transportation, the system is DOS-based and needs to be updated to continue to efficiently meet its mission.[10] Specifically, some of the core system components are mainframe applications that have been in operation since 1984. In addition, the system is running unsupported software, including one operating system that was last supported by the vendor in 2010.

FAA is planning to implement a new system to streamline processes, allow for the submission of electronic applications and forms, automate registration processes, improve data availability, and implement additional security controls. However, the agency does not currently have a documented modernization plan. Officials stated that the agency is seeking alternatives to modernize the system and meet legislative requirements. FAA has asked interested vendors to respond to a request for information. According to the agency, the responses to this request are intended to inform strategic decisions about the modernization, and are planned to ultimately lead to proposed solutions from industry.

While FAA has not calculated the specific cost savings associated with modernizing the system, the agency stated that it anticipates potential cost savings. Agency officials stated that they plan to have information on the anticipated cost savings in November 2019. The agency also expects that the modernized system will provide enhanced security.

[10]DOS, originally known as a disk operating system, is the operating system of a computer that can be stored on and run off of a computer disk drive.

System 8

Office of Personnel Management

Reported number of users: Millions of external users and 9,500 internal users

Initial year of implementation: 1985

System hardware under warranty? Yes

Software vendor supported? No

Operating system(s) supported? Yes

Legacy programming language(s) used? Yes

System criticality (as determined by agency): High

System security risk (as determined by agency): Moderately low

Reported annual operating costs: $45.0 million

Reported annual labor costs: $6.0 million

Reported cost of modernization: Approximately $10 million

Potential cost savings: Approximately $16.0 million in cost avoidance in fiscal year 2018

Other benefits: Reduction in cybersecurity and operational risks, ability to address security vulnerabilities, avoidance of operational downtime

Status of modernization plans: Agency has documented modernization plans that partially include milestones to complete the modernization and partially describe the work necessary to modernize the legacy system; however, they do not include plans for the disposition of legacy system components following system modernization

Source: GAO analysis of agency documentation and interviews. | GAO-19-471

The Office of Personnel Management's (OPM) System 8 consists of the hardware, software, and service components that support OPM's information technology (IT) applications and services. This system supports the agency's business functions and supports the agency in providing investigative products and services for more than 100 federal agencies.

Modernizing this system is especially important due to past security incidents and persistent security concerns. Specifically, according to OPM, segments of the agency's infrastructure were allowed to age beyond end of life and now pose a significant risk in performance and security to IT operations.[11] Further, in October 2017, OPM's Office of the Inspector General (OIG) reported that the agency's IT environment contained many instances of unsupported software and hardware, where the vendor no longer provided patches, security fixes, or updates for the software. As a result, the OIG noted that there was increased risk that OPM's IT environment contained known vulnerabilities that would never be patched, and could have been exploited to allow unauthorized access to data. In June 2015, OPM reported that an intrusion into its systems had affected the personnel records of about 4.2 million current and former federal employees. Then, in July 2015, the agency reported that a separate but related incident had compromised its systems and the files related to background investigations for 21.5 million individuals. At a June 2015 Congressional hearing, OPM's Director stated that the modernization of the IT infrastructure was critical to protecting the agency's data from adversaries. The Director also stated that it was not feasible to implement encryption on networks that were too old, but noted that OPM was taking other steps to secure the networks.[12]

OPM plans to modernize System 8 by upgrading hardware at the end of life, migrating off of legacy operating systems and support software, and augmenting the agency's established policies and procedures. In fiscal year 2018, OPM completed software and hardware upgrades, including replacement of core switches, network end points, and laptops. In fiscal year 2019, the agency plans to continue its focus on refreshing aged IT infrastructure, so that its hardware components will have the proper

[11]OPM, *Congressional Budget Justification and Annual Performance Plan, Fiscal Year 2019*, (Washington, D.C.: February 2018).

[12]*OPM: Data Breach, Hearing Before the House Committee on Oversight and Government Reform*, 114th Cong. (statement of Director of the Office of Personnel Management Katherine Archuleta).

vendor support. OPM developed multiple documents related to the planning of this modernization effort, including a modernization schedule, and its fiscal year 2019 budget justification.

However, the modernization plans contained in these documents did not include details for the entire modernization effort. The milestones in these documents, for instance, were either no longer current or only contained milestones regarding one part of the project. While the budget justification did outline what it planned to accomplish in fiscal years 2018 and 2019, it did not mention the rest of the work needed to complete the infrastructure modernization.

Similarly, the OIG has reported concerns regarding the agency's plans to modernize its infrastructure.[13] Most recently, in June 2018, the OIG reported that OPM was generally continuing in the right direction toward modernizing its IT environment, but the OIG had concerns with the agency's plan for modernization and its overall approach to IT modernization. For example, the OIG was concerned that OPM's planning documents did not identify the full scope of the modernization effort or contain cost estimates for the individual initiatives or the effort as a whole. The OIG planned to monitor and continue to report on the agency's progress in modernizing its infrastructure.

OPM anticipates realizing both financial and nonfinancial benefits with the modernization of its infrastructure. For example, as a part of its overall infrastructure modernization, the agency avoided approximately $16 million in costs as part of its data center consolidation efforts for fiscal year 2018. The agency also expects that cybersecurity and operational risks associated with end of life hardware will be reduced. To that end, the agency stated that remediating end of life hardware also should allow OPM the ability to address identified security vulnerabilities and avoid operational downtime, as support is more readily available.

[13]See, for example: OPM Office of the Inspector General, Office of Audits, *Management Advisory: U.S. Office of Personnel Management's Fiscal Year 2017 IT Modernization Expenditure Plan*, Report Number 4A-CI-00-18-022 (Feb. 15, 2018) and *Final Management Advisory: U.S. Office of Personnel Management's Fiscal Year 2018 IT Modernization Expenditure Plan*, Report Number 4A-CI-00-18-044 (June 20, 2018).

System 9

Small Business Administration

Reported number of users: Approximately 274,000

Initial year of implementation: 2002

System hardware under warranty? No

Software vendor supported? No

Operating system(s) supported? No

Legacy programming language(s) used? Yes

System criticality (as determined by agency): High

System security risk (as determined by agency): Moderately high

Reported annual operating costs: $62,000

Reported annual labor costs: $214,600

Reported cost of modernization: $750,000

Potential cost savings: None

Other benefits: Increased security and stability of the system

Status of modernization plans: Agency has a documented modernization plan that includes milestones to complete the modernization and plans for the disposition of the legacy system following system modernization; however, it does not include a description of the work necessary to complete the modernization

Source: GAO analysis of agency documentation and interviews. | GAO-19-471

The Small Business Administration's (SBA) System 9 is a system that, according to the agency, provides identification, authentication, and authorization services[14] for several of the agency's applications.

According to the agency, the system was developed by SBA and originally implemented in 2002. Agency officials stated that System 9's hardware and software are no longer supported by the associated vendors. Consequently, according to the agency, it is paying for extended support contracts that have increased operating costs for the system. Further, agency officials stated that the system resides on a platform that is scheduled to be decommissioned within the next year. In addition, the system is coded using a programing language that the agency considers to be a legacy programming language (among others).

The agency's documented modernization plan includes milestones to complete the modernization and plans for the disposition of the legacy system following system modernization; however, the plan does not include a description of the work necessary to complete the modernization. However, agency officials stated that it intends to replace the system's functionality with login.gov. Login.gov was developed and is maintained by the General Services Administration as a single sign-on trusted identity platform.[15] Login.gov provides identification and authentication for applications and is intended to offer the public secure and private online access to participating government programs. However, according to the agency, since login.gov does not provide authorization controls, SBA intends to develop additional software to provide authorization controls beginning in March 2019.

[14]Agencies design and implement access controls to provide assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals. These controls protect computer resources from unauthorized use, modification, disclosure, and loss by limiting, preventing or detecting inappropriate access to them. Two of these control areas are identification and authentication, and authorization. Identification and authentication controls allow a computer system to identify and authenticate different users so that activities on the system can be linked to specific individuals. Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file.

[15]Single sign-on reduces the burden of multiple passwords. It is intended to increase security of the data and systems and compliance with federal information technology policies and best practices.

According to the agency, it does not anticipate any cost benefits from modernizing System 9. However, the agency expects that the security and stability of the system will increase.

System 10

Social Security Administration

Reported number of users: Over 30,000

Initial year of implementation: 1974

System hardware under warranty? Yes

Software vendor supported? Yes

Operating system(s) supported? Yes

Legacy programming language(s) used? Yes

System criticality (as determined by agency): High

System security risk (as determined by agency): Moderate

Reported annual operating costs: $139.2 million[a]

Reported annual labor costs: $6.7 million

Reported cost of modernization: $24.6 million (from fiscal year 2017 to 2022)

Potential cost savings: Approximately $4 million per year from fiscal year 2019 through fiscal year 2027a

Other benefits: Better access to beneficiary data, faster and more efficient claim processing, reduced need for manual data entry, and lower number of improper payments, among others

Status of modernization plans: Agency has documented plans that contain milestones that partially cover the modernization effort and partially describe the work necessary to modernize the system; however, they do not contain plans for the disposition of legacy system components following system modernization

Note: [a]The agency was unable to isolate the operating costs or potential cost savings for this system. The figures presented are the costs and potential savings for all of the systems operating in the mainframe environment.

Source: GAO analysis of agency documentation and interviews. | GAO-19-471

The Social Security Administration's (SSA) System 10 supports the provision of particular Social Security benefits to eligible people. Currently, SSA collects detailed information from the recipients in person, by telephone, and via the internet on multiple platforms (e.g., desktops and hand-held devices), and from internal and external interface methods. System 10 is comprised of many applications that collect information, make payments, and communicate with SSA's clients.

According to SSA's October 2017 information technology modernization plan, the agency needed to modernize its core systems, including System 10, because of complications related to their age and original system design.[16] SSA's modernization plan indicates that, since implementation, these systems had been subjected to constant modifications to incorporate changes in legislation, regulations, and policy. Through the years, new technologies and capabilities had been integrated into the core systems and delivering new capabilities was becoming exorbitantly expensive.

Further, most of the agency's systems, including System 10, are generally unconnected to each other, creating functional silos servicing independent lines of business. According to the agency, navigating these systems is challenging, and copying beneficiary data from system to system can result in data becoming out of sync.

According to the agency's modernization plan, SSA intends to replace its core systems, including System 10, with new components and platforms, engineered for usability, interoperability, and future adaptability. Work accomplished over several years of incremental modernization has already resulted in moving a substantial portion of System 10 away from old technologies. For instance, according to SSA officials in the Office of the Deputy Commissioner, Systems, SSA moved System 10 to a modern, relational database platform and modernized aspects of the user interface.[17] According to an SSA 5-year modernization roadmap, the agency is currently working to modernize and create web services as a part of the effort to consolidate SSA's initial claims processes; however, the roadmap does not offer specific information about these efforts.

[16]Social Security Administration, *IT Modernization: A Business and IT Journey* (Baltimore, MD: Oct. 2017).

[17]A relational database is a system that allows users to store data in and retrieve data from linked databases that are perceived as a collection of relations or tables.

As for its modernization planning efforts, SSA's plans include overall modernization goals, a high-level overview of the planned system architecture, milestones for fiscal year 2018, and a description of the work that it had planned to accomplish in fiscal year 2018. However, the plans do not include either System 10-specific milestones or a description of the work necessary to modernize the legacy system beyond fiscal year 2018. Further, the document does not include plans for the disposition of the legacy system after modernization. According to officials in the Office of the Deputy Commissioner, Systems, the agency will update the planning documentation and make further decisions as the modernization effort progresses.

SSA expects that modernizing System 10 will result in cost savings in addition to many other benefits. For instance, the agency expects that it will be able to save approximately $38 million from modernizing System 10 and other systems running in the agency's mainframe environment. In addition, increased staff access to benefit recipients' data will enable staff to review medical evidence faster and process claims more accurately, among other things. According to the agency's modernization plan, the improvements to the system should improve productivity and service to the public, as well as reduce the number of improper payments due to technician error.

Appendix IV: Comments from the Department of Education

UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE CHIEF INFORMATION OFFICER

THE CHIEF INFORMATION OFFICER

May 10, 2019

Ms. Carol Harris
Director, Information Technology Management Issues
Information Technology and Cybersecurity Team
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Harris:

I am pleased to provide the U.S. Department of Education's (Department's) response to the Government Accountability Office's (GAO's) draft report, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems, GAO-19-471.* We understand GAO conducted this audit to review the Department's legacy systems and evaluate the Department's plans for modernizing the systems.

The Department concurs with GAO's recommendation and will continue necessary efforts to modernize legacy systems.

You may direct your questions to Mr. Thomas Miles, Financial Student Aid, Chief Information Officer, at (202) 377-4125 or at Thomas.Miles@ed.gov.

Sincerely,

Jason K. Gray

400 MARYLAND AVE. S.W., WASHINGTON, DC 20202
www.ed.gov

The Department of Education's mission is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access.

Appendix V: Comments from the Department of Health and Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

MAY 16 2019

Carol C. Harris
Director, Information Technology Management Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Harris:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "*Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*" (GAO-19-351SU).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Matthew D. Bassett
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED – INFORMATION TECHNOLOGY: AGENCIES NEED TO DEVELOP MODERNIZATION PLANS FOR CRITICAL LEGACY SYSTEMS (GAO-19-351SU)

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

Recommendation 2

The Secretary of HHS should ensure that the CIO documents the department's modernization plans for its [redacted] to include milestones and a description of the work necessary to modernize the system, and details on the disposition of the work necessary to modernize the system, and details on the disposition of the legacy system.

HHS Response

HHS concurs with GAO's recommendation. HHS will evaluate ways to provide its modernization plan, including milestones and a description of the work necessary to modernize the system.

Page 1 of 1

Appendix VI: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

May 17, 2019

Carol C. Harris
Director, Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-19-471, "INFORMATION TECHNOLOGY: Agencies Need to Develop Modernization Plans for Critical Legacy Systems"

Dear Ms. Harris:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's positive recognition of DHS's work related to the modernization of multiple Information Technology (IT) infrastructure systems, specifically the agency-wide transition to a DHS private cloud system and migrating legacy services to 13 private cloud offerings. This has allowed DHS to realize $1.6 billion in cost savings, streamline the supply chain for IT services, reduce the amount of labor needed to maintain legacy systems and software, and enhance security. The Department understands the need for diligence with regard to ongoing systems modernization and continues to work towards integrating systems and processes to further enable a more cohesive implementation of future modernization efforts.

The draft report contained eight recommendations, including one for DHS with which the Department concurs. Our detailed response to this recommendation can be found in an Appendix to the "Limited Official Use Only" restricted version of this report (GAO-19-351SU). Technical comments were previously provided under separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

2

Appendix VII: Comments from the Internal Revenue Service

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

DEPUTY COMMISSIONER

May 14, 2019

Ms. Carol C. Harris
Director, Information Technology Management Issues
Information Technology and Cybersecurity (ITC) Team
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Harris:

Thank you for the opportunity to comment on the draft report entitled Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems, GAO-19-351SU and GAO-19-471 (Public) reports.

We recognize the importance of modernizing the Internal Revenue Service's Information Technology (IT) systems, specifically the [redacted] We appreciate the interest that GAO has shown in ensuring we are properly planning for the retirement of legacy systems.

As we reported to GAO, we are currently working to modernize core components of the [redacted] through the [redacted] project, which will be followed by additional work to be planned and delivered by [redacted]. However, the report does not accurately convey that the [redacted] project will replace only the core components of the [redacted] system, not the entire system. Even when the entire [redacted] is completed, this will address only a portion of the work required to retire the [redacted]. We agree with recommendation five in your report: The Secretary of the Treasury should ensure that the CIO includes in the department's modernization plans for its [redacted], milestones to complete the modernization and details on the disposition of its legacy system.

Planning for the retirement of [redacted] is very complex and must be done incrementally. We acknowledge that, to date, the IRS has focused on the [redacted] scope. We must also develop and execute a multiyear strategy, conceptual roadmap and high-level plan for incrementally retiring all functionality of the [redacted]. We agree with the recommendation and will provide a detailed corrective action plan in our 180-day letters to Congress.

If you have any questions, please contact me or a member of your staff may contact Gina Garza, Chief Information Officer, at 202-317-5000.

Sincerely,

Jeffrey J. Tribiano

Enclosure

Enclosure

Information Technology:
Agencies Need to Develop Modernization Plans for Critical Legacy Systems.
GAO-19-351SU
Job Code #102591

Recommendation 5:

The Secretary of the Treasury should ensure that the CIO includes in the department's modernization plans for its [redacted], milestones to complete the modernization and details on the disposition of its legacy system

Response: The IRS agrees with the recommendation. The IRS shall develop a multiyear [redacted] Retirement strategy including: clear boundaries for which [redacted] capabilities are in scope for [redacted]; those that will be accomplished by other programs; an approach and criteria for addressing all components required to retire [redacted]; high level release strategy with estimates of cost and staffing; and, subsequent Independent Verification and Validation of the strategy.

Appendix VIII: Comments from the Office of Personnel Management

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the Chief
Information Officer

MAY 13 2019

Carol C. Harris
Director, Information Technology Management Issues
Information Technology and Cybersecurity (ITC) Team
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Ms. Harris:

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, entitled *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-351SU).

Recommendation #6: The Director of OPM should ensure that the CIO includes in the agency's modernization plans for its [redacted], all milestones to complete the modernization, a description of all the work necessary to modernize the system, and a description of how it intends to dispose of its legacy system.

Management Response:

We concur. We plan to further develop our existing plans for the modernization of the OPM [redacted]. In such plans, we intend to include additional milestones needed to complete the modernization efforts, a fuller description of the work necessary to modernize the infrastructure, and also a description of how we intend to dispose of any legacy components of the existing [redacted]. Our modernization plan will include efforts such as the following:

- Upgrade agency email functionality and migration to Office 365
- Upgrade VOIP/SIP Trunking/ACD
- Further reduce end-of-life equipment
- Implement mainframe modernization plan, informed by the assessment of alternatives
- Continue upgrade efforts of Legacy Applications, to include Retirement Benefits and Trust Fund
- Continue Datacenter Consolidation Activities

In addition, as we have previously reported, we have already accomplished numerous modernization efforts to include:

- Upgraded network equipment and configurations to better align with standards
- Reduced end-of-life equipment by 30%
- Developed a mainframe modernization assessment of alternatives
- Upgraded video chat and video messaging services

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact MC Price, (478) 744-2051, Mary.Price1@opm.gov.

Sincerely,

Clare Martorana
Chief Information Officer

OPM.GOV Empowering Excellence in Government through Great People USAJOBS.GOV

Appendix IX: Comments from the Small Business Administration

LIMITED OFFICIAL USE ONLY

U.S. Small Business Administration

May 17, 2019

Ms. Carol C. Harris
Director, Information Technology Acquisition Management Issues
U. S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Harris:

Thank you for providing the U. S. Small Business Administration (SBA) with a copy of the Government Accountability Office (GAO) draft report titled "Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems" GAO-19-19-471 (103413). The draft report reviewed federal agencies legacy systems to identify the most critical federal legacy systems in need of modernization. In addition, they identified examples of legacy system modernization initiatives that agencies considered successful.

Recommendation 7: The Administrator of the Small Business Administration should ensure that the CIO includes in the agency's modernization plans for the [redacted], a description of the work necessary to modernize the system.

SBA Response: Concur. SBA Office of the Chief Information Officer (OCIO) and the appropriate program offices will include a description of the work necessary to modernize the system in the [redacted] Project Plan. Estimated Completion Date: 07-31-2019.

Thank you for the opportunity to comment on this draft report.

Sincerely,

MARIA ROAT
Digitally signed by MARIA ROAT
Date: 2019.05.17 08:07:40 -04'00'

Maria Roat
Chief Information Officer

LIMITED OFFICIAL USE ONLY

Appendix X: Comments from the Social Security Administration

SOCIAL SECURITY
Office of the Commissioner

May 10, 2019

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

Dear Ms. Harris,

Thank you for the opportunity to review the public draft report "INFORMATION TECHNOLOGY: Agencies Need to Develop Modernization Plans for Critical Legacy Systems (GAO-19-471).

We are modernizing the System 10 using agile software methods and a multi-year roadmap of development activity and milestones. To date, we have modernized claim intake for System 10, and we are now focusing on modernization for post-eligibility transactions. We update our roadmap on a regular basis to meet changing business needs and technology. As we complete our modernization work, we expect to retire most of the System 10 legacy software.

We submitted technical comments and a sensitivity review of this draft report at the staff level.

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

Sincerely,

Stephanie Hall

Stephanie Hall
Acting Deputy Chief of Staff

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Appendix XI: Comments from the Department of Housing and Urban Development

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-3000

CHIEF INFORMATION OFFICER

MAY 16 2019

Mr. Kevin Walsh
Assistant Director, IT
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Walsh:

Thank you for the opportunity to review and comment on the draft report for GAO-19-351SU / GAO-19-471, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*. HUD reviewed both versions of the draft document and has no comments or concerns regarding release of the public draft.

If you have questions or require additional information, please contact Janice Ausby, Deputy Chief Information Officer, Business and IT Resource Management Office, at (202) 402-7605 (Janice.L.Ausby@hud.gov), or Juanita L. Toatley, Audit Liaison, Audit Compliance Branch, at (202) 402-3555 (Juanita.L.Toatley@hud.gov).

Sincerely,

David Chow
Chief Information Officer

Appendix XII: Comments from the U.S. Agency for International Development

Carol C. Harris
Director, Information-Technology Management Issues
Information Technology and Cybersecurity (ITC) Team
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20226

Re: Agencies Need to Develop Modernization Plans for Critical Legacy Systems (GAO-19-351SU and GAO-19-471)

Dear Ms. Harris:

I am pleased to provide the formal response of the U.S. Agency for International Development (USAID) to the draft reports produced by the U.S. Government Accountability Office (GAO) titled, "Agencies Need to Develop Modernization Plans for Critical Legacy Systems" (GAO-19-351SU and GAO-19-471).

As a leader in the modernization of information technology (IT) in the Federal Government, USAID remains committed to keeping its IT current and avoiding costly legacy systems. A pioneer of cloud-based email and an early adopter of the Data-Center Optimization Initiative, USAID has effectively followed the model of successful IT-modernization initiatives highlighted in the GAO's report. USAID has leveraged IT to enhance our development mission and achieve a wide range of benefits, including cost-savings, as noted in the case studies.

I am transmitting this letter and the enclosed comments from USAID for inclusion in the final report. Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement. We appreciate the opportunity to participate in the complete and thorough evaluation of critical legacy systems across the Federal Government. USAID does not consider any of the material in the public version of GAO-19-471 to be sensitive in nature.

Sincerely,

Frederick Nutt
Assistant Administrator
Bureau for Management

Appendix XIII: 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: Dave Powner (Director), Kevin Walsh (Assistant Director), Jessica Waselkow (Assistant Director), Chris Businsky, Rebecca Eyler, Angel Ip, and Meredith Raymond.