United States Government Accountability Office

Testimony

Before the Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00, a.m ET
Tuesday, April 27, 2021

INFORMATION TECHNOLOGY

Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems

Statement of Kevin Walsh, Director, Information Technology and Cybersecurity

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-21-524T

GAO@100

Highlights

Highlights of GAO-21-524T, a testimony before the Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs, U.S. Senate

April 2021

INFORMATION TECHNOLOGY

Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems

Why GAO Did This Study

Each year, the federal government spends more than $100 billion on IT and cyber-related investments. Of this amount, agencies have typically spent about 80 percent on the operations and maintenance of existing IT investments, including legacy systems. However, federal legacy systems are becoming increasingly obsolete. In May 2016, GAO 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. Similarly, in June 2019 GAO reported that several of the federal government's most critical legacy systems used outdated languages, had unsupported hardware and software, and were operating with known security vulnerabilities.

GAO was asked to testify on its June 2019 report on federal agencies' legacy systems. Specifically, GAO summarized (1) the critical federal legacy systems that we identified as most in need of modernization and (2) its evaluation of agencies' plans for modernizing them. GAO also provided updated information regarding agencies' implementation of its related recommendations.

What GAO Recommends

In a "limited official use only" version of its June 2019 report, GAO made 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.

View GAO-21-524T. For more information, contact Kevin Walsh at (202) 512-6151 or WalshK@gao.gov.

What GAO Found

In June 2019, GAO identified 10 critical federal information technology (IT) legacy systems that were most in need of modernization. These legacy systems provided vital support to agencies' missions. According to the agencies, these legacy systems ranged from about 8 to 51 years old and, collectively, cost about $337 million annually to operate and maintain. Several of the systems used older languages, such as Common Business Oriented Language (COBOL). GAO has previously reported that reliance on such languages has risks, such as a rise in procurement and operating costs, and a decrease in the availability of individuals with the proper skill sets. Further, several of the legacy systems were operating with known security vulnerabilities and unsupported hardware and software.

Of the 10 agencies responsible for these legacy systems, GAO reported in June 2019 that 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). Of the seven agencies with plans, only the Departments of the Interior's and Defense's modernization plans included all of 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). The other five agencies lacked complete modernization plans. The Departments of Education, Health and Human Services, and Transportation did not have documented modernization plans.

Table: Extent to Which Agencies' Had Documented Modernization Plans for Legacy Systems That Included Key Elements, as of June 2019

Agency	Included milestones to complete the modernization	Described work necessary to modernize system	Summarized planned disposition of legacy system
Department of Defense	Yes	Yes	Yes
Department of Education	n/a – did not have a documented modernization plan		
Department of Health and Human Services	n/a – did not have a documented modernization plan		
Department of Homeland Security	No	Yes	No
Department of the Interior	Yes	Yes	Yes
Department of the Treasury	Partial	Yes	No
Department of Transportation	n/a – did not have a documented modernization plan		
Office of Personnel Management	Partial	Partial	No
Small Business Administration	Yes	No	Yes
Social Security Administration	Partial	Partial	No

Source: GAO analysis of agency modernization plans. | GAO-21-524T

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

GAO stressed that, until the eight agencies established complete plans, their modernizations would face an increased risk of cost overruns, schedule delays, and project failure. Accordingly, GAO recommended that each of the eight develop such plans. However, to date, seven of the agencies had not done so. It is essential that agencies implement GAO's recommendations and these plans in order to meet mission needs, address security risks, and reduce operating costs.

Chair Hassan, Ranking Member Paul, and Members of the Subcommittee:

I am pleased to participate in today's hearing on the federal government's legacy information technology (IT) systems. Each year, the federal government spends more than $100 billion on IT and cyber-related investments. Of this amount, agencies have typically reported spending about 80 percent on the operations and maintenance of existing IT investments, including legacy systems.[1]

However, federal legacy systems are becoming increasingly obsolete. In May 2016, we 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.[2] Likewise, in June 2019, we reported that several of the federal government's most critical legacy systems used outdated languages, had unsupported hardware and software, and were operating with known security vulnerabilities.[3]

As you requested, my testimony today discusses the results from our June 2019 report on federal agencies' legacy systems. Specifically, it summarizes (1) the critical federal legacy systems that we identified as most in need of modernization and (2) our evaluation of agencies' plans for modernizing them. Detailed information on the objectives, scope, and methodology for that work can be found in the issued report. In addition, this statement includes updated information regarding agencies' implementation of related recommendations that we made in a "limited official use only" version of the June 2019 report.

We conducted the work on which this statement is based 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

[1]The provisions commonly referred to as the Modernizing Government Technology (MGT) Act define 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, 131 Stat. 1586-94 (2017).

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

[3]GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems,* GAO-19-471 (Washington, D.C.: June 11, 2019).

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.[4] 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.

- **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.[5] 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.[6]
- **Unmet mission needs**. Legacy systems may not be able to reliably meet mission needs because they are outdated or obsolete. For

[4]As a result of the difficulties in acquiring, developing, and managing IT investments the federal government has experienced, we identified "Improving the Management of IT Acquisitions and Operations" as a high-risk area in February 2015. GAO's high-risk program identifies government operations with vulnerabilities to fraud, waste, abuse, and mismanagement, or in need of transformation to address economy, efficiency, or effectiveness challenges. Every 2 years, we issue an update that describes the status of these high-risk areas and actions that are still needed to assure further progress, and identifies new high-risk areas needing attention by Congress and the executive branch. We continue to identify this area as high risk. GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas,* GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

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

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

instance, in 2016, the Department of State's (State) Inspector General reported on the unreliability of the Bureau of Consular Affairs' legacy systems.[7] 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).[8] Agencies have had difficulty finding employees with such knowledge and may have to pay a premium for specialized staff or contractors. For example, we reported in May 2016 that the Social Security Administration (SSA) had to rehire retired employees to maintain its COBOL systems.[9]

  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.[10] 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.

[7]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).

[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. See Gartner, *IT Market Clock for Application Development,* August 2010. In another report, Gartner noted that COBOL is an aging language, with declining skill sets. See *IT Modernization the Changing Technology of Batch Processing*, August 2010.

[9]GAO-16-468.

[10]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).

- **Increased costs.** The cost of operating and maintaining legacy systems increases over time. The issue of cost is linked to security risks, unmet mission needs, and staffing issues, as described above, 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.

Agencies reported that they consider several factors prior to deciding whether to modernize a legacy system. In particular, they reported evaluating 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.[11] 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 mitigate a legacy system's cybersecurity risk by preventing remote hackers from having system access.[12]

  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.[13] 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.

[11]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.

[12]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).

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

- **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 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 the 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 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.

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 December 2018, OMB issued a memorandum that provided guidance regarding the

establishment and enhancement of the High Value Asset program.[14] It stated that the program is to be operated by the Department of Homeland Security (DHS) in coordination with OMB. 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.[15]

- **Enactment of provisions commonly referred to as 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.[16] 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.[17] 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. Specifically, the guidance allowed agencies

[14]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.

[15]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.

[16]*National Defense Authorization Act for Fiscal Year 2018*, Pub. L. No. 115-91, Div. A, Title X, Subtitle G, 131 Stat. 1586-94 (2017).

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

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 Chief Information Officer (CIO) (Chair); (2) a senior official with IT development technical expertise from GSA; (3) a member of DHS's National Protection and Program Directorate;[18] and (4) four federal employees with technical expertise in IT development, financial management, cybersecurity and privacy, and acquisition, appointed by the Director of OMB.[19]

In December 2019, we reported that Congress had appropriated $125 million to the fund, but that challenges with covering the cost of operating the fund had resulted in fewer funds being available than anticipated for the new projects.[20] On March 11, 2021, Congress and the President enacted legislation that appropriated an additional $1 billion to be available until September 30, 2025, to carry out the purposes of the fund.[21]

As of April 2021, the Technology Management Fund Board had approved approximately $89 million for 11 IT modernization projects across seven agencies: the Department of Agriculture, the Department of Energy, DHS, the Department of Housing and Urban Development (HUD), the Department of Justice, the Department of Labor, and GSA. For example, the board approved $13.9 million for HUD to modernize a mainframe and five COBOL-based applications that are expensive to maintain. According to the board's website,

[18]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 as the Cybersecurity and Infrastructure Security Agency and established a director and responsibilities for the agency.

[19]As of April 2021, these four employees were the Department of Agriculture's Farm Production and Conservation Mission Area Assistant CIO, National Science Foundation's Deputy Assistant Director for Computer and Information Science and Engineering, National-Geospatial Intelligence Agency's Deputy Chief Technology Officer, and VA's Chief Technology Officer.

[20]GAO, *Technology Modernization Fund: OMB and GSA Need to Improve Fee Collection and Clarify Cost Estimating Guidance for Awarded Projects*, GAO-20-3 (Washington, D.C.: Dec. 12, 2019).

[21]American Rescue Plan Act of 2021, Pub. L. No: 117-2, Title IV, § 4011, 135 Stat. 4, 80 (2021).

without these funds, HUD would not have been able to pursue this project for several years.

GAO Identified the 10 Most Critical Federal Legacy Systems; Agencies Often Lacked Complete Plans for Their Modernization

Of 65 critical federal legacy systems that agencies identified for our June 2019 report (further discussed in appendix I), we determined the 10 that were most in need of modernization.[22] These legacy systems provided vital support to their agencies' missions.

According to the agencies, at the time, these 10 legacy systems ranged from about 8 to 51 years old and, collectively, cost approximately $337 million annually to operate and maintain.[23] Several of the systems used older languages, such as COBOL and assembly language code.[24] 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.[25]

Further, several of these legacy systems were 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.

[22]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 I 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.

[23]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.

[24]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.

[25]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).

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, the Department of the Interior's (Interior) system contained obsolete hardware that was 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 remained operational may have had long-term exposure to security and performance weaknesses.

Table 1 provides a generalized list of each of the 10 critical legacy systems that we identified, as of June 2019, 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 II provides additional generalized agency-reported details on each of these 10 legacy systems, as of June 2019.

Table 1: The 10 Critical Federal Legacy Systems Most in Need of Modernization, as of June 2019

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

Source: GAO analysis of agency data. | GAO-21-524T

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.

[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 Lacked 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. Our review of government and industry best practices for the modernization of federal IT[26] stressed that 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, as of June 2019, the majority lacked complete plans for modernizing the systems. Specifically, seven agencies (DOD, DHS, Interior, Treasury, the Office of Personnel Management (OPM), the Small Business Administration (SBA), and SSA) had documented

[26]GSA, Unified Shared Services Management, *Modernization and Migration Management (M3) Playbook* (Aug. 3, 2016); and *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).

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.

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, the modernization plan that DHS's Federal Emergency Management Agency developed for its selected legacy system described the work that the department needed to accomplish; however, the plan 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 for 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,[27] agencies should have high-level information on cost, scope, and timing.[28]

Table 2 identifies the extent to which agencies had documented modernization plans for their critical systems that included the three key elements, as of June 2019. (Due to sensitivity concerns, we substituted a numeric identifier for the system names.)

Table 2: Extent to Which Agencies' Had Documented Modernization Plans for Legacy Systems That Included Key Elements, as of June 2019

Agency	System name[a]	Included milestones to complete the modernization	Described work necessary to modernize system	Summarized planned disposition of legacy system
Department of Defense	System 1	Yes	Yes	Yes
Department of Education	System 2	n/a – did not have a documented modernization plan		
Department of Health and Human Services	System 3	n/a – did not have a documented 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	n/a – did not have a documented 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 modernization plans. | GAO-21-524T

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.

[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:

[27]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.

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

- 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 had yet to complete its modernization planning, even though modernization efforts were currently underway. The officials said that they would update the planning documentation and make further decisions as the modernization effort progresses.

Officials within the DHS Federal Emergency Management Agency's Office of the CIO stated that the office's plans for modernizing the system we reviewed (System 4) were contingent on receiving funding and being able to allocate staffing resources to planning activities. According to the officials, the agency was 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 had 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.

As we noted in our report, we recognize that system modernizations are dependent on funding; however, 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.

Given these risks, in June 2019, we issued a "limited official use only" report that we issued concurrently with the June 2019 report that contained eight recommendations to eight federal agencies to identify and document modernization plans for their respective legacy systems. These plans were to include milestones, a description of the work necessary, and details on the disposition of the legacy system. However, as of April 2021, seven of the eight agencies had not implemented the recommendations.

Further, agencies may not have effectively planned for the modernization of legacy systems, in part, because they were not required to. As we reported in May 2016, agencies were not required to identify, evaluate, and prioritize existing IT investments to determine whether they should be kept as-is, modernized, replaced, or retired.[29] Accordingly, we recommended that OMB direct agencies to identify legacy systems needing to be replaced or modernized.

As of April 2021, 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 OMB's December 2018 guidance.[30] However, 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.

In summary, our June 2019 report emphasized the need and importance for agencies to develop a complete plan to modernize their federal 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 increased the likelihood of cost overruns, schedule delays, and

[29]GAO-16-468.

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

overall project failure. Such outcomes would be particularly detrimental because of the importance of these systems to agency missions.

In this regard, in June 2019, we recommended that the eight federal agencies 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. It is essential that agencies implement our recommendations and these plans in order to meet mission needs, address security risks, and reduce operating costs.

Chair Hassan, Ranking Member Paul, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Kevin C. Walsh, Director of Information Technology and Cybersecurity, at (202) 512-6151 or walshk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Jessica Waselkow (Assistant Director), Ashfaq Huda (Analyst-in-Charge), Andrew Avery, Sharhonda Deloach, Rebecca Eyler, and Scott Pettis.

Appendix I: The 24 Chief Financial Officers Act Agencies' Critical Legacy Systems Most in Need of Modernization, as of June 2019

Each of the 24 Chief Financial Officers Act[1] agencies identified their agency's critical legacy systems most in need of modernization. The agencies identified a total of 65 such systems.[2] The agencies also identified various attributes of the legacy systems, including the systems' age, hardware age,[3] system criticality, and security risk. Table 3 provides a generalized list of the critical legacy systems most in need of modernization, as identified by the agencies as of June 2019, 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 critical legacy systems most in need of modernization that we discussed in our report and we assigned a letter or letters to identify the remaining 55 systems.)

Table 3: Combined List of Agencies' Critical Legacy Systems Most in Need of Modernization, as of June 2019

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

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

[2]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.

[3]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)
	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
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

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)
	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
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.				

Source: GAO analysis of agency documentation. | GAO-21-524T

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.

[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 II: Profiles of the 10 Critical Legacy Systems Most in Need of Modernization, as of June 2019

This appendix provides additional details on the 10 critical legacy systems with the greatest need for modernization, as we identified during our June 2019 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.

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 had documented modernization plans that included 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, as of June 2019. | GAO-21-524T

System 1, as of June 2019

The Department of Defense (DOD)—U.S. Air Force's System 1 provided configuration control and management to support wartime readiness and operational support of aircraft, among other things.

According to Air Force documentation, the cost to maintain and sustain the system had 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)[4] programmers, poor legacy documentation, and an aging infrastructure and code. In addition, the system ran on a mainframe that was hosted by another agency. As a result of these issues, Air Force officials expected annual costs to rise from $21.8 million in 2018 to approximately $35 million beginning in 2020.

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 contained goals and outlined how the contractor planned to move through the modernization process, listing out sequential tasks leading to project completion. In addition, it outlined milestones from the starting point through implementation, and provided for the disposition of the legacy system. After the migration, as funding allowed, the Air Force planned to incrementally transform the system's COBOL code to a more modern language.

Air Force program office officials stated that the modernized system would 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 expected increased functionality with this modernization leading to

[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. See Gartner, *IT Market Clock for Application Development,* August 2010. In another report, Gartner noted that COBOL is an aging language, with declining skill sets. See *IT Modernization the Changing Technology of Batch Processing*, August 2010.

increased aircraft touch time[5] and aircraft availability by enabling adoption of new technologies.

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

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 had not determined costs

Potential cost savings: Agency had not calculated

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

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

Source: GAO analysis of agency documentation and interviews, as of June 2019. | GAO-21-524T

System 2, as of June 2019

The Department of Education's (Education) System 2 processed and stored student information and supported the processing of federal student aid applications.

Education first implemented System 2 in 1973.[6] Agency officials stated that the system ran approximately 1 million lines of Common Business Oriented Language (COBOL)[7] on an IBM mainframe. COBOL is a legacy language that can be costly to maintain. The department noted that 18 contractors were employed to maintain the COBOL programming language for this and another system. At the time, 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 intended to modernize System 2 as part of its Next Generation Financial Services Environment initiative. This initiative was to modernize Federal Student Aid's technical and operational architecture and improve the customer experience. The agency expected to consolidate all customer-facing websites and implement a new loan servicing platform to benefit federal student loans.

As of June 2019, Education had not developed a plan for the modernization of System 2. According to agency officials, at the time, modernization plans were 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 had not calculated the specific cost savings associated with modernizing System 2, the department anticipated potential cost savings, including decreased hardware and software licensing costs and

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

[7]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. See Gartner, *IT Market Clock for Application Development,* August 2010. In another report, Gartner noted that COBOL is an aging language, with declining skill sets. See *IT Modernization the Changing Technology of Batch Processing*, August 2010.

decreased costs associated with changes to business rules. According to the agency, other potential benefits of modernizing this system included integration across the enterprise, improved cybersecurity and data protection, reduced system complexity, and improved system efficiency.

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 had not calculated

Potential cost savings: Agency had not calculated

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

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

Source: GAO analysis of agency documentation and interviews, as of June 2019. | GAO-21-524T

System 3, as of June 2019

The Department of Health and Human Services' (HHS) System 3 was a clinical and patient administrative information system. HHS's component, Indian Health Service (IHS), used 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.

At the time, HHS officials stated that the modernization of System 3 was imperative. Specifically, the agency noted that the system's technical architecture and infrastructure were outdated. This resulted in challenges in developing new capabilities in response to business and regulatory requirements. Further, System 3 was coded in C++ and MUMPS. MUMPS is a programming language that HHS considered to be a legacy language.[8] The agency noted that it had 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 was installed on hundreds of separate computers, which 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 as of June 2019, the agency did 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 was to be conducted in several stages, and a substantial part of the research was to be an evaluation of the current state of health IT across IHS's health facilities. Once the research was conducted, in consultation with IHS and its stakeholders, the contractor intended to use the findings and recommendations to propose a prioritized roadmap for modernization. According to HHS, the agency anticipated that it might have been able to begin to execute an implementation plan as early as 2020.

[8]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 would take significant capital investment to complete and it was 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.

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 had not calculated

Potential cost savings: Agency had not calculated

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

Status of modernization plans: Agency had documented modernization plans that described the work necessary to modernize the system; however, they did 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, as of June 2019. | GAO-21-524T

System 4, as of June 2019

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

According to the agency, at the time, System 4 needed to be modernized because there were 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, at the time, 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 was not certain exactly how many devices made 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 planned to develop an inventory reconciliation strategy and process to address this issue.

As of June 2019, FEMA intended to replace System 4's devices in two phases. The first phase was planned to target the agency's smaller facilities, while the second phase was planned to address the larger facilities, which may require more complex installations. In 2019, FEMA's Office of the Chief Information Officer was conducting site surveys to better define requirements and cost estimates. While the agency had 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, as of June 2019, FEMA intended to replace 240 of the 545 devices that were at the end of support, if funds were available. The agency also intended to upgrade the remaining 305 devices in the future, if funds were available.

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

technology and increased throughput.[9] 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.

[9]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.

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 had documented modernization plans that included 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, as of June 2019. | GAO-21-524T

System 5, as of June 2019

The Department of the Interior's (Interior) System 5 was an Industrial Control System (ICS) Supervisory Control and Data Acquisition (SCADA) System that supported the general operation of dams and power plants on a particular river and its tributaries. The system served 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.

As of June 2019, the system was approximately 18 years old and contained obsolete hardware that was 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 remained 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 provided flexibility, functionality, and resilience, large segments of the systems remained vulnerable to attack, potentially causing significant economic or human impact. Further, according to Interior's system modernization plans, the agency needed to modernize the system in order to increase data collection capabilities and security. Specifically, the system was 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 was expected to accommodate future growth requirements. The plans also supported the complete replacement of the system's obsolete hardware and software. The modernization plans also outlined goals, milestones, and the work to be accomplished. The agency planned to complete the modernization by January 2020.

By replacing the legacy system, Interior planned to realize a number of potential benefits, including annual cost savings of $152,000. In addition, with modernization, the system would no longer run on obsolete, unsupported hardware. Furthermore, newer software and hardware were 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.

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 had documented modernization plans that described the work necessary to modernize the legacy system; however, they only partially included milestones and did not include details on the disposition of the legacy system

Note: [a]The agency stated that the system did not have traditional users and instead passed along data for applications to use. In 2018, the system helped process over 154 million tax returns.

Source: GAO analysis of agency documentation and interviews, as of June 2019. | GAO-21-524T

System 6, as of June 2019

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

System 6 was written in a now outdated assembly language code[10] and Common Business Oriented Language (COBOL).[11] 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 for staff or contractors with the knowledge to maintain these systems.[12]

IRS planned to address these concerns by modernizing core components of System 6. The new system was intended to provide improved functionality. However, at the time, IRS was having trouble fully staffing the modernization effort, resulting in significant delays. While the agency had developed modernization plans, they were incomplete. For example, the plans' milestones did 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 had not provided a target date for decommissioning the legacy system.

[10]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.

[11]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. See Gartner, *IT Market Clock for Application Development,* August 2010. In another report, Gartner noted that COBOL is an aging language, with declining skill sets. See *IT Modernization the Changing Technology of Batch Processing*, August 2010.

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

While IRS did not anticipate cost savings associated with the modernization of this system, it anticipated many internal and external benefits for both the taxpayer and the agency. In particular, according to the IRS's *Fiscal Year 2019 Capital Investment Plan*, the benefits of modernizing this system included: (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 were not possible.

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 had not calculated

Potential cost savings: Agency had not calculated

Other benefits: Enhanced security, compliance with law

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

Source: GAO analysis of agency documentation and interviews, as of June 2019. | GAO-21-524T

System 7, as of June 2019

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

According to Transportation, the system was DOS-based and needed to be updated to continue to efficiently meet its mission.[13] Specifically, some of the core system components were mainframe applications that had been in operation since 1984. In addition, the system was running unsupported software, including one operating system that was last supported by the vendor in 2010.

As of June 2019, FAA was 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 did not have a documented modernization plan. At the time, officials stated that the agency was seeking alternatives to modernize the system and meet legislative requirements. FAA had asked interested vendors to respond to a request for information. According to the agency, the responses to this request were intended to inform strategic decisions about the modernization, and are planned to ultimately lead to proposed solutions from industry.

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

[13]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.

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 had documented modernization plans that partially included milestones to complete the modernization and partially described the work necessary to modernize the legacy system; however, they did not include plans for the disposition of legacy system components following system modernization

Source: GAO analysis of agency documentation and interviews, as of June 2019. | GAO-21-524T

System 8, as of June 2019

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

Modernizing this system was 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 posed a significant risk in performance and security to IT operations.[14] 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.[15]

At the time, OPM planned 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 planned to continue its focus

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

[15]*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).

on refreshing aged IT infrastructure, so that its hardware components will have the proper 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 outlined 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 had reported concerns regarding the agency's plans to modernize its infrastructure.[16] 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 anticipated 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 expected that cybersecurity and operational risks associated with end of life hardware would 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 became more readily available.

[16]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).

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 had a documented modernization plan that included milestones to complete the modernization and plans for the disposition of the legacy system following system modernization; however, it did not include a description of the work necessary to complete the modernization

Source: GAO analysis of agency documentation and interviews, as of June 2019. | GAO-21-524T

System 9, as of June 2019

The Small Business Administration's (SBA) System 9 was a system that, according to the agency, provided identification, authentication, and authorization services[17] for several of the agency's applications.

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

As of June 2019, the agency's documented modernization plan included milestones to complete the modernization and plans for the disposition of the legacy system following system modernization; however, the plan did not include a description of the work necessary to complete the modernization. However, agency officials stated that it intended 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.[18] 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 did not provide authorization controls, SBA intended to develop additional software to provide authorization controls beginning in March 2019.

[17]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.

[18]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.

As of June 2019, according to the agency, it did not anticipate any cost benefits from modernizing System 9. However, the agency expected that the security and stability of the system would increase.

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 2027[a]

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 had documented plans that contained milestones that partially covered the modernization effort and partially described the work necessary to modernize the system; however, they did 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, as of June 2019. | GAO-21-524T

System 10, as of June 2019

The Social Security Administration's (SSA) System 10 supported the provision of particular Social Security benefits to eligible people. At the time, SSA collected 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 was comprised of many applications that collected information, made payments, and communicated 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.[19] SSA's modernization plan indicated 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, as of June 2019, most of the agency's systems, including System 10, were generally unconnected to each other, creating functional silos servicing independent lines of business. According to the agency, navigating these systems was challenging, and copying beneficiary data from system to system could result in data becoming out of sync.

According to the agency's modernization plan, SSA intended 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 had 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.[20] According to an SSA 5-year modernization roadmap, the agency was currently working to modernize and create web services as a part of the effort to consolidate SSA's initial

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

[20]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.

claims processes; however, the roadmap did not offer specific information about these efforts.

As for its modernization planning efforts, SSA's plans included 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 did 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 did 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 intended to update the planning documentation and make further decisions as the modernization effort progressed.

SSA expected that modernizing System 10 would result in cost savings in addition to many other benefits. For instance, the agency expected that it would 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 would 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 would improve productivity and service to the public, as well as reduce the number of improper payments due to technician error.