United States Government Accountability Office

Testimony

Before the Subcommittee on Cybersecurity, Information Technology, and Government Innovation, Committee on Oversight and Accountability, House of Representatives

For Release on Delivery
Expected at 2:00, p.m. EST
Wednesday, May 10, 2023

INFORMATION TECHNOLOGY

Agencies Need to Continue Addressing Critical Legacy Systems

Statement of Kevin Walsh, Director, Information Technology and Cybersecurity

GAO-23-106821

May 2023

INFORMATION TECHNOLOGY

Agencies Need to Continue Addressing Critical Legacy Systems

GAO Highlights

Highlights of GAO-23-106821, a testimony before the Subcommittee on Cybersecurity, Information Technology, and Government Innovation, Committee on Oversight and Accountability, House of Representatives

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 reported spending about 80 percent on operations and maintenance of existing IT, including legacy systems.

Maintaining federal legacy systems can pose significant challenges. In May 2016, GAO reported instances where agencies had systems with components that were at least 50 years old or vendors that 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 Similarly, in June 2019, GAO reported that several of the federal government's most critical legacy systems used outdated languages, had unsupported hardware and software, and were operating with known security vulnerabilities.

This statement is based primarily on GAO's 2019 report on federal agencies' legacy systems. GAO summarized the (1) critical federal legacy systems identified as most in need of modernization and (2) status of agencies' plans for modernizing them. It also analyzed updated information on agencies' implementation of GAO's recommendations, and summarized other relevant legacy systems reports.

What GAO Recommends

In a 2019 report, GAO recommended that eight agencies have modernization plans for legacy systems. The agencies agreed but two have not yet implemented the recommendations. GAO also had a 2016 recommendation to OMB on agency identification of systems needing modernization, and OMB agreed with it. The recommendation has not yet been implemented.

View GAO-23-106821. 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 IT legacy systems (i.e., systems that are outdated or obsolete) 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 eight agencies either did not have documented plans for modernizing their systems or had incomplete plans. Agency plans were incomplete if they were missing any of the 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.

Six of those eight agencies have implemented GAO's recommendations to identify and document modernization plans for their respective legacy systems. However, as of May 2023, two agencies (the Department of Transportation and the Office of Personnel Management) have not developed complete modernization plans (see table). Developing such plans is essential to addressing mission needs, dealing with security risks, and reducing operating costs.

Table: Extent to Which Selected Agencies Had Documented Modernization Plans for Legacy Systems

Agency	Had modernization plan with key elements, as of June 2019?	Has addressed incomplete elements of modernization plan, as of May 2023?
Department of Transportation	No. Agency did not have a documented modernization plan.	No. In April 2022, agency officials informed GAO that they expected to go live with the modernized system in the fall of 2022; however, as of May 2023, GAO has not received documented plans for this modernization effort.
Office of Personnel Management	Partial. Agency had a modernization plan but it did not fully include milestones or work necessary, and it did not include the disposition of the legacy system.	No. As of May 2023, GAO has not received evidence that the agency has developed a comprehensive modernization plan for this system.

Source: GAO analysis of agency modernization plans. | GAO-23-106821

Implementing GAO's prior recommendation to the Office of Management and Budget (OMB) on finalizing guidance directing agencies to identify systems needing modernization is essential. While OMB had drafted such guidance, it has not yet been issued. Doing so would provide greater assurance that the risks of continuing to operate legacy systems are being addressed government-wide.

Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee:

I am pleased to participate in today's hearing on the federal government's legacy 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]

Maintaining federal legacy systems can pose significant challenges. For example, in May 2016, we reported instances where agencies had systems with components that were at least 50 years old or had vendors that 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 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) the status 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 our analysis of updated information regarding agencies' implementation of related recommendations that we made in a "limited official use only" version of the 2019 report. We also summarize recently issued GAO and Inspector General reports that discuss legacy systems.

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

[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, § 1076(8), 131 Stat. 1586, 1587 (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).

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.[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 October 2017, the Office of Personnel Management's (OPM) Office of the Inspector General 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.[5] The report noted that as a result, 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.

  Additionally, in November 2017, the Department of Education's Inspector General identified security weaknesses that included the department's use of unsupported operating systems, databases, and

[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: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas,* GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

[5]U.S. Office of Personnel Management, Office of the Inspector General, *Final Audit Report: Federal Information Security Modernization Act Audit Fiscal Year 2017*, Report Number 4A-CI-00-17-020 (Washington, D.C.: Oct. 27, 2017).

applications.[6] 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.[7]

Further, in January 2023, we reported that about 33 percent of the Internal Revenue Service's (IRS) applications, 23 percent of the software instances in use, and 8 percent of hardware assets were considered legacy.[8] This included applications ranging from 25 to 64 years in age, as well as software up to 15 versions behind the current version. The IRS acknowledged that operating in this environment would continue to contribute to security risks, among other challenges.

- **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 Inspector General reported on the unreliability of the Bureau of Consular Affairs' legacy systems.[9] 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.

  Additionally, in January 2023, we reported that the IRS' 60-year old system for individual tax data, the Individual Master File (IMF), needed to be modernized to help address business and technical challenges. Such challenges included the inability to get a real-time view of the taxpayer's account and provide additional information to combat fraud and identity theft. We reported that the IRS had suspended the operations of six initiatives, including two which are essential to replacing the IMF. According to officials, the suspensions were due to IRS's determination to shift resources to higher priorities,

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

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

[8]GAO, *Information Technology: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements,* GAO-23-104719 (Washington, D.C.: Jan. 12, 2023).

[9]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).

and staff members working on these suspended initiatives were reassigned to other projects. As a result, the schedule for these initiatives was undetermined, and the 2030 target completion date for replacing the IMF became unknown. We reported that this would lead to mounting challenges in continuing to rely on a critical system with software written in an archaic language requiring specialized skills. IRS officials subsequently reported in April 2023 that they now plan to use additional funding to complete IMF system modernization by fiscal year 2028.

- **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).[10] 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.[11]

  In addition, 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 IRS was experiencing shortages of staff with the skills to support key tax processing systems that used legacy programming languages.[12] 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.

  Further, having a shortage of personnel with necessary expertise can lead to delays in modernizing legacy systems. As we reported in February 2022, OPM's legacy financial system, Trust Funds Federal Financial System, was outdated and consisted of unsupported software. In fiscal year 2017, OPM created the Trust Funds Modernization Program to replace the legacy system. However, OPM had to extend the planned completion date of two project milestones

[10]COBOL, which was introduced in 1959, became the first widely used, high-level programming language for business applications.

[11]GAO-16-468.

[12]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).

by one year. OPM attributed the delay to a variety of reasons, including insufficient staff expertise regarding the legacy system.[13]

- **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. 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.

  For example, as we reported in October 2022, the Department of Education's Next Gen program was to develop and implement modernized technology, processes, and operations to improve its customer experiences and outcomes, across the entire student aid lifecycle.[14] In 2021, Education spent about $1.3 billion to maintain its current operating environment. However, the Next Gen program experienced several schedule delays that affected the agency's ability to retire two legacy systems. Maintaining one of these legacy systems longer than originally planned introduced more risk and would cost at least $26.5 million.

As we reported in June 2019, agencies cited several factors they consider 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 may prioritize the modernization of legacy systems that have security vulnerabilities or software that is unsupported by the vendor.[15] 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

[13]GAO, *Information Technology: OPM Needs to Adopt Key Practices in Modernizing Legacy Financial System,* GAO-22-104206 (Washington, D.C.: Feb. 23, 2022).

[14]GAO, *Information Technology: Education Needs to Address Student Aid Modernization Weaknesses*, GAO-23-105333 (Washington, D.C.: Oct. 20, 2022).

[15]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.[16]

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.[17] 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.** 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 can consider the costs of maintaining a legacy system versus modernizing the system. For example, according to the Department of Veterans Affairs, 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 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

[16]See Department of Energy, Brookhaven National Laboratory, *Computer Security – Indirect Vulnerabilities and Threat Vectors (Air-Gap In-depth)*, BNL-114524-2017-CP (paper presented by Michael DePhillips at the International Conference on Physical Protection of Nuclear Material and Nuclear Facilities Conference, Vienna, Austria: November 2017).

[17]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 can 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 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.

Executive Branch and Congress Have Made Efforts to Modernize Federal IT

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

- **National Cybersecurity Strategy.** In March 2023, the President released a strategy to elevate the cybersecurity posture of the federal government.[18] The strategy indicated that the Office of Management and Budget (OMB) would lead development of a multi-year plan to accelerate technology modernization. The plan would prioritize federal efforts on eliminating legacy systems that are costly to maintain and difficult to defend against sophisticated cyber threats. Specifically, the plan is to identify milestones to remove all legacy systems incapable of implementing the zero trust architecture strategy within a decade, or otherwise mitigate risks to those that cannot be replaced in that timeframe.[19]
- **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.[20] 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

[18]The White House, *National Cybersecurity Strategy*, (Washington, D.C.: Mar. 1, 2023).

[19]Zero trust architecture is a cybersecurity approach that works on the "never trust, always verify" principle. It is intended to address the rapidly evolving security risks faced by IT systems worldwide. These risks include insider threats from employees who either deliberately or unintentionally create a security breach and new, more sophisticated and persistent threats from around the globe. For more information, see GAO, *Science & Tech Spotlight: Zero Trust Architecture,* GAO-23-106065 (Washington, D.C.: Nov. 18, 2022).

[20]Office of Management and Budget, *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.

include legacy systems), assess them for security risks, and remediate any weaknesses identified, including those associated with obsolete or unsupported technology.[21]

- **Enactment of provisions commonly referred to as the Modernizing Government Technology (MGT) Act.** 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.[22] The law also created the Technology Modernization Fund, from which agencies can obtain funds 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.[23] 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 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 the General Services Administration; (3) a member of DHS's National

[21]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.

[22]The MGT Act commonly refers to technology modernization provisions in the National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Div. A, Title X, Subtitle G, 131 Stat. 1283, 1586-94 (2017).

[23]Office of Management and Budget, *Implementation of the Modernizing Government Technology Act*, M-18-12 (Washington, D.C.: Feb. 27, 2018).

Protection and Program Directorate;[24] and (4) four federal employees with technical expertise in IT development, financial management, cybersecurity and privacy, and acquisition, appointed by the Director of OMB.[25]

Congress initially appropriated $175 million in no-year funding to the Technology Modernization Fund through the annual appropriations process. 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.[26] In May 2021, OMB provided updated guidance to agencies regarding this $1 billion, which (1) prioritized projects that cut across agencies and address immediate cybersecurity gaps, and (2) allowed agencies to apply for a partial or minimal reimbursement of the funds provided.

According to OMB's website for the Technology Modernization Fund, the Technology Modernization Board had approved 40 projects across 24 federal agencies, totaling about $713 million, as of May 2023.[27] For example, the board approved about $13.9 million for the Department of Housing and Urban Development (HUD) to modernize a mainframe and five COBOL-based applications that were expensive to maintain. According to OMB's website, the investment began in August 2018 and was closed out in August 2022, with no reported cost overruns and projected savings of about $8 million annually. According to HUD, securing these funds served as a catalyst inside the department and led to gathering strong support for this project.

[24]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.

[25]As of May 2023, these four employees were the Federal Deposit Insurance Corporation's CIO, Chief Privacy Officer, and Director of the Division of Information Technology; National Archives and Records Administration's CIO; National-Geospatial Intelligence Agency's Chief Technology Officer; and United States Digital Service's Administrator.

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

[27]The MGT Act requires the Director of OMB to issue guidance on the administration of the fund and report the status of the awarded projects on a public website. OMB provides information on the status of awarded projects on the Technology Modernization Fund's website at https://tmf.cio.gov/.

Without these funds, according to HUD, it would not have been able to pursue the project for several years.

However, we reported in December 2021 that, for numerous Technology Modernization Fund projects, agencies had yet to realize any cost savings, narrowed their respective projects' scopes resulting in reduced award amounts, and continued to use unreliable cost estimates.[28] We stated that, given the significant expansion in available funds, it was increasingly important for OMB and the General Services Administration to implement our prior recommendations from December 2019. This included developing and implementing a plan to fully recover operating expenses with fee collection and developing detailed cost estimating guidance.[29]

Agencies With the 10 Most Critical Federal Legacy Systems Made Progress Developing Modernization Plans, but Work Remains

Of 65 critical federal legacy systems that agencies identified for our June 2019 report, we determined the 10 that were most in need of modernization.[30] 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.[31] Several of the systems used

[28]GAO, *Technology Modernization Fund: Implementation of Recommendations Can Improve Fee Collection and Proposal Cost Estimates,* GAO-22-105117 (Washington, D.C.: Dec. 10, 2021).

[29]As described in the report, the Technology Modernization Fund received a significant expansion in March 2021 when the American Rescue Plan Act of 2021, Pub. L. No. 117-2, Title IV, § 4011, 135 Stat. 4, 80 (2021), appropriated an additional $1 billion to the fund. Prior to that time, the fund had received a total of $175 million through the annual appropriations process.

[30]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. We then selected the 10 systems with the highest scores as the most critical legacy systems in need of modernization.

[31]The Social Security Administration was unable to isolate the costs for just System 10 and, as a result, this number includes the cost of operating some of the administration's other mainframe systems.

older languages, such as COBOL and assembly language code.[32] 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.[33]

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. 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 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 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.)

[32]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.

[33]GAO-18-298.

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-23-106821

Legend:

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.

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[34] 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, two had documented modernization plans that addressed each of the three key elements, as of June 2019—the Departments of Defense and Interior. However, the other eight agencies lacked complete plans for modernizing the systems. Specifically, three agencies did not have documented modernization plans for their critical legacy systems—Education, HHS, and Transportation. The other five agencies—DHS, Treasury, OPM, Small Business Administration, and Social Security Administration—had modernization plans, however the plans did not fully address one or more of the three key elements.

The agencies provided a variety of explanations for the missing modernization plans. For example, according to Transportation, it did not have a documented modernization plan because it had solicited information from industry to determine whether the agency's ideas for modernization were feasible. 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.

In June 2019, we issued a "limited official use only" report that had 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. The eight agencies to which we made recommendations agreed with our findings and recommendations.

[34]General Services Administration, 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); 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).

Six of those eight agencies addressed our recommendations to identify and develop complete modernization plans for their respective legacy systems—Education, HHS, DHS, Treasury, Small Business Administration, and Social Security Administration. However, as of May 2023, two of the eight agencies have yet to fully implement the recommendations—Transportation and OPM.

Table 2 compares the extent to which agencies had documented modernization plans for their critical systems that included the three key elements, as of June 2019 and May 2023, respectively. (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 and May 2023

Agency	System name[a]	Had modernization plan with key elements, as of June 2019?[b]	Has addressed incomplete elements of modernization plan, as of May 2023?[b]
Department of Defense	System 1	Yes. Agency included all elements in its modernization plan.	Not applicable.
Department of Education	System 2	No. Agency did not have a documented modernization plan.	Yes. Agency included all elements in its modernization plan.
Department of Health and Human Services	System 3	No. Agency did not have a documented modernization plan.	Yes. Agency included all elements in its modernization plan.
Department of Homeland Security	System 4	Partial. Agency had a modernization plan but it did not include milestones or the disposition of the legacy system.	Yes. Agency included all elements in its modernization plan.
Department of the Interior	System 5	Yes. Agency included all elements in its modernization plan.	Not applicable.
Department of the Treasury	System 6	Partial. Agency had a modernization plan but it did not fully include milestones and it did not include the disposition of the legacy system.	Yes. Agency included all elements in its modernization plan.
Department of Transportation	System 7	No. Agency did not have a documented modernization plan.	No. In April 2022, agency officials informed us that they expected to go live with the modernized system in the fall of 2022; however, as of May 2023, we have not received documented plans for this modernization effort.
Office of Personnel Management	System 8	Partial. Agency had a modernization plan but it did not fully include milestones or work necessary, and it did not include the disposition of the legacy system.	No. As of May 2023, we have not received evidence that the agency has developed a comprehensive modernization plan for this system.
Small Business Administration	System 9	Partial. Agency had a modernization plan but it did not include the work necessary.	Yes. Agency included all elements in its modernization plan.
Social Security Administration	System 10	Partial. Agency had a modernization plan but it did not fully include milestones or work necessary, and it did not include the disposition of the legacy system.	Yes. Agency included all elements in its modernization plan.

Source: GAO analysis of agency modernization plans. | GAO-23-106821

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

[b]The key elements of a legacy system modernization plan included: (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.

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 their most critical legacy systems. In addition, Congress provided 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 remaining agencies establish complete plans that include milestones, describe the work necessary to modernize the system, and detail the disposition of the legacy system, the agencies' efforts will have an increased likelihood of cost overruns, schedule delays, and overall project failure. Project failure would be particularly detrimental for these critical federal legacy systems. In addition to wasted resources, it would prolong the lifespan of increasingly vulnerable and obsolete systems.

In May 2016, we reported that 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.[35] OMB staff from the Office of E-Government and Information Technology, stated that OMB created draft guidance that would require agencies to identify and prioritize legacy information systems that were in need of replacement or modernization. Specifically, the guidance was to develop criteria through which agencies could identify the highest priority legacy systems, evaluate and prioritize their portfolio of existing IT systems, and develop modernization plans that would guide agencies' efforts to streamline and improve their IT systems. The draft guidance included time frames for the efforts regarding developing criteria, identifying and prioritizing systems, and planning for modernization.

However, OMB did not commit to a firm time frame for when it would issue the policy. Accordingly, we recommended that OMB commit to a firm date by which its draft guidance on legacy systems would be issued, and subsequently direct agencies to identify legacy systems needing to be replaced or modernized.

OMB agreed with our recommendation but has not yet implemented it. In April 2021, OMB staff had stated that agencies were directed to manage

[35]GAO-16-468.

the risk to High Value Assets associated with legacy systems in OMB's December 2018 guidance.[36] 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. In December 2022, OMB stated that it planned to compare the recommendation with recent actions, guidance, and policy memoranda issued since the recommendation was made, to determine if an update to OMB's response was appropriate.

In summary, we reiterate the importance of our 2016 recommendation for OMB to finalize guidance directing agencies to identify legacy systems needing to be replaced or modernized. Taking such action could provide greater assurance that the risks of continuing to operate legacy systems are being addressed government-wide.

Further, 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 overall project failure. Such outcomes would be particularly detrimental because of the importance of these systems to agency missions. Although the majority of agencies we made recommendations to have developed complete modernization plans for their respective legacy systems, two agencies have not.

Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

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

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 Jeanne Sung (Assistant Director), Paige Teigen (Analyst-in-Charge), Donna Epler, Kim LaMore, and Jessica Steele.