



Report to the Committee on Oversight
and Government Reform
House of Representatives

July 2025

INFORMATION TECHNOLOGY

Agencies Need to Plan for Modernizing Critical Decades-Old Legacy Systems

GAO Highlights

Highlights of [GAO-25-107795](#), a report to the Committee on Oversight and Government Reform, 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. This includes maintaining legacy systems that can pose significant challenges, such as increased costs and cybersecurity vulnerabilities.

In June 2019, GAO identified 10 critical federal legacy IT systems that were most in need of modernization. As of February 2025, agencies have completed three of the 10 modernizations. Of the seven remaining modernizations, agencies planned to complete four in the next few years, two in 5 or more years, and one does not yet have a planned completion date established.

GAO was asked to conduct an updated review of federal agencies' current legacy systems. GAO's specific objective for this report was to identify the federal legacy systems most in need of modernization and evaluate plans for modernizing them.

To do so, GAO asked the 24 Chief Financial Officers Act agencies to provide their three legacy IT systems most in need of modernization and obtained a total of 69 systems. GAO scored these systems based on 16 system attributes and associated point values, such as age, vendor support, use of legacy programming languages, degree of cybersecurity risk, and operating costs. GAO ranked the systems based on their scores and selected those with the highest scores.

View [GAO-25-107795](#). For more information, contact Kevin Walsh at walshk@gao.gov.

July 2025

INFORMATION TECHNOLOGY

Agencies Need to Plan for Modernizing Critical Decades-Old Legacy Systems

What GAO Found

As determined by GAO's review of 69 federal legacy IT systems, the 11 legacy systems most in need of modernization are maintained by 10 federal agencies. These agencies' missions are essential to government operations such as health care, critical infrastructure, tax processing, and national security, and these legacy systems provide vital support to the agencies' missions.

GAO identified 11 legacy IT systems as most in need of modernization (see table 1). Eight of the 11 systems use outdated languages, four have unsupported hardware or software, and seven are operating with known cybersecurity vulnerabilities. For example, both of the Department of the Treasury's selected systems run on Common Business Oriented Language (COBOL) and Assembly Language Code—programming languages that have a dwindling number of people available with the skills needed to support them. In addition, the Environmental Protection Agency's system contains obsolete hardware that is not supported by manufacturers and has known cybersecurity vulnerabilities that cannot be remediated without modernization.

Table 1: The 11 Most Critical Federal Legacy IT Systems in Need of Modernization

Agency	System name ^a	Age of system	Hardware/software/operating system(s) supported	Legacy programming language(s) used
Department of Agriculture	System 1	41	Yes	Yes
Department of Commerce	System 2 ^b	30	Unknown ^c	No
Department of Defense	System 3 ^b	60	Yes	Yes
Department of Energy	System 4	25	Yes	Yes
Department of Health and Human Services	System 5 ^b	55	Yes	Yes
Department of Homeland Security	System 6	30	No	No
Department of the Interior	System 7 ^b	23	No	Yes
Department of Transportation	System 8	31	No	Yes
Department of the Treasury	System 9	59	Yes	Yes
	System 10	51	Yes	Yes
Environmental Protection Agency	System 11	51	No	No

Legend: green shade = favorable characteristic, red shade = unfavorable characteristic, and grey shade = unknown characteristic.

Source: GAO analysis of agency data. | GAO-25-107795

^aDue to sensitivity concerns, GAO substituted a numeric identifier for the system names.

^bThis system was previously identified in GAO's 2019 review as one of the federal government's legacy systems in need of modernization (see [GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU).

^cCommerce officials stated that the Census Bureau, National Institute of Standards and Technology, and National Oceanic and Atmospheric Administration manage their own hardware for System 2, and that hardware information was unknown for the Census Bureau.

For the resulting 11 systems, GAO compared the agencies' modernization plans against leading practices. According to government and industry best practices, agencies' documented plans for system modernization should include, at a minimum, (1) milestones, (2) a description of the work, and (3) details regarding disposition of the legacy system. GAO then analyzed agencies' documented modernization plans for the selected systems to determine whether the plans included these elements.

This is a public version of a sensitive report that is being issued concurrently. Sensitive information, such as system names and identifiers, has been omitted.

What GAO Recommends

GAO is making one matter for congressional consideration: Congress should consider requiring major federal agencies to develop modernization plans for their legacy systems that have been identified as most in need of modernization.

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

Three agencies agreed with GAO's recommendations and three agencies neither agreed nor disagreed. In addition, one agency disagreed with its recommendation and GAO revised it to reflect updated information.

As shown in table 2, agencies had developed modernization plans for nine of the 11 systems. Of the nine systems with plans, three included all three elements of a plan (at Homeland Security, the Interior, and the Environmental Protection Agency), and six did not include all elements of a plan (at Agriculture, Commerce, Health and Human Services, Transportation, and the Treasury). The two systems without plans belonged to Defense and Energy.

Table 2: Extent to Which Agencies' Legacy IT Systems Documented Modernization Plans Included Key Elements				
Agency	System name ^a	Includes milestones to complete the modernization	Describes the work necessary to modernize the system	Summarizes planned disposition of legacy system
Department of Agriculture	System 1	Yes – planned completion 2031	No	Partial
Department of Commerce	System 2	Partial	Partial	Partial
Department of Defense	System 3	No modernization plan		
Department of Energy	System 4	No modernization plan		
Department of Health and Human Services	System 5	Partial	Partial	Partial
Department of Homeland Security	System 6	Yes – planned completion September 2026	Yes	Yes
Department of the Interior	System 7	Yes – planned completion August 2027	Yes	Yes
Department of Transportation	System 8	Yes – planned completion 2030	No	Partial
Department of the Treasury	System 9	Partial	Partial	No
	System 10	Partial	Yes	Partial
Environmental Protection Agency	System 11	Yes – planned completion December 2028	Yes	Yes

Source: GAO analysis of agency modernization plans. | GAO-25-107795
Note: Agencies received a "partial" if the element was completed for a portion of the modernization.
^aDue to sensitivity concerns, GAO substituted a numeric identifier for the system names.

The incomplete modernization plans are especially concerning for seven of the systems because they reportedly have modernizations already underway. These seven systems belonged to six agencies: Agriculture, Commerce, Defense, Health and Human Services, Transportation, and the Treasury.

Until agencies fully document modernization plans for critical legacy IT systems, their modernization initiatives will have an increased likelihood of cost overruns, schedule delays, and overall project failure. Project failure would be particularly detrimental not only because of wasted resources, but also because it would prolong the lifespan of increasingly vulnerable and obsolete systems. This could expose agencies and system clients to security threats and potentially significant performance issues. Further, there are likely more legacy systems needing attention beyond what is highlighted in this report.

GAO recommended nearly a decade ago, and has since made it a priority recommendation, that OMB direct agencies to identify legacy systems and/or investments needing to be modernized. OMB has not yet taken action. Given OMB's lack of action, Congress requiring federal agencies to develop modernization plans for critical legacy systems can expedite agencies' efforts.

Contents

Letter		1
	Background	4
	GAO Identified 11 Critical Legacy Systems; Most Agencies Lacked Complete Modernization Plans	18
	Conclusions	25
	Matter for Congressional Consideration	25
	Recommendations for Executive Action	25
	Agency Comments and Our Evaluation	26
Appendix I	Objective, Scope, and Methodology	29
Appendix II	Status of Legacy IT Systems Identified in 2019 as Most in Need of Modernization	35
Appendix III	Legacy IT Systems Identified in 2025 as Most in Need of Modernization	39
Appendix IV	Profiles of the 11 Legacy IT Systems Most in Need of Modernization	44
Appendix V	Comments from the Department of Defense	65
Appendix VI	Comments from the Department of Energy	66
Appendix VII	Comments from the Department of Health and Human Services	68
Appendix VIII	Comments from the Social Security Administration	70

Appendix IX	GAO Contact and Staff Acknowledgments	71
-------------	---------------------------------------	----

Tables

Table 1: The Most Critical Federal Legacy Systems in Need of Modernization That GAO Identified in 2019	15
Table 2: Agency-Reported Status of 10 Critical Legacy IT Systems from 2019, as of February 2025	16
Table 3: Modernization Status of Legacy Systems from GAO-19-471, as of February 2025	17
Table 4: The 11 Most Critical Federal Legacy IT Systems in Need of Modernization	19
Table 5: Extent to Which Agencies' Legacy IT Systems Documented Modernization Plans Included Key Elements	23
Table 6: System Attributes and Associated Point Values Used to Rank Legacy Systems	31
Table 7: The 11 Selected Federal Legacy IT Systems Most in Need of Modernization	33
Table 8: Agency-Reported Status of Legacy IT Systems Identified in 2019 as Most in Need of Modernization, as of February 2025	35
Table 9: Legacy IT Systems Identified in 2025 as Most in Need of Modernization and Select Attributes	39
Table 10: Crosswalk of System Identifiers for the 17 Legacy Systems Reported in Both 2019 and 2025	42

Figures

Figure 1: Planned IT Spending, as Reported on the IT Dashboard for Fiscal Year 2025, in millions of dollars	5
Figure 2: Photograph of a Dam	56

Abbreviations

CIO	Chief Information Officer
COBOL	Common Business Oriented Language
DHS	Department of Homeland Security
DOD	Department of Defense
EHR	electronic health record
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
HHS	Department of Health and Human Services
IHS	Indian Health Service
IRS	Internal Revenue Service
MGT	Modernizing Government Technology
NFC	National Finance Center
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OPM	Office of Personnel Management

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



July 17, 2025

The Honorable James Comer
Chairman
The Honorable Robert Garcia
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

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.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 vendors that were no longer providing support for hardware or software.² Similarly, 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 We noted that, as they age, legacy systems can become more expensive to maintain, more exposed to cybersecurity risks, and less effective in accomplishing their intended purpose. We also identified 10 critical federal legacy IT systems that were most in need of modernization and found that eight of those 10 systems did not have documented plans or had incomplete plans for modernizing their systems.

Subsequently, you asked us to conduct an updated review of federal agencies' current legacy systems. Our specific objective was to identify

¹The provisions commonly referred to as the Modernizing Government Technology Act (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, 131 Stat. 1283, 1586-87 (2017), 40 U.S.C. § 11301 note.

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

³GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, [GAO-19-471](#) (Washington, D.C.: June 11, 2019) and concurrent limited official use only report GAO-19-351SU.

the federal legacy IT systems most in need of modernization and evaluate plans for modernizing them.

This report presents a public version of a “limited official use only” (LOUO) report that we are also issuing today.⁴ The LOUO report includes eight recommendations that we made to seven agencies to identify and document modernization plans for particular legacy systems, including milestones, a description of the work necessary, and details on the disposition of the legacy system.⁵ In this public version of the report, we have omitted sensitive information regarding particular legacy systems, including the systems’ names and other information that would identify the systems. Although the information provided in this report is more limited, this report addresses the same objectives as the LOUO report and is based on the same audit methodology.

To identify the legacy IT systems most in need of modernization, we asked each of the 24 Chief Financial Officers Act agencies to provide their three legacy IT systems most in need of modernization.⁶ This resulted in a list of 69 systems.

To develop a set of attributes for determining systems’ obsolescence and their need for modernization, we considered the attributes used in our 2019 review of federal legacy systems and relevant federal guidance that had been issued since then.⁷ We also consulted with our system development and cybersecurity experts. In addition to using the system attributes from our 2019 review (such as a system’s age, hardware age, operating and labor costs, and vendor warranty and support status), we

⁴GAO, *Information Technology: Agencies Need to Plan for Modernizing Critical Decades-Old Legacy Systems*, GAO-25-107289SU (Washington, D.C.: July 17, 2025).

⁵We made recommendations to the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Transportation, and the Treasury.

⁶The 24 major federal agencies covered by the Chief Financial Officers Act of 1990 are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development. 31 U.S.C. § 901(b).

⁷[GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU.

included two additional attributes due to an increased importance on cybersecurity issues in modernizing the federal government's legacy IT:

- Whether the system was capable of implementing the zero trust strategy.⁸
- Whether the system had known cybersecurity vulnerabilities that could only be remediated with modernization, and if so, whether the agency was mitigating the risks.

We assigned point values to each system based on their agency-reported attributes. We then totaled the assigned point values for each legacy system and ranked the results from highest to lowest number of assigned points. We intended to select approximately 10 systems that were ranked highest among the 69 systems. Accounting for tied scores, we identified 11 systems with the highest scores as those legacy systems most in need of modernization.⁹ However, due to sensitivity concerns, in this report we substituted a numeric identifier for the system names and are not providing detailed descriptions.

To evaluate agencies' plans for modernizing the 11 legacy systems most in need of modernization, we requested that the relevant agencies provide their documented plans for modernizing the selected systems. We determined that the criteria used in our 2019 review, which was based on government and industry best practices related to the modernization of legacy systems, were still current and relevant. According to these sources, agencies' documented plans for system modernization should include, at a minimum, (1) milestones to complete the modernization, (2) a description of the work necessary to modernize the system, and (3) details regarding the disposition of the legacy

⁸Zero trust architecture is a cybersecurity approach that works on the "never trust, always verify" principle and is intended to address rapidly evolving security risks. In January 2022, the Office of Management and Budget published a strategy aimed at moving the U.S. government toward zero trust cybersecurity principles. Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, M-22-09 (Washington, D.C.: Jan. 26, 2022).

⁹The 10 agencies with the 11 legacy IT systems most in need of modernization are the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Homeland Security, the Interior, Transportation, and the Treasury; and the Environmental Protection Agency.

system.¹⁰ We then analyzed agencies' documented modernization plans for the selected systems to determine whether the plans included these elements. We supplemented our work with interviews of officials in the agencies' offices of the Chief Information Officer (CIO) and program offices for the selected legacy systems. For more information on our objective, scope, and methodology, see appendix I.

We conducted this performance audit from January 2024 to July 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

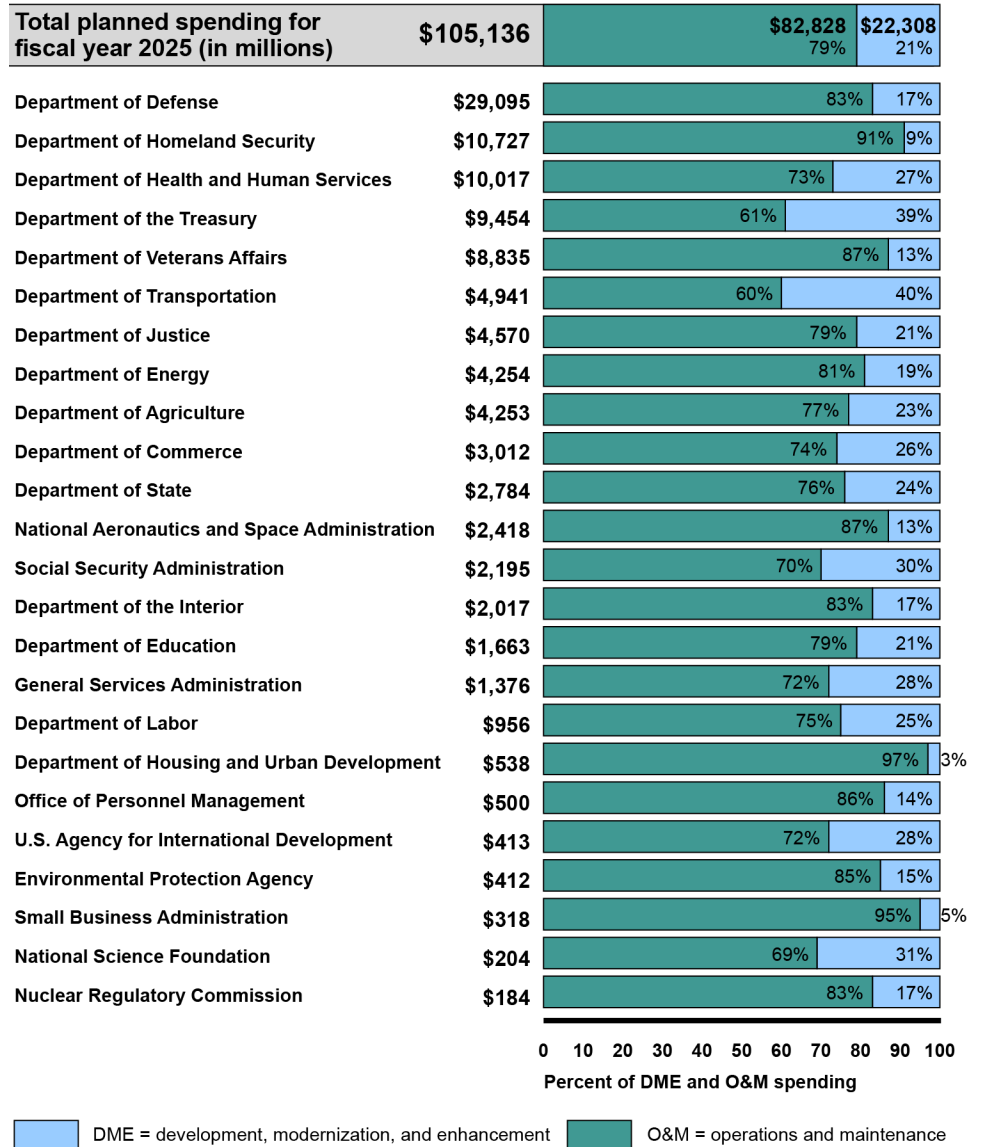
Background

While the extent of legacy IT in the federal government is unknown, the government spends a large portion of its IT spending on operating and maintaining existing systems or capabilities. For example, as shown in figure 1, about \$83 billion (79 percent) in planned total IT spending for fiscal year 2025 was intended for operations and maintenance, according to the federal IT dashboard, for the 24 Chief Financial Officers Act agencies.¹¹ The figure also shows how agencies can vary in their percentage of operations and maintenance spending. However, it is uncertain how much of the operations and maintenance is spent on legacy technology because the Office of Management and Budget (OMB) does not require agencies to include information on whether their investments are considered legacy IT.

¹⁰General Services Administration, Unified Shared Services Management, *Modernization and Migration Management (M3) Playbook* (Aug. 3, 2016); *M3 Playbook Guidance* (Aug. 3, 2016); American Technology Council, *Report to the President on Federal IT Modernization* (Dec. 13, 2017); Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018); 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); and American Council for Technology-Industry Advisory Council, *Legacy System Modernization: Addressing Challenges on the Path to Success* (Fairfax, VA: Oct. 7, 2016).

¹¹The other 21 percent of funds were for the development, modernization, and enhancement of new systems or capabilities.

Figure 1: Planned IT Spending, as Reported on the IT Dashboard for Fiscal Year 2025, in millions of dollars



Source: GAO analysis of IT Dashboard data. | GAO-25-107795

Agencies have reported a variety of ways in which they identify their legacy IT systems and determine the need to prioritize those systems for modernization, replacement, or retirement. For example, some agencies reportedly tracked information on their legacy systems (e.g., system age, decommission date, use of archaic programming languages, security

posture, architecture, and end-of-life technology) in a centralized repository and updated the system information on a recurring basis.

In addition, some agencies said they had established a definition for legacy systems or were working on developing a definition. For example, National Aeronautics and Space Administration officials stated that the agency defines legacy IT systems in the context of criticality to the agency's mission, technological obsolescence, ongoing operations and maintenance costs, and extent to which the system can meet IT security standards. The Department of Defense (DOD) defines a system as legacy when it is scheduled to be retired in the next 3 years.¹² In contrast, some agencies said they did not have a standard definition or a department-wide approach to managing their legacy systems, and instead relied on their components to identify their legacy systems.

Considerations and Consequences of Legacy IT

According to agencies, they consider several factors prior to deciding whether to modernize a legacy system 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 cybersecurity vulnerabilities or software that is unsupported by the vendor.¹³
- **Criticality.** Agencies consider how critical the system is to their missions. Several agencies stated that they would consider how essential a legacy system is to their agencies' missions before deciding to modernize it.
- **Costs.** Agencies consider the costs of maintaining a legacy system and modernizing the system.

¹²In January 2024, DOD's Office of Inspector General recommended that the department reconsider the definition of a legacy system to ensure that it encompasses a system that is outdated and needs to be modernized or retired, regardless of when DOD chooses to retire it. See U.S. Department of Defense Inspector General, *(U) Audit of the DoD's Plans to Address Longstanding Issues with Outdated Financial Management Systems*, DODIG-2024-047 (Alexandria, VA: Jan. 19, 2024).

¹³When 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.

-
- **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.

The consequences of not updating legacy systems have contributed to, among other things, cybersecurity risks, unmet mission needs, a shortage of staff with specialized skills, and increased costs.

- **Cybersecurity risks.** Legacy systems may operate with known cybersecurity vulnerabilities that are either technically difficult or prohibitively expensive to address. In some cases, vendors no longer provide support for hardware or software, creating cybersecurity vulnerabilities and additional costs.
- **Unmet mission needs.** Legacy systems may not be able to reliably meet mission needs because they are outdated or obsolete. Further, system outages potentially caused by hardware failure may disrupt an organization's operations. In addition, outdated systems can be more difficult to modify or upgrade for emerging mission needs.
- **Shortage of staff with specialized skills.** 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).¹⁴ Agencies have had difficulty finding employees with such knowledge and may have to pay a premium for specialized staff or contractors. In addition, having a shortage of expert personnel available to maintain a critical system creates significant risk to an agency's mission.
- **Increased costs.** The cost of operating and maintaining legacy systems increases over time. 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.

¹⁴COBOL, which was introduced in 1959, became the first widely used, high-level programming language for business applications.

Federal Agencies Have Been Challenged with Legacy IT Modernizations

Historically, the federal government has had difficulties acquiring, developing, and managing IT investments, including updating its legacy IT.¹⁵ 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. For example,

- We have previously designated the Department of Veterans Affairs health care as a high-risk area for the federal government, in part due to its IT challenges and implementation of the Electronic Health Record (EHR) Modernization program.¹⁶ In addition, we have reported on a number of initiatives the Department of Veterans Affairs has undertaken to improve interoperability (i.e., the ability to exchange and use electronic health information) and modernize EHRs across the department.¹⁷ These initiatives have included four efforts over two decades to modernize the Veterans Health Information Systems and Technology Architecture. The first three efforts reflect varying approaches that the department had taken since 2001 to achieve a modernized EHR system. However, these approaches were

¹⁵As 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, and in 2025 renamed it to “Improving IT Acquisitions and Management.” GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, [GAO-25-107743](#) (Washington, D.C.: Feb. 25, 2025).

¹⁶VA’s IT issues were highlighted in our 2015 high-risk report and subsequent high-risk reports. See 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).

¹⁷See, for example, GAO, *Electronic Health Records: VA Needs to Address Management Challenges with New System*, [GAO-23-106731](#) (Washington, D.C.: May 18, 2023); *Electronic Health Records: VA Needs to Address Data Management Challenges for New System*, [GAO-22-103718](#) (Washington, D.C.: Feb. 1, 2022); *Electronic Health Records: VA Has Made Progress in Preparing for New System, but Subsequent Test Findings Will Need to Be Addressed*, [GAO-21-224](#) (Washington, D.C.: Feb. 11, 2021); *Electronic Health Records: Ongoing Stakeholder Involvement Needed in the Department of Veterans Affairs’ Modernization Effort*, [GAO-20-473](#) (Washington, D.C.: June 5, 2020); *Electronic Health Records: VA Needs to Identify and Report System Costs*, [GAO-19-125](#) (Washington, D.C.: July 25, 2019).

abandoned due to concerns about project planning, high costs, and length of time to deliver capabilities.

In March 2025, we reported on the department's fourth effort—the EHR Modernization program—to replace its legacy EHR system with a modernized, commercial system.¹⁸ The department began this effort in 2017, first deployed the new system in October 2020, and followed up with further deployments to four additional sites in 2022. In April 2023, after deploying the new system to five of its medical centers, VA paused deployments due to feedback from veterans and clinicians that the new system was not meeting expectations. In March 2024, VA deployed the new EHR system at the Captain James A. Lovell Federal Health Care Center, and in December 2024, announced resumption of planned deployments to four facilities.

We noted that although user satisfaction had improved over the last 3 years, users at the five initial sites continued to be generally dissatisfied with the new system. To provide insights on system progress, VA had finalized baselines and targets for most of the identified relevant metrics. Finalizing the lone remaining metric's baseline and target can provide department leadership with important information of program performance. We made three new recommendations to the department, in addition to the 15 EHR recommendations previously made. As of April 2025, the department has fully implemented one, partially implemented one, and not yet implemented 16 recommendations.

- In September 2024, we reported that for several decades the Federal Aviation Administration (FAA) had experienced challenges with its aging air traffic control systems due to unavailability of parts, reduced technical expertise in outdated technologies, and growth in airspace demand.¹⁹ We found that 105 of 138 legacy air traffic control systems had been deemed unsustainable or potentially unsustainable—58 of which had critical operational impacts on the safety and efficiency of the national airspace.

We also reported that FAA had been slow to modernize some of the most critical and at-risk systems because it had not initiated investments for modernizing all the systems. Further, once modernizations were initiated, FAA can take years to establish a cost,

¹⁸GAO, *Electronic Health Records: VA Making Incremental Improvements in New System but Needs Updated Cost Estimate and Schedule*, [GAO-25-106874](#) (Washington, D.C.: Mar. 12, 2025).

¹⁹GAO, *Air Traffic Control: FAA Actions Are Urgently Needed to Modernize Aging Systems*, [GAO-24-107001](#) (Washington, D.C.: Sept. 23, 2024).

schedule, and performance baseline; and once planned, the investments can take an average of over 12 years to complete. We stated that a contributing factor to the lengthy implementation was that FAA did not always ensure that investments were organized into manageable segments, which is counter to OMB and FAA policies that require this approach.

We noted that until FAA takes urgent action to reduce the time frames to replace critical and at-risk air traffic control systems, it will continue to rely on a large percentage of unsustainable systems to perform critical functions for safe air travel. We made seven recommendations to FAA, one of which was to ensure that air traffic control modernization investments establish baselines in an expeditious manner. The department concurred with six of the recommendations and partially concurred with one. As of April 2025, it has fully implemented one, partially implemented one, and not yet implemented five recommendations.

- We and the Treasury's Office of Inspector General for Tax Administration have previously reported on the Internal Revenue Service's (IRS) reliance on IT that includes a significant amount of outdated legacy systems.²⁰ For example, Treasury's Inspector General for Tax Administration reported in August 2024 that IRS did not have any specific or long-term plans for 191 of 231 legacy systems that it had identified as of April 2020. Additionally, it reported that 105 of 107 legacy systems that had been identified for retirement (as of December 2023) did not have specific decommissioning plans.

Further, in January 2023, we reported that about 259 (33 percent) of the IRS's applications, 1,111,419 (23 percent) of the software instances in use, and 9,280 (8 percent) of hardware assets were considered legacy. This included applications ranging from 25 to 64 years in age, as well as software up to 15 versions behind the current version. IRS acknowledged that operating in this environment would continue to significantly contribute to security risks, unmet mission needs, staffing issues, and increased costs, among other challenges.

²⁰See for example, Treasury Inspector General for Tax Administration (TIGTA), *Legacy Systems Management Needs Improvement*, 2020-20-044 (Aug. 19, 2020); TIGTA, *The IRS Does Not Have Specific Plans to Replace and Decommission Legacy Systems*, 2024-200-038 (Aug. 7, 2024); GAO, *Information Technology: IRS Needs to Complete Planning and Improve Reporting for Its Modernization Programs*, [GAO-24-106566](#) (Washington, D.C.: Mar. 19, 2024); and GAO, *Information Technology: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements*, [GAO-23-104719](#) (Washington, D.C.: Jan. 12, 2023).

We also reported that IRS's system for individual tax data, the Individual Master File, needed to be modernized to help address business and technical challenges, such as the inability to get a real-time view of the taxpayer's account. We observed that continuing to rely on a critical system with software written in an archaic language requiring specialized skills would lead to mounting challenges. We made nine recommendations to IRS, six of which included establishing time frames to complete selected modernization plans for its legacy systems. IRS agreed with all nine recommendations, but as of April 2025, has not yet implemented them.

- In October 2022, we reported that the Department of Education's Office of Federal Student Aid spent about \$1.3 billion to maintain its legacy operating environment, though it had a number of shortcomings with that environment that adversely affected customers' experiences.²¹ The resulting effort to modernize these systems is called the Next Gen program and was intended to develop and implement modernized technology, processes, and operations to improve its customer experiences and outcomes, across the entire student aid lifecycle.

However, the program experienced several schedule delays that affected the agency's ability to retire two legacy systems. Among other things, officials attributed those delays to staffing limitations and excessive staffing workloads. Maintaining one of these legacy systems longer than originally planned introduced more risk to Education's Office of Federal Student Aid and was estimated to cost at least \$26.5 million. We made 14 recommendations to Education, including addressing weaknesses in cost, scheduling, and project management practices. The Office of Federal Student Aid, on behalf of Education, generally concurred with the recommendations, but as of April 2025, has not yet implemented any of them.

Executive and Legislative Efforts to Modernize Federal Legacy IT

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

- **National Cybersecurity Strategy.** In March 2023, the President released a strategy to elevate the cybersecurity posture of the federal government.²² The strategy indicated that OMB would lead development of a multi-year plan to accelerate technology modernization. The plan would prioritize federal efforts on eliminating

²¹GAO, *Information Technology: Education Needs to Address Student Aid Modernization Weaknesses*, [GAO-23-105333](#) (Washington, D.C.: Oct. 20, 2022).

²²The White House, *National Cybersecurity Strategy*, (Washington, D.C.: Mar. 1, 2023).

legacy systems that are costly to maintain and difficult to defend against sophisticated cyber threats. In addition, the plan was 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 time frame.²³

- **High Value Asset program.** In December 2018, OMB issued a memorandum that provided guidance regarding the establishment of the High Value Asset program.²⁴ 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.²⁵
- **Provisions commonly referred to as the Modernizing Government Technology (MGT) Act.** In December 2017, Congress 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. Known as the MGT Act, the law authorizes covered agencies to establish IT working capital funds for use in transitioning from legacy systems, as well as for addressing evolving threats to information security.²⁶ 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. Three months later, in February 2018, OMB issued guidance for agencies to implement the MGT

²³Zero trust architecture is a cybersecurity approach that works on the “never trust, always verify” principle and is intended to address rapidly evolving security risks. In January 2022, OMB published a strategy aimed at moving the U.S. government toward zero trust cybersecurity principles.

²⁴Office 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).

²⁵A high value asset is a designation for federal information or a federal information system that processes, stores, or transmits high value information, is considered vital to an agency fulfilling its primary mission, or serves a critical function in maintaining the security and resilience of the federal civilian enterprise.

²⁶The 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, § 1076, 131 Stat. 1283, 1586-87 (2017), 40 U.S.C. § 11301 note.

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

Act.²⁷ 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.

Congress initially appropriated \$175 million in no-year funding to the Technology Modernization Fund through the annual appropriations process. On March 11, 2021, Congress appropriated an additional \$1 billion to be available until September 30, 2025, to carry out the purposes of the fund.²⁸ 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 69 projects across 34 federal agencies, totaling over \$1 billion, as of April 2025.²⁹ However, we have previously reported that the Technology Modernization Fund projects have thus far achieved minimal cost savings.³⁰ For example, in December 2023, we reported that 24 of the projects that had been awarded funding from the Technology Modernization Fund at the time anticipated total cost savings of about \$756 million. However, we noted that only about \$14.8 million of the anticipated savings had thus far been realized (by eight projects).

As previously mentioned, in May 2016, we reported that federal legacy IT investments were becoming increasingly obsolete.³¹ For example, agencies had reported operating systems that used outdated languages and old parts, which were difficult to replace. Further, we noted that each of the 12 selected agencies had reported using unsupported operating

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

²⁸American Rescue Plan Act of 2021, Pub. L. No: 117-2, Title IV, § 4011, 135 Stat. 4, 80 (2021).

²⁹The MGT Act requires the Director of OMB to publicly issue updates 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/>.

³⁰GAO, *Technology Modernization Fund: Although Planned Amounts Are Substantial, Projects Have Thus Far Achieved Minimal Savings*, [GAO-24-106575](#) (Washington, D.C.: Dec. 12, 2023); and *Technology Modernization Fund: Implementation of Recommendations Can Improve Fee Collection and Proposal Cost Estimates*, [GAO-22-105117](#) (Washington, D.C.: Dec. 10, 2021).

³¹[GAO-16-468](#).

systems and components, which could create security vulnerabilities and additional costs.³² At the time, five of the selected agencies reported using 1980s and 1990s Microsoft operating systems that stopped being supported by the vendor more than a decade before. We concluded that agencies were maintaining obsolete investments, in part, because they were not required to identify, evaluate, and prioritize investments to determine whether the investments should be kept as-is, modernized, replaced, or retired. We pointed out that, at the time, OMB had created draft guidance that would require agencies to do so, but OMB had not committed to a firm time frame for when the guidance would be issued.

As such, we made 16 recommendations to OMB and the selected federal agencies. The agencies agreed with the recommendations or had no comment. However, as of April 2025, three recommendations had not been implemented. In particular, OMB has not finalized and issued its draft guidance on legacy systems. Given OMB's lack of action, in May 2023, we sent a letter to the Director of OMB that detailed this recommendation as one of 40 open recommendations that we deemed the highest priority for OMB implementation.³³

In February 2024, OMB stated that it did not plan to issue any additional guidance on legacy systems, and in March 2024, OMB stated that it believed it had met the intent of the recommendation and considered it closed. We disagreed and believed that until OMB issues guidance on identifying and modernizing legacy systems, the federal government runs the risk of continuing to maintain investments that have outlived their effectiveness and are consuming resources that outweigh their benefits. In January 2025, OMB indicated it had actions planned to address this recommendation that were not yet underway. However, OMB did not provide additional information, such as what specific actions were planned and associated time frames.

In June 2019, we noted that 24 federal agencies had identified 65 legacy systems that were most in need of modernization, and we identified 10 of

³²The agencies in our 2016 review were the 12 that reported the highest planned IT spending for fiscal year 2015. These agencies were the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Homeland Security, Justice, State, Transportation, the Treasury, and Veterans Affairs; and the Social Security Administration.

³³GAO, *Priority Open Recommendations: Office of Management and Budget*, [GAO-23-106298](#) (Washington, D.C.: May 23, 2023).

those as the most critical systems in need of modernization.³⁴ According to the agencies, at the time, the 10 most critical legacy systems ranged from about 8 to 51 years old and, collectively, cost approximately \$337 million annually to operate and maintain.³⁵ Table 1 provides a generalized list of each of the 10 selected systems 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.)

Table 1: The Most Critical Federal Legacy Systems in Need of Modernization That GAO Identified in 2019

Agency	2019 system name ^a	Agency-reported system attributes, as of 2019			
		Age of system, in years	Age of oldest hardware, in years	System criticality (according to agency)	Security risk (according to agency)
Department of Defense	2019 System 1	14	3	Moderately high	Moderate
Department of Education	2019 System 2	46	3	High	High
Department of Health and Human Services	2019 System 3	50	Unknown ^b	High	High
Department of Homeland Security	2019 System 4	8 – 11 ^c	11	High	High
Department of the Interior	2019 System 5	18	18	High	Moderately high
Department of Transportation	2019 System 7	35	7	High	Moderately high
Department of the Treasury	2019 System 6	51	4	High	Moderately low
Office of Personnel Management	2019 System 8	34	14	High	Moderately low
Small Business Administration	2019 System 9	17	10	High	Moderately high
Social Security Administration	2019 System 10	45	5	High	Moderate

Source: [GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU. | GAO-25-107795

^aDue to sensitivity concerns, we substituted a numeric identifier for the system names.

^bThe agency stated in 2019 that the system’s hardware had various refresh dates and was not able to identify the oldest hardware.

^cThe agency stated in 2019 that the majority of the network’s hardware was purchased between 2008 and 2011.

Several of the systems used older languages, such as COBOL and assembly language code. The use of these 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

³⁴[GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU.

³⁵The Social Security Administration was unable to isolate the costs for its system and, as a result, this number includes the cost of operating some of the administration’s other mainframe systems.

these legacy systems were operating with known security vulnerabilities and unsupported hardware and software.

We reported that a majority of the agencies that were responsible for the 10 most critical legacy systems lacked complete modernization plans. We issued a “limited official use only” report concurrently with the June 2019 report that had eight recommendations to eight federal agencies to identify and document modernization plans for their respective legacy systems.³⁶ As of April 2024, all eight agencies had implemented their recommendations to develop modernization plans.

Status of 2019 Federal Legacy Systems in Need of Modernization

Agencies have completed modernizations for three of the 10 most critical legacy systems we identified in 2019, but as of February 2025, have not completed seven of 10 modernizations. In general, the agencies expect the ongoing modernizations will be completed within the next few years, the longest of which was expected to take 10 years. One agency did not yet have a planned completion date for its system modernization. Table 2 summarizes the modernization status of the 10 systems, as of February 2025. (Due to sensitivity concerns, we substituted a numeric identifier for the system names.)

Table 2: Agency-Reported Status of 10 Critical Legacy IT Systems from 2019, as of February 2025

Agency	2019 system name ^a	Agency-reported modernization status	Agency-reported expected completion of modernization, as of February 2025
Department of Defense	2019 System 1	Completed in fiscal year 2020	
Department of Education	2019 System 2 ^b	In progress	September 2025
Department of Health and Human Services	2019 System 3 ^c	In progress	End of fiscal year 2035
Department of Homeland Security	2019 System 4	In progress	Not yet established
Department of the Interior	2019 System 5 ^c	In progress	August 2027
Department of Transportation	2019 System 7	In progress	2026
Department of the Treasury	2019 System 6 ^b	In progress	2028
Office of Personnel Management	2019 System 8	Completed in September 2024	
Small Business Administration	2019 System 9	Completed in April 2023	
Social Security Administration	2019 System 10 ^b	In progress	2 or more years from February 2025

Legend: green shade = modernization completed.

Source: GAO analysis of agency-reported information. | GAO-25-107795

^aDue to sensitivity concerns, we substituted a numeric identifier for the system names.

³⁶GAO-19-351SU.

^bThis system was also identified in 2025 as one of the federal government's 69 legacy IT systems in need of modernization.

^cThis system was also identified in 2025 as one of the federal government's 11 most critical legacy IT systems in need of modernization.

In addition, federal agencies have partially completed their efforts to modernize the 65 critical legacy systems that were most in need of modernization. In particular, as shown in table 3, as of February 2025, agencies reportedly completed 28 of the 65 modernizations (43 percent), have modernizations underway for 34 systems (52 percent), and have not yet begun modernizations for three systems (5 percent). The associated agencies had planned completion dates for 28 of the 37 systems that have not yet been modernized. See appendix II for the generalized list of systems and their modernization status.

Table 3: Modernization Status of Legacy Systems from GAO-19-471, as of February 2025

Status	Number of systems
Completed	28
In progress, planned completion in the next 2 years	17
In progress, planned completion in 2–5 years	6
In progress, planned completion in over 5 years	4
In progress, planned completion date not yet established	7
Not yet begun	3
Total	65

Source: GAO analysis of agency-reported information. | GAO-25-107795

Note: The planned duration of system modernizations can vary due to a variety of factors, such as the amount of resources available and the complexity and size of the work that is needed. Further, we have previously reported that system modernizations can take longer than expected due to, among other things, poor IT project management practices that lead to schedule delays.

GAO Identified 11 Critical Legacy Systems; Most Agencies Lacked Complete Modernization Plans

Eleven Legacy IT Systems Most in Need of Modernization

As determined by our review of 69 federal legacy IT systems (see appendix III), the 11 legacy systems most in need of modernization are maintained by 10 federal agencies. These agencies' missions are essential to government operations such as health care, critical infrastructure, tax processing, and national security, and these legacy systems provide vital support to the agencies' missions. According to the agencies, these 11 systems ranged from about 23 to 60 years old and collectively cost approximately \$754 million annually to operate and maintain.³⁷

Table 4 provides a generalized list of the 11 legacy IT systems most in need of modernization as well as agency-reported system attributes, such as the system's age, hardware's age, and whether legacy programming languages are used. (Due to sensitivity concerns, we substituted a numeric identifier for the system names and are not providing detailed descriptions.) Appendix IV provides additional agency-reported details on each of these 11 legacy systems.

³⁷Energy's System 4 included costs for two other interwoven systems. DOD's System 3, HHS's System 5, and Transportation's System 8 did not include operating costs for certain components or locations.

Table 4: The 11 Most Critical Federal Legacy IT Systems in Need of Modernization

Agency	System name ^a	System description	Age of system, in years	Age of oldest hardware, in years	Hardware/software/operating system(s) supported	Legacy programming language(s) used
Department of Agriculture	System 1	A system that manages personnel and payroll data	41	—	Yes	Yes
Department of Commerce	System 2 ^b	A system that supports financial management	30	Unknown	Unknown ^d	No
Department of Defense	System 3 ^b	A system that manages defense contracts	60	2	Yes	Yes
Department of Energy	System 4	A system that supports human resource activities	25	3	Yes	Yes
Department of Health and Human Services	System 5 ^c	A system that supports clinical and patient administrative activities	55	1	Yes	Yes
Department of Homeland Security	System 6	A system that supports the management of biometric information	30	13	No	No
Department of the Interior	System 7 ^c	A system that supports the operation of certain dams and powers plants	23	23	No	Yes
Department of Transportation	System 8	A system that manages aeronautical information	31	16	No	Yes
Department of the Treasury	System 9	A system that supports tax processing	59	1	Yes	Yes
	System 10	A system that supports tax processing	51	6 months	Yes	Yes
Environmental Protection Agency	System 11	A system that supports radiation monitoring	51	16	No	No

Legend: — = agency reported that the system does not have dedicated hardware, green shade = favorable characteristic, red shade = unfavorable characteristic, and grey shade = unknown characteristic.

Source: GAO analysis of agency data. | GAO-25-107795

^aDue to sensitivity concerns, we substituted a numeric identifier for the system names and only provided general details.

^bThis system was one of the federal government's 65 legacy systems in need of modernization identified in our 2019 review. See [GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU.

^cThis system was one of the 10 most critical legacy systems in need of modernization that we identified in our 2019 review. See [GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU.

^dCommerce officials stated that the Census Bureau, National Institute of Standards and Technology, and National Oceanic and Atmospheric Administration manage their own hardware for System 2, and that hardware information was unknown for the Census Bureau.

Two systems on our updated list of 11 legacy IT systems most in need of modernization were also part of our 2019 list of 10 most critical legacy systems in need of modernization.³⁸ These systems belonged to the Department of Health and Human Services' (HHS) and Interior. In addition, two other systems on our updated list of 11 systems were previously on our 2019 list of 65 legacy systems in need of modernization. These two systems belonged to Commerce and DOD.

Most of these 11 legacy systems used outdated languages, had unsupported hardware and software, and operated with known cybersecurity vulnerabilities. For example, eight of the 11 systems reported using legacy programming languages, such as COBOL and assembly language code. Relying on assembly language code and COBOL has risks, such as a rise in procurement and operating costs, and fewer individuals with the proper skill sets.

The hardware used among the 11 most critical legacy systems ranged in age from 6 months to 23 years old. Four of those systems reportedly had some unsupported hardware, software, or operating systems. Hardware failure may cause system outages and disrupt an organization's operations, and outdated systems may be more difficult to modify or upgrade to meet emerging mission needs. Agencies reported that two systems—belonging to Interior and the Environmental Protection Agency (EPA)—had all hardware, software, and operating systems no longer supported by the vendor.

Seven of these 11 legacy systems are also reportedly operating with known cybersecurity vulnerabilities that cannot be remediated without modernization. This can lead to increased risks of loss of data and compromised systems. The agencies responsible for some of these systems stated that they were taking steps to mitigate the vulnerabilities. For example, one agency reported that its system contains legacy system components that are unable to receive software updates. However, officials noted that they work to mitigate this risk by system isolation (i.e., it is not interconnected with other components or to the department's network or the internet).

Further, the agencies reported that eight of their legacy systems are not capable of implementing OMB's zero trust strategy without

³⁸[GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU.

modernization.³⁹ For example, one agency reported that its system does not support certain zero trust capabilities to fortify data, such as multi-factor authentication and advanced encryption. In addition, another agency stated that the organizational standards for its system were created over two decades ago and are not compatible with current zero trust capabilities.

Agencies Lacked Complete Modernization Plans for Eight of the 11 Most Critical Legacy IT Systems

Given the age of the hardware and software in legacy systems, the systems' criticality to agency missions, and the security risks posed by operating aging systems, it is imperative that agencies carefully plan for their successful modernization. Documenting modernization plans in sufficient detail increases the likelihood that modernization initiatives will succeed. According to our review of government and industry best practices for the modernization of federal IT,⁴⁰ agencies should have documented modernization plans for legacy systems that, at a minimum, include three key elements:

- milestones to complete the modernization,
- a description of the work necessary to modernize the legacy system, and
- details regarding the disposition of the legacy system.

Of the 11 legacy systems most in need of modernization, three systems had fully documented modernization plans, six systems had partially documented plans, and two systems did not have plans. The two systems that did not have modernization plans belonged to DOD and Energy.

The agencies provided a variety of explanations for not having documented modernization plans. Specifically,

³⁹The 2023 National Cybersecurity Strategy calls for agencies to remove their legacy systems that are incapable of implementing OMB's zero trust architecture strategy within a decade, or otherwise mitigate risks to those that cannot be replaced in that time frame.

⁴⁰General Services Administration, Unified Shared Services Management, *Modernization and Migration Management (M3) Playbook* (Aug. 3, 2016); *M3 Playbook Guidance* (Aug. 3, 2016); American Technology Council, *Report to the President on Federal IT Modernization* (Dec. 13, 2017); OMB, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018); 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).

-
- DOD officials stated that they had a 2015 plan for System 3 that was never implemented. Officials stated they had attempted to secure funding for system modernization over the years but were unable to due to other higher level department priorities. Officials planned to have an updated modernization plan upon completion of a proof of concept that is underway; however, they did not have an estimated time frame for completion.
 - Energy officials stated that they had prepared an initial modernization proposal in October 2023, but it was no longer viable. Officials stated that the department had requested funding through the fiscal year 2026 budget process, and they would update the modernization plan once funding was identified.

Of the nine systems with documented plans, three plans (belonging to DHS, Interior, and EPA) included all three key elements. The other six systems (at Agriculture, Commerce, HHS, Transportation, and Treasury) had modernization plans, but the plans did not include all key elements. Table 5 identifies the nine systems with documented modernization plans, as well as the extent to which the plans included the three key elements. (Due to sensitivity concerns, we substituted a numeric identifier for the system names.)

Table 5: Extent to Which Agencies' Legacy IT Systems Documented Modernization Plans Included Key Elements

Agency	System name ^a	Includes milestones to complete the modernization	Describes the work necessary to modernize the system	Summarizes planned disposition of legacy system
Department of Agriculture	System 1	Yes	No	Partial
Department of Commerce	System 2	Partial	Partial	Partial
Department of Health and Human Services	System 5	Partial	Partial	Partial
Department of Homeland Security	System 6	Yes	Yes	Yes
Department of the Interior	System 7	Yes	Yes	Yes
Department of Transportation	System 8	Yes	No	Partial
Department of the Treasury	System 9	Partial	Partial	No
	System 10	Partial	Yes	Partial
Environmental Protection Agency	System 11	Yes	Yes	Yes

Legend: Yes – Agency included element in modernization plan. Partial – Agency partially included the element in the modernization plan (e.g., the element was completed for only a portion of the modernization, rather than the entire modernization). No – Agency did not include element in modernization plan.

Source: GAO analysis of agency modernization plans. | GAO-25-107795

^aDue to sensitivity concerns, we substituted a numeric identifier for the system names.

The five agencies that had the six incomplete modernization plans provided a variety of reasons for the missing elements:

- Agriculture officials stated that they would develop more detailed plans for modernizing System 1 once the administration confirms the path forward, funding for the project is approved, and the software contract has been awarded.
- Commerce officials stated that detailed plans for modernizing the remaining phase of its System 2 would be developed once funding is identified, but did not have a time frame for completion. Officials further stated that each bureau would develop decommissioning plans as they are undergoing deployment to the modernized system, according to their phased approach.
- HHS officials stated that they did not have updated plans for the System 5 modernization that reflect the milestones and details for a new completion date of 2035 (5 years later than the original plan) and decommissioning of the legacy system. Officials stated that the schedule had to be adjusted due to funding availability for the project, and that a firm completion date would depend on how many tribal and urban Indian organization partners participate in implementing the solution. Officials further stated that plans for the overall modernization initiative have not changed.

-
- Transportation officials stated that its System 8 roadmap was only intended to identify overall phases for the modernization, and that detailed work schedules and decommissioning plans would be developed with the vendor once a contract is awarded. However, Transportation did not have an estimated time frame for completion.
 - Treasury officials stated that plans for its System 9 modernization initially focused on delivering value as quickly as possible using an iterative and incremental approach, so they initially developed a roadmap outlining releasable features for 2024 through 2026. Officials stated that they are now shifting focus to future releases and refining the plans to include releases for 2027 through 2029. However, they did not have an estimated time frame for completion.

For System 10, Treasury officials stated that they have not yet established plans with specific dates because they are performing an analysis to identify a cost-effective path for delivering tax services. However, they did not have an estimated time frame for completion.

Finally, seven of the eight systems with incomplete or missing plans reportedly have modernizations that are already underway (Agriculture's System 1, Commerce's System 2, DOD's System 3, Health and Human Services System 5, Transportation's System 8, Treasury's System 9, and Treasury's System 10).

While we recognize that system modernizations are dependent on funding, it is important for agencies to prioritize funding for the modernization of these critical legacy systems. In addition, Congress provided increased authority for agencies to fund such modernization efforts through the MGT Act's Technology Modernization Fund and the related IT working capital funds. Further, the National Cybersecurity Strategy has prioritized federal efforts to eliminate legacy systems that are costly to maintain and difficult to defend against sophisticated cyber threats.

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, their modernization initiatives will have an increased likelihood of cost overruns, schedule delays, and overall project failure. Project failure would be particularly detrimental, not only because of wasted resources, but also because it would prolong the lifespan of increasingly vulnerable and obsolete systems. This could expose the agency and system clients to security threats and potentially significant performance issues.

Further, agencies may not be effectively planning for the modernization of legacy systems, in part, because they are not required to. As we reported in May 2016, agencies are not required to identify, evaluate, and prioritize existing IT investments to determine whether they should be kept as-is, modernized, replaced, or retired.⁴¹ We recommended that OMB direct agencies to identify legacy systems needing to be replaced or modernized. Given OMB's lack of action, we designated this as a priority recommendation in May 2023.⁴²

However, it has been 9 years since we made the recommendation and OMB has not taken action to implement it. Thus, Congressional action to require agencies to develop modernization plans could help ensure that agencies prioritize the planning of their legacy systems that are most in need of modernization.

Conclusions

Federal legacy systems are critical to the functioning of the government, but often operate with outdated computer languages, unsupported hardware and software, and known cybersecurity vulnerabilities. This makes them difficult to maintain, increases costs, and increases risks. Further, of the 11 most critical legacy systems that we identified, eight lack complete modernization plans. Documenting plans is just an initial step in an often overly lengthy process to successfully plan, modernize, and replace these legacy systems. Nevertheless, OMB has not acted on our longstanding recommendation to require agencies to identify legacy systems needing modernization. Accordingly, it is appropriate to ask Congress to take such action. Doing so can reduce agencies' growing reliance on outdated, insufficient, and vulnerable legacy systems to carry out their missions.

Matter for Congressional Consideration

Congress should consider requiring major federal agencies to develop modernization plans for their legacy systems that have been identified as most in need of modernization.

Recommendations for Executive Action

In the LOUO report that we are issuing concurrently with this report, we are making a total of eight recommendations to seven federal agencies to document modernization plans for their respective legacy systems,

⁴¹[GAO-16-468](#).

⁴²[GAO-23-106298](#).

including milestones, a description of the work necessary, and details on the disposition of the legacy system.

Agency Comments and Our Evaluation

We requested comments on a draft of this report from OMB and the other 24 agencies included in our review. Of the seven agencies we made recommendations to, three agreed with our recommendations, three did not agree or disagree, and one disagreed with our recommendations. In addition, OMB and the 17 agencies to which we did not make recommendations either did not agree nor disagree with our findings, or stated that they had no comments. Further, six agencies provided technical comments, which we have incorporated, as appropriate.

The following three agencies agreed with our recommendations:

- In written comments from DOD on the LOUO version of this report, the agency stated that it concurred with our recommendation and identified steps it would take to address the recommendation. DOD's comments are reprinted in appendix V.
- In written comments from Energy on the LOUO version of this report, the agency stated that it concurred with our recommendation. Energy stated that as part of a broader effort to modernize its human capital IT, the management and support of System 4 has recently been transferred from the agency's Office of the Chief Financial Officer to its OCIO. Due to staff and organizational changes, the OCIO is in the process of revising its modernization strategy. The OCIO, along with the Office of the Chief Financial Officer and Office of the Chief Human Capital Office, are actively migrating several functions with significant system dependencies on System 4 to a new platform, which is scheduled to be completed by December 2026. Following the completion of migration, the OCIO intends to undertake a formal modernization planning approach to address the remaining functions and dependent systems. In the interim, the system's hardware and software is continuously maintained with the latest patches and updates, in accordance with current cybersecurity requirements. Energy's comments are reprinted in appendix VI.
- In comments received via email on May 8, 2025, a Management Analyst from Transportation stated that the agency concurred with our recommendation and would provide a detailed response within 180 days of the final report.

The following three agencies did not state whether they agreed or disagreed with our recommendations:

-
- In comments received via email on May 22, 2025, Commerce's GAO/OIG Audit Liaison stated that the agency did not have any comments, and did not state whether it agreed or disagreed with our recommendation.
 - In written comments from HHS, the agency did not agree nor disagree with our recommendation, but it identified activities planned to address it. Specifically, HHS stated that its OCIO continues to work with the Indian Health Service to refine and execute modernization plans consistent with the observations and recommendations made as part of this engagement. This includes the development and implementation of all milestones necessary to undertake the system modernization, and plans that provide greater insight on the disposition of the legacy system itself. HHS's comments are reprinted in appendix VII.
 - In comments received via email on May 23, 2025, a representative from Treasury's OCIO stated that the agency did not have any comments, and did not state whether they agreed or disagreed with our recommendations.

The following agency disagreed with our recommendation:

- In comments received via email on May 15, 2025, a Program Analyst from Agriculture stated that the agency did not agree with our finding that it did not have a modernization plan for its system. Agriculture officials agreed that they did not have a final documented modernization plan when GAO inquired in July 2024. However, they said they had since developed their plan and provided a draft modernization plan in June 2025. According to officials, this plan was developed in February 2025.

We reviewed the document and determined that it partially addressed the key elements. Specifically, it included milestones to complete the modernization, did not describe the work necessary to modernize the legacy system, and partially included plans for the disposition of the legacy system. Accordingly, we revised our report findings to give the agency partial credit for having a modernization plan. We also revised our recommendation for the agency to include the missing elements.

Of the 18 agencies to which we did not make recommendations, one agency (the Social Security Administration) provided written comments on the LOUO version of this report. In its written response (reprinted in appendix VIII), the agency expressed appreciation for the opportunity to review the report, and that it continues to evaluate its legacy systems and make efforts to modernize and enhance them in accordance with

budgetary considerations. The agency did not state whether they agreed or disagreed with our findings. OMB and 16 other agencies did not have comments (Education, DHS, Housing and Urban Development, Justice, Labor, Interior, State, Veterans Affairs, EPA, the General Services Administration, the National Aeronautics and Space Administration, the National Science Foundation, the Nuclear Regulatory Commission, the Office of Personnel Management, the Small Business Administration, and the U.S. Agency for International Development). In addition, we received technical comments from six agencies (DHS, Justice, Labor, Interior, Veterans Affairs, and EPA), which we have incorporated as appropriate.

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

If you or your staff have any questions about this report, please contact Kevin Walsh at walshk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IX.

//SIGNED//

Kevin Walsh
Director, Information Technology and Cybersecurity

Appendix I: Objective, Scope, and Methodology

Our objective was to identify the federal legacy IT systems most in need of modernization and evaluate plans for modernizing them. The scope of our review included the 24 agencies covered by the Chief Financial Officers Act of 1990.¹

This report presents a public version of a “limited official use only” (LOUO) report that we are also issuing today.² The LOUO report includes eight recommendations that we made to seven agencies to identify and document modernization plans for particular legacy systems, including milestones, a description of the work necessary, and details on the disposition of the legacy system.³ In this public version of the report, we have omitted sensitive information regarding particular legacy systems. Specifically, we have deleted systems’ names and other information that would identify the particular system, such as specific descriptions of the systems’ purposes and vulnerabilities. Although the information provided in this report is more limited, this report addresses the same objectives as the LOUO report and is based on the same audit methodology.

To address our objective, we followed a similar approach as in our 2019 review of federal legacy systems.⁴ Specifically, to identify the federal legacy IT systems most in need of modernization, we first asked each of the agencies to provide their three legacy IT systems most in need of modernization.⁵ This resulted in a list of 69 systems. However, due to

¹The 24 major federal agencies covered by the Chief Financial Officers Act of 1990 are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development. 31 U.S.C. § 901(b).

²GAO, *Information Technology: Agencies Need to Plan for Modernizing Critical Decades-Old Legacy Systems*, GAO-25-107289SU (Washington, D.C.: July 17, 2025).

³We made recommendations to the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Transportation, and the Treasury.

⁴GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, [GAO-19-471](#) (Washington, D.C.: June 11, 2019) and concurrent limited official use only report GAO-19-351SU.

⁵The Modernizing Government Technology Act defines a legacy IT system as a system that is outdated or obsolete. *National Defense Authorization Act for Fiscal Year 2018*, Pub. L. No. 115-91, Div. A, Title X, Subtitle G, § 1076, 131 Stat. 1283, 1586-87 (2017), 40 U.S.C. § 11301 note.

sensitivity concerns, we are not disclosing the names of the systems in this report. Appendix III provides a generalized list of those systems.⁶

To develop a set of attributes for determining systems' obsolescence and their need for modernization, we considered the attributes used in our 2019 review of federal legacy systems and determined whether they should be modified.⁷ In doing so, we reviewed relevant federal guidance that had been issued since our prior review and consulted with our system development and cybersecurity experts. We concluded that the 14 system attributes used in our 2019 review were still relevant, except we updated the time-based attributes to reflect the 5 years that have passed since our prior review. We also decided to include two additional system attributes due to an increased importance on cybersecurity issues in modernizing the federal government's legacy IT:

- Whether the system was capable of implementing the zero trust strategy.⁸
- Whether the system had known cybersecurity vulnerabilities that could only be remediated with modernization, and if so, whether the agency was mitigating the risks.

We then asked the agencies in our review to provide the associated details for the selected systems. We considered these details to rank the systems against the attributes that we compiled. We assigned point values to each system based on their agency-reported attributes. Table 6 details the 16 system attributes and associated point values and ranges we used to rank the agency-provided legacy systems.

⁶Most agencies provided a list of three legacy systems in need of modernization. However, the Department of Veterans Affairs reported six legacy systems, the Departments of Transportation and the Treasury each reported four legacy systems, and the Department of Homeland Security and the National Science Foundation each reported two legacy systems. The Nuclear Regulatory Commission and U.S. Agency for International Development stated that they did not have any legacy systems in need of modernization.

⁷[GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU.

⁸Zero trust architecture is a cybersecurity approach that works on the "never trust, always verify" principle and is intended to address rapidly evolving security risks. In January 2022, the Office of Management and Budget published a strategy aimed at moving the U.S. government toward zero trust cybersecurity principles. Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, M-22-09 (Washington, D.C.: Jan. 26, 2022).

Table 6: System Attributes and Associated Point Values Used to Rank Legacy Systems

System attribute	Point values
Initial year of implementation	0 points if the systems had been implemented less than 10 years ago (since 2015)
	2 points if the systems had been implemented in the past 10-19 years (2005-2014)
	4 points if the systems had been implemented in the past 20-29 years (1995-2004)
	6 points if the systems had been implemented in the past 30-39 years (1985-1994)
	8 points if the systems had been implemented in the past 40-49 years (1975-1984)
	10 points if the systems had been implemented over 50 years ago (before 1975)
Date of oldest hardware	0 points if the oldest hardware had been installed less than 10 years ago (since 2015)
	2 points if the oldest hardware had been installed in the past 10-19 years (2005-2014)
	4 points if the oldest hardware had been installed in the past 20-29 years (1995-2004)
	6 points if the oldest hardware had been installed in the past 30-39 years (1985-1994)
	8 points if the oldest hardware had been installed in the past 40-49 years (1975-1984)
	10 points if the oldest hardware had been installed over 50 years ago (before 1975)
Hardware warranty status	0 points if the system's hardware was under warranty
	5 points if the system's hardware was no longer under warranty
Operating system support status	0 points if the system's operating system was supported by the vendor
	5 points if the system's operating system was no longer supported by the vendor
Software support status	0 points if the system's software was supported by the vendor
	5 points if the system's software was no longer supported by the vendor
Use of legacy programming language	0 points if the system did not use a programming language that the agency identified as a legacy language
	5 points if the system used a programming language that the agency identified as a legacy language
System criticality (on a scale of 1 to 5; 5 being most critical to the agency's mission)	1-5 points, as assessed by the agency
Cybersecurity risk to the system (on a scale of 1 to 5; 5 having the highest risk)	1-5 points, as assessed by the agency
High Value Asset ^a status	0 points if the system had not been a High Value Asset
	10 points if system had been a High Value Asset
Zero trust implementation capability ^b	0 points if the system was capable of implementing the zero trust strategy
	5 points if the system was not capable of implementing the zero trust strategy
Known cybersecurity vulnerabilities	0 points if the system did not have known cybersecurity vulnerabilities that could only be remediated with modernization
	5 points if the system had known cybersecurity vulnerabilities that could only be remediated with modernization, and the agency was mitigating the risks
	10 points if the system had known cybersecurity vulnerabilities that could only be remediated with modernization, and the agency was not mitigating the risks

Appendix I: Objective, Scope, and Methodology

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

Source: GAO analysis. | GAO-25-107795

^aA high value asset is a designation for federal information or a federal information system that processes, stores, or transmits high value information, is considered vital to an agency fulfilling its primary mission, or serves a critical function in maintaining the security and resilience of the federal civilian enterprise.

^bThe National Cybersecurity Strategy of 2023 called for the federal government to prioritize efforts to eliminate legacy systems that are costly to maintain and difficult to defend against sophisticated cyber threats. This included removing all legacy systems incapable of implementing the zero trust architecture strategy within a decade, or otherwise mitigating risks to those that cannot be replaced in that timeframe.

We then totaled the assigned points for each legacy system and ranked the results from highest to lowest number of assigned points. We looked for approximately 10 systems that were ranked among the highest, accounting for several tied scores, and identified 11 systems with the highest scores as those legacy systems most in need of modernization. The scores for the 11 selected systems ranged from 51 to 60 points, and the other systems ranged from nine to 48 points. We also compared our list of systems against the 2019 list to identify systems that had also been in our prior review. Table 7 provides a generalized list of the 11 selected legacy systems most in need of modernization. However, due to sensitivity concerns, we substituted a numeric identifier for the system names.

Table 7: The 11 Selected Federal Legacy IT Systems Most in Need of Modernization

Agency	System name ^a
Department of Agriculture	System 1
Department of Commerce	System 2 ^b
Department of Defense	System 3 ^b
Department of Energy	System 4
Department of Health and Human Services	System 5 ^c
Department of Homeland Security	System 6
Department of the Interior	System 7 ^c
Department of Transportation	System 8
Department of the Treasury	System 9
	System 10
Environmental Protection Agency	System 11

Source: GAO analysis. | GAO-25-107795

^aDue to sensitivity concerns, we substituted a numeric identifier for the system names.

^bThis system was previously identified as one of the 65 federal government's legacy systems in need of modernization. See [GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU.

^cThis system was previously identified as one of the federal government's 10 most critical legacy systems in need of modernization. See [GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU.

To evaluate agencies' plans for modernizing the 11 federal legacy systems most in need of modernization, we requested that agencies provide their documented plans for modernizing the selected systems. These modernization plans could have been contained within several types of documentation, since a system modernization could be a new system development, a system acquisition, or a renovation of the legacy system. For example, if an agency were acquiring a new system from a

vendor, the plans for modernization could have been contained within an acquisition plan or a statement of work in a contract. Likewise, if an agency was developing a new system on its own, the modernization plans could have been within a project plan or design document.

We determined that the criteria used in our 2019 review, which was based on government and industry best practices on the identification and modernization of legacy systems, were still current and relevant.⁹

According to these sources, agencies' documented plans for system modernization should include, at a minimum, (1) milestones to complete the modernization, (2) a description of the work necessary to modernize the system, and (3) details regarding the disposition of the legacy system.¹⁰ We then analyzed agencies' documented modernization plans for the selected systems to determine whether the plans included these elements. If an agency's plans included milestones for only a portion of the initiative or only described a portion of the work necessary to complete the modernization, we assigned the agency a partial rating. Appendix IV provides generalized details on each of the selected systems and the agencies' plans for modernizing them.

We conducted this performance audit from January 2024 to July 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

⁹[GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU.

¹⁰General Services Administration, Unified Shared Services Management, *Modernization and Migration Management (M3) Playbook* (Aug. 3, 2016); *M3 Playbook Guidance* (Aug. 3, 2016); American Technology Council, *Report to the President on Federal IT Modernization* (Dec. 13, 2017); Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018); 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); and American Council for Technology-Industry Advisory Council, *Legacy System Modernization: Addressing Challenges on the Path to Success* (Fairfax, VA: Oct. 7, 2016).

Appendix II: Status of Legacy IT Systems Identified in 2019 as Most in Need of Modernization

In June 2019, we reported on the 24 Chief Financial Officers Act agencies’ legacy IT systems most in need of modernization. At that time, the agencies identified a total of 65 such systems.¹ We obtained updates from the agencies on their reported status of modernizing the 65 systems, as of February 2025. Overall, of the 24 agencies:

- two agencies had reportedly completed modernizations for all their systems identified in 2019 (Nuclear Regulatory Commission and Small Business Administration),
- six agencies had modernizations that were not yet completed for all of their systems (the Departments of Agriculture, Energy, Labor, State, Transportation, and Veterans Affairs), and
- the remaining 15 agencies had a mix of modernization completion statuses.

In addition, two agencies had modernizations that had not yet begun (one at the Department of Health and Human Services and two at the Department of State). Table 8 provides a generalized list of agencies’ legacy systems most in need of modernization from 2019, as well as an updated status of modernizing these systems, according to the agencies, as of February 2025. (Due to sensitivity concerns, we substituted a numeric identifier for the names of the 10 most critical legacy systems in need of modernization and assigned a letter or letters for the names of the remaining 55 systems.)

Table 8: Agency-Reported Status of Legacy IT Systems Identified in 2019 as Most in Need of Modernization, as of February 2025

Agency	2019 system name ^a	Agency-reported modernization status	Agency-reported expected completion of modernization, as of February 2025
Department of Agriculture	2019 System A	In progress	End of fiscal year 2025
Department of Commerce	2019 System C ^b	In progress	October 2026
	2019 System B	Completed in December 2022	
Department of Defense	2019 System 1 ^c	Completed in fiscal year 2020	
	2019 System D ^b	In progress	Not yet established
	2019 System E	Completed in March 2020	

¹Most 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 in need of modernization.

**Appendix II: Status of Legacy IT Systems
Identified in 2019 as Most in Need of
Modernization**

Agency	2019 system name^a	Agency-reported modernization status	Agency-reported expected completion of modernization, as of February 2025
Department of Education	2019 System 2 ^{b, c}	In progress	September 2025
	2019 System F	Completed in November 2018	
	2019 System G	Completed in September 2023	
	2019 System H	In progress	September 2025
Department of Energy	2019 System I	In progress	5 or more years from fiscal year 2026
Department of Health and Human Services	2019 System J	Not yet begun	Latter half of 2027
	2019 System K	Completed in November 2021	
	2019 System 3 ^{b, c}	In progress	End of fiscal year 2035
Department of Homeland Security	2019 System 4 ^c	In progress	Not yet established ^e
	2019 System L	Completed in Fiscal year 2022	
	2019 System M	In progress	Not yet established ^e
Department of Housing and Urban Development	2019 System N	In progress	Not yet established
	2019 System O	Completed in December 2021	
	2019 System P	Completed in December 2019	
Department of the Interior	2019 System 5 ^{b, c}	In progress	August 2027
	2019 System Z	Completed in January 2022	
	2019 System AA	In progress	2029
Department of Justice	2019 System S	Completed in 2021	
	2019 System Q	Completed in December 2023	
	2019 System R	In progress	January 2027
Department of Labor	2019 System V ^d	In progress	Second quarter of fiscal year 2025
	2019 System Tb	In progress	End of fiscal year 2028
	2019 System U	In progress	Fourth quarter of fiscal year 2025
Department of State	2019 System X	Not yet begun	Not yet established
	2019 System Y	In progress	Not yet established
	2019 System W	Not yet begun	Not yet established
Department of Transportation	2019 System 7 ^c	In progress	2026
	2019 System AE	In progress	Fiscal year 2026
	2019 System AD ^b	In progress	July 2025
Department of the Treasury	2019 System AC	Completed in July 2020	
	2019 System 6 ^{b, c}	In progress	2028
	2019 System AB	In progress	December 2026
Department of Veterans Affairs	2019 System AG ^b	In progress	First quarter of 2026
	2019 System AF	In progress	End of fiscal year 2031
	2019 System AH ^d	In progress	Not yet established
	2019 System AJ	In progress	March 2027

**Appendix II: Status of Legacy IT Systems
Identified in 2019 as Most in Need of
Modernization**

Agency	2019 system name^a	Agency-reported modernization status	Agency-reported expected completion of modernization, as of February 2025
Environmental Protection Agency	2019 System AK	Completed in December 2020	
	2019 System AI ^b	In progress	2026
General Services Administration	2019 System AN	Completed in June 2021	
	2019 System AL ^b	In progress	Fiscal year 2026
	2019 System AM	Completed in March 2019	
National Aeronautics and Space Administration	2019 System AP	Completed in October 2022	
	2019 System AO	In progress	March 2025
	2019 System AQ	In progress	June 2025
National Science Foundation	2019 System AU	Completed in November 2020	
	2019 System AW ^b	In progress	December 2026
	2019 System AV	Completed in November 2019	
Nuclear Regulatory Commission	2019 System AR	Completed in 2018	
	2019 System AT	Completed in fiscal year 2020	
	2019 System AS	Completed in 2018	
Office of Personnel Management	2019 System 8 ^c	Completed in September 2024	
	2019 System AY	In progress	Not yet established
	2019 System AX	Completed in October 2022	
Small Business Administration	2019 System BA	Completed in May 2018	
	2019 System AZ	Completed in March 2024	
	2019 System 9 ^c	Completed in April 2023	
Social Security Administration	2019 System BC ^b	Completed in January 2025	
	2019 System BB ^b	In progress	10 or more years from February 2025
	2019 System 10 ^{b, c}	In progress	2 or more years from February 2025
United States Agency for International Development	Not applicable – agency stated that it does not have any legacy systems		

Legend: green shade = modernization completed.

Source: GAO-19-351SU and analysis of agency data. | GAO-25-107795

Note: If the agency reported that the system modernization was completed, the actual completion date is listed. If the agency reported that the system modernization was in progress, the planned completion date is listed.

^aDue to sensitivity concerns, we substituted a numeric identifier for the names of the 10 most critical legacy systems in need of modernization and assigned a letter or letters for the names of the remaining 55 systems.

^bThis system was also identified in 2025 as one of the federal government's 69 legacy IT systems in need of modernization.

^cThis system was previously identified as one of the federal government's 10 most critical legacy systems in need of modernization. See [GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU.

^dA component of this system was also identified in 2025 as one of the federal government's 69 legacy IT systems in need of modernization.

**Appendix II: Status of Legacy IT Systems
Identified in 2019 as Most in Need of
Modernization**

^eThe agency stated that it does not intend to establish a modernization completion date for this system.

Appendix III: Legacy IT Systems Identified in 2025 as Most in Need of Modernization

For this review, each of the 24 Chief Financial Officers Act agencies identified their agency’s legacy systems most in need of modernization. The agencies identified a total of 69 such systems.¹ The agencies also identified various attributes of the legacy systems, including the systems’ age; hardware age; hardware, software, and operating system support; use of legacy programming languages; the system’s ability to implement a zero trust architecture; and known cybersecurity vulnerabilities of the system. Table 9 provides a generalized list of the agencies’ legacy systems most in need of modernization, as well as selected attributes related to each system, as reported by the agencies.² (Due to sensitivity concerns, we substituted a numeric identifier for the names of the 11 most critical legacy systems in need of modernization and assigned a letter or letters for the names of the remaining 58 systems.)

Table 9: Legacy IT Systems Identified in 2025 as Most in Need of Modernization and Select Attributes

Agency	System name ^a	Age of system, in years	Age of oldest hardware, in years	Hardware/software/operating system(s) supported	Legacy programming language(s) used	Able to implement zero trust	Known cyber-security vulnerabilities
Department of Agriculture	System A	10	2	Unknown	No	No	No
	System 1	41	–	Yes	Yes	Yes	No
	System B	57	1	Yes	Yes	Yes	No
Department of Commerce	System C	20	–	Yes	No	No	Unknown
	System 2 ^b	30	Unknown	Unknown	No	No	No
	System D	14	14	No	No	Yes	Yes, but mitigating
Department of Defense	System E	6	–	Yes	No	Yes	No
	System F	16	–	Yes	No	No	No
	System 3 ^b	60	2	Yes	Yes	No	Yes, but mitigating

¹Most agencies provided a list of three legacy systems in need of modernization. However, the Department of Veterans Affairs reported six legacy systems, the Departments of Transportation and the Treasury each reported four legacy systems, and the Department of Homeland Security and National Science Foundation each reported two legacy systems. The Nuclear Regulatory Commission and U.S. Agency for International Development stated that they did not have any legacy systems in need of modernization.

²Some of the system attributes can change over time, such as whether hardware, software, or operating systems are currently vendor supported. The system attributes are based on the data we collected to score and rank the systems, which was around summer 2024 for all agencies, except for Commerce, which was around November 2024.

**Appendix III: Legacy IT Systems Identified in
2025 as Most in Need of Modernization**

Agency	System name ^a	Age of system, in years	Age of oldest hardware, in years	Hardware/software/ operating system(s) supported	Legacy programming language(s) used	Able to implement zero trust	Known cyber-security vulnerabilities
Department of Education	System G	19	–	Yes	No	Yes	No
	System H ^c	51	2	Yes	Yes	Unknown	No
	System I	13	–	Yes	Yes	Yes	No
Department of Energy	System J	24	3	Yes	No	Yes	No
	System 4	25	3	Yes	Yes	No	Yes, not mitigating
	System K	18	3	No	Yes	No	Yes, but mitigating
Department of Health and Human Services	System L	4	4	Yes	No	Yes	No
	System M	22	–	Yes	No	Yes	No
	System 5 ^c	55	1	Yes	Yes	No	Yes, but mitigating
Department of Homeland Security	System 6	30	13	No	No	Yes	Yes, but mitigating
	System N	29	4	Yes	Yes	Yes	Yes, not mitigating
Department of Housing and Urban Development	System O	8	3	Yes	No	Yes	No
	System P	42	3	Yes	Yes	Yes	No
	System Q	39	3	Yes	No	Yes	No
Department of the Interior	System R	25	1	No	Yes	Yes	Yes, but mitigating
	System 7 ^c	23	23	No	Yes	Not applicable	Yes, but mitigating
	System S	35	5	Yes	No	No	Yes, but mitigating
Department of Justice	System T	38	–	Yes	Yes	Yes	No
	System U	10	9	Yes	No	Unknown	Yes, but mitigating
	System V	3	9	Yes	No	Yes	No
Department of Labor	System W ^b	19	1	Yes	Yes	No	No
	System X ^d	20	5	Yes	Yes	No	Yes, but mitigating
	System Y	29	3	Yes	No	Yes	No
Department of State	System Z	26	4	Yes	No	Yes	No
	System AA	16	–	No	No	Yes	No
	System AB	24	–	Yes	No	Yes	No
Department of Transportation	System 8	31	16	No	Yes	No	Yes, but mitigating

**Appendix III: Legacy IT Systems Identified in
2025 as Most in Need of Modernization**

Agency	System name ^a	Age of system, in years	Age of oldest hardware, in years	Hardware/software/ operating system(s) supported	Legacy programming language(s) used	Able to implement zero trust	Known cyber-security vulnerabilities
	System AC	11	7	Yes	No	No	Yes, not mitigating
	System AD	9	–	No	Yes	No	Yes, but mitigating
	System AE ^b	22	1	Yes	No	No	Yes, but mitigating
Department of the Treasury	System 9	59	1	Yes	Yes	No	No
	System AF	41	–	Unknown	Yes	No	No
	System AG ^c	56	1	Yes	Yes	Yes	No
	System 10	51	0	Yes	Yes	No	No
Department of Veterans Affairs	System AH ^b	54	2	Yes	Yes	Yes	No
	System AI	31	–	No	No	No	No
	System AJ	32	4	No	No	No	No
	System AK	11	4	No	Unknown	No	No
	System AL	9	–	Yes	No	Yes	Yes, but mitigating
	System AM ^d	27	4	No	No	No	No
Environmental Protection Agency	System 11	51	16	No	No	No	Yes, but mitigating
	System AN	21	3	No	No	Yes	No
	System AO ^b	29	–	No	Unknown	Yes	No
General Services Administration	System AP ^b	44	2	Yes	Yes	Yes	No
	System AQ	29	–	No	Yes	Yes	No
	System AR	20	2	Yes	No	Yes	No
National Aeronautics and Space Administration	System AS	12	6	Yes	Yes	Yes	No
	System AT	22	3	Yes	No	Yes	No
	System AU	22	1	Yes	No	Yes	No
National Science Foundation	System AV ^b	27	–	Yes	No	Yes	No
	System AW	15	1	No	No	Yes	No
Nuclear Regulatory Commission	Not applicable – agency stated that it does not have any legacy systems in need of modernization						
Office of Personnel Management	System AX	40	4	Yes	Yes	Yes	No
	System AY	40	4	Yes	Yes	Yes	No
	System AZ	Unknown	3	Yes	Yes	Yes	No
Small Business Administration	System BA	22	–	Yes	No	Yes	No
	System BB	22	–	Yes	No	Yes	No

Appendix III: Legacy IT Systems Identified in 2025 as Most in Need of Modernization

Agency	System name ^a	Age of system, in years	Age of oldest hardware, in years	Hardware/software/ operating system(s) supported	Legacy programming language(s) used	Able to implement zero trust	Known cyber-security vulnerabilities
Social Security Administration	System BC	22	–	Yes	No	Yes	No
	System BD ^b	43	3	Yes	Yes	Yes	No
	System BE ^b	39	4	Yes	Yes	Yes	No
	System BF ^c	50	4	Yes	Yes	Yes	No
United States Agency for International Development	Not applicable – agency stated that it does not have any legacy systems in need of modernization						

Legend: – = agency reported that the system does not have dedicated hardware, green shade = favorable characteristic, red shade = unfavorable characteristic, and grey shade = unknown characteristic.

Source: GAO analysis of agency data. | GAO-25-107795

^aDue to sensitivity concerns, we substituted a numeric identifier for the names of the 11 most critical legacy systems in need of modernization and assigned a letter or letters for the names of the remaining 58 systems.

^bThis system was previously identified as one of the 65 federal government’s legacy systems in need of modernization. See [GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU.

^cThis system was previously identified as one of the federal government’s 10 most critical legacy systems in need of modernization. See [GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU.

^dThis is a component of a system that was previously identified as one of the 65 federal government’s legacy systems in need of modernization. See [GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU.

Of the 69 systems, or components of systems, provided by agencies for this review, 17 systems were previously on our 2019 list of 65 legacy systems in need of modernization. Table 10 provides a crosswalk of the alphanumeric identifiers that were used to identify the same 17 systems reported in 2019 and in this report.

Table 10: Crosswalk of System Identifiers for the 17 Legacy Systems Reported in Both 2019 and 2025		
Agency	System name, as reported in GAO-19-471 ^a	System name, as reported in GAO-25-107795 ^b
Department of Commerce	System C	System 2
Department of Defense	System D	System 3
Department of Education	System 2	System H
Department of Health and Human Services	System 3	System 5
Department of the Interior	System 5	System 7
Department of Labor	System V	System X
	System T	System W

Appendix III: Legacy IT Systems Identified in 2025 as Most in Need of Modernization

Agency	System name, as reported in GAO-19-471^a	System name, as reported in GAO-25-107795^b
Department of Transportation	System AD	System AE
Department of the Treasury	System 6	System AG
Department of Veterans Affairs	System AG	System AH
	System AH	System AM
Environmental Protection Agency	System AI	System AO
General Services Administration	System AL	System AP
National Science Foundation	System AW	System AV
Social Security Administration	System BC	System BD
	System BB	System BE
	System 10	System BF

Source: [GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU and analysis of agency data. | GAO-25-107795

^aDue to sensitivity concerns, we substituted a numeric identifier for the names of the 10 most critical legacy systems in need of modernization, identified in [GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU, and assigned a letter or letters for the names of the remaining 55 systems.

^bDue to sensitivity concerns, we substituted a numeric identifier for the names of the 11 most critical legacy systems in need of modernization and assigned a letter or letters for the names of the remaining 58 systems.

Appendix IV: Profiles of the 11 Legacy IT Systems Most in Need of Modernization

This appendix describes the 11 legacy IT systems most in need of modernization, as identified during our review. The profiles of each system describe (1) the system's purpose, (2) the reason that the system needs to be modernized, (3) the status of agency's plans for modernization, and (4) possible benefits to be realized once the system is modernized.

System 1

U.S. Department of Agriculture—National
Finance Center

Initial year of implementation: 1983

System hardware under warranty? Not
applicable

Software vendor supported? Yes

Operating system(s) supported? Yes

Legacy programming language(s) used?
Yes

System criticality (as determined by
agency): High

System cybersecurity risk (as determined
by agency): Moderate

Capable of implementing zero trust? Yes
Known cybersecurity vulnerabilities that
cannot be remediated without
modernization? No

Reported number of users: 85,000

Reported annual operating costs: \$103.8
million

Reported status of modernization: In
progress; planned completion fiscal year 2031

Reported cost of modernization: Agency
has not calculated

Potential cost savings: Agency has not
calculated

Other benefits: Agency has not identified

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

Source: GAO analysis of agency documentation and
interviews. | GAO-25-107795

The Department of Agriculture National Finance Center’s (NFC) System 1 provides comprehensive and automated actions necessary for recording, processing, and reporting the personnel and payroll data for Agriculture and other federal agencies.

Officials from the department Office of the Chief Information Officer (OCIO) and Office of the Chief Financial Officer stated that Agriculture selected its systems most in need of modernization, including System 1, based on the date the system was expected to be decommissioned, the inherent risks to the system, and the age of the system. According to Agriculture officials, the system is 41 years old and uses Common Business Oriented Language (COBOL), which is considered to be a legacy programming language.¹

The department intends to replace the system by implementing another modernization program, which is to modernize its service offerings, technical architecture, and operational capabilities. However, in July 2024, department officials stated they had not developed a modernization plan for the system due to insufficient staffing. In February 2025, officials stated that they had since conducted a market analysis, operational assessment, and architecture assessment to understand the current system’s capabilities and limitations. Officials also stated that they had begun the acquisition planning phase and provided a timeline with some key dates they considered to be tentative.

In May 2025, officials stated that their plans had solidified and in June 2025, provided a draft system modernization plan. According to officials, Agriculture’s IT Governance Board had reviewed and approved the modernization plan and established the modernization program as a formal IT investment; however, the plan was still pre-decisional because the administration was in the process of reviewing the modernization approach and making determinations on a path forward. Although the draft plan included milestones to complete the modernization through fiscal year 2031, including dates for decommissioning the legacy system, it did not include details on the work necessary to complete these milestones or to decommission the legacy system. Officials stated that

¹COBOL, 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.

they would develop these details once the administration confirms the path forward, funding for the project is approved, and the software contract has been awarded.²

Regarding potential cost savings or other benefits for modernizing the system, Agriculture officials stated that a new system had not yet been identified or planned for, and that modernization costs would be determined at the conclusion of the previously mentioned assessment.

²According to Agriculture officials in June 2025, they had submitted a project proposal for System 1 to the General Services Administration's Technology Modernization Fund and were awaiting approval of the requested funding for fiscal years 2026 through 2027 implementation activities. They further stated that the amount and timeliness of funding may impact System 1 modernization plan timeline and activities.

System 2

Department of Commerce
Initial year of implementation: 1994
System hardware under warranty?
Unknown
Software vendor supported? Yes
Operating system(s) supported? Yes
Legacy programming language(s) used?
No
System criticality (as determined by agency): High
System cybersecurity risk (as determined by agency): High
Capable of implementing zero trust? No
Known cybersecurity vulnerabilities that cannot be remediated without modernization? No
Reported number of users: 7,800^a
Reported annual operating costs: \$41.4 million
Reported status of modernization: In progress; planned completion October 2026
Reported cost of modernization: Agency has not calculated
Potential cost savings: Agency has not calculated
Other benefits: Ability to implement zero trust, simplified IT asset management, and increased functionality
Status of modernization plans: Agency has documented modernization plans that partially include milestones to complete the modernization, partially describe the work necessary to modernize the legacy system, and partially include plans for the disposition of the legacy system

^aThis includes users from the National Oceanic and Atmospheric Administration, which were no longer using System 2 as the financial system of record, as of fiscal year 2024.

Source: GAO analysis of agency documentation and interviews. | GAO-25-107795

The Department of Commerce’s System 2 is a financial management system that produces both financial and budget reports. It is used throughout the department to record and track customer charges and payments.

Commerce officials stated that they selected this system as one of its systems most in need of modernization because of the system’s business criticality and ubiquity and increasing risk to mission delivery. The system was acquired as a commercial off-the-shelf product in 1994 and has been modified to support the department’s business functions. The department’s financial systems have presented operation and maintenance challenges, including compliance with evolving federal requirements for financial management and higher costs associated with maintaining a duplicative IT infrastructure.

Commerce intends to replace the system by implementing a modernization program.³ The modernization program began around 2009 and initially was to deploy at three bureaus—the National Oceanic and Atmospheric Administration (NOAA), Census Bureau, and the National Institute of Standards and Technology (NIST). Due to challenges in developing the approach for the program, the department paused the program for 5 years, from 2013 until 2018. Commerce’s modernization plan, dated November 2020, included high-level milestones for implementing the modernization program and decommissioning the legacy systems in three phases, one phase for each of the three bureaus. However, this plan became outdated as the department experienced delays with the program. Commerce officials stated that the modernization program was deployed at NOAA in October 2023 (1 year later than original planned). Officials stated in February 2025, that they planned to deploy the modernization program at the Census Bureau in 2025 and at NIST in 2026.

Further, Commerce provided updated modernization plans, dated February 2025, that included details on the work needed to implement the modernization program at the Census Bureau, but did not include details for implementing the system at NIST. In addition, Commerce’s decommissioning plans, dated March 2023, included details for decommissioning the legacy system for NOAA, but not for the Census

³The modernization is also intended to replace other legacy systems at the department.

Bureau and NIST. Officials stated that detailed plans for modernizing the remaining phase would be developed once funding is identified, but did

that each bureau would develop more detailed decommissioning plans as they are undergoing the modernization program deployment, according to their phased approach.

While Commerce officials stated that they anticipated potential cost savings from modernizing System 2 by, for example, reducing maintenance and support costs, they did not have a specific estimate. Commerce officials also stated that the modernization would enable the use of a cloud system, instead of locally developed software on locally owned hardware as with the legacy system. This would enable zero trust implementation, simplify IT asset management for system components, and offer increased functionality in nearly all aspects of operation, especially reporting and data analysis.

System 3

Department of Defense—Defense Contract Management Agency and Defense Finance and Accounting Service

Initial year of implementation: 1964

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 cybersecurity risk (as determined by agency): Moderately high

Capable of implementing zero trust? No

Known cybersecurity vulnerabilities that cannot be remediated without modernization? Yes

Reported number of users: 13,322

Reported annual operating costs: \$8.7 million^a

Reported status of modernization: In progress; planned completion date not yet established

Reported cost of modernization: Approximately \$60–90 million

Potential cost savings: Approximately \$870,000–\$2.6 million annually

Other benefits: Enhanced system performance, reliability, and availability, among others

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

^aThese are costs for the Defense Contract Management Agency only and does not include the Defense Finance Accounting Service's labor to support the system.

Source: GAO analysis of agency documentation and interviews. | GAO-25-107795

The Department of Defense's (DOD) Defense Contract Management Agency and Defense Finance and Accounting Service's System 3 is the department's standard system for managing major defense acquisitions. The Defense Contract Management Agency and Defense Finance and Accounting Service use System 3 to administer and pay contracts issued to both domestic and foreign defense contractors.

System 3 was initially developed in 1964 and that technology and architecture remains largely in use today to support system capabilities. The current technology mainframe depends on obsolete programming languages, specifically COBOL and assembly language code.⁴ The last significant system upgrade was in 2005, which involved relocating the systems mainframe; however, the underlying technology and architecture remained largely the same. According to DOD officials, the system's technical infrastructure is reaching a state of obsolescence with limited skilled personnel and vendor expertise required for its continued sustainment. They further stated that although they currently have the IT skills needed to maintain the system, the average age of developers and technical subject matter experts on the system's team is above 60, putting the system at significant risk in being able to support and maintain it into the future. Officials also stated it is difficult to find COBOL and assembly language code developers and the learning curve once they are identified is also significant.

DOD has made attempts to modernize the system over the last 25 years. In March 2000, DOD announced that the system would be retired in October 2002 and it assembled an integrated conversion/closeout team in August 2000. However, DOD did not meet the October 2002 deadline and the system was not replaced due to challenges with the existing technologies and architectures in supporting complex system functions. DOD officials stated that since 2002, the system has undergone significant system changes within the application due to policy and regulation changes over the years, but there have not been significant changes or updates to the technology and architecture due to a lack of funding for modernizing the system. In 2016, DOD stood up a program

⁴Assembly 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 are also typically able to run only on the make of computer for which they were originally developed.

office under the Defense Contract Management Agency/Defense Finance and Accounting Service Joint Program Management Office.

System 3 was previously included in our 2019 list of 65 legacy systems most in need of modernization.⁵ Since then, officials stated that the program office completed an initial technical study in September 2024 to validate options to upgrade/refresh the system and provide acquisition and technical strategies for achieving critical stabilization. Since the recommendation from this study included automated code translation, the agency began a proof of concept to validate the use of tools to automate the translation of the system's current code base into a modern software language.

DOD officials also stated that the critical stabilization of the system would focus on (1) updating the current code base, (2) upgrading the current database model, and (3) migrating to a cloud computing environment. The officials further noted that stabilization could be accomplished within 2 to 3 years as funding is made available. However, they were not certain when the critical stabilization work would begin because they were unable to secure funding to start in fiscal year 2025; they are now aiming for fiscal year 2026.

DOD did not have a current modernization plan for System 3. According to department officials, they had a modernization plan in 2015, but because DOD did not fund the system modernization, the plans were never implemented and subsequently became outdated. Officials stated that the Defense Contract Management Agency/Defense Finance and Accounting Service team had attempted over the years to secure funding for modernization but was unable to secure funding due to other higher level department priorities. DOD officials further stated they would have an updated modernization plan for the system upon completion of the proof of concept discussed previously; however, they did not have an estimated time frame for completion.

DOD officials said that they expect to save approximately \$870,000 to \$2.6 million annually by the elimination of external applications currently needed to support system functionality. DOD officials reported that modernizing the system could result in (1) enhanced system performance and reliability by utilizing modern software development and testing tools,

⁵GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, [GAO-19-471](#) (Washington, D.C.: June 11, 2019) and concurrent limited official use only report GAO-19-351SU.

(2) improved system availability through the elimination of batch processing and flat files,⁶ (3) eliminated maintenance risks by adopting modern software languages to ensure programmers are available to support the system, (4) mitigated compliance and cybersecurity risks, and (5) improved time taken to make changes in support of department policies and regulations.

⁶A flat file is a database system in which each database contains only one file, which is not linked to any other file. Flat files are considered to be outdated technology.

System 4

Department of Energy
Initial year of implementation: Late 1990s
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): Moderate
System cybersecurity risk (as determined by agency): Moderate
Capable of implementing zero trust? No
Known cybersecurity vulnerabilities that cannot be remediated without modernization? Yes
Reported number of users: 14,000
Reported annual operating costs: \$4.4 million^a
Reported status of modernization: Not yet begun
Reported cost of modernization: Agency has not calculated
Potential cost savings: None
Other benefits: Increased functionality, cybersecurity, and faster product deployment into production, among others
Status of modernization plans: Agency does not have a modernization plan

^aThis includes costs for two additional interwoven applications. The department was unable to isolate the annual operating costs for the system.

Source: GAO analysis of agency documentation and interviews. | GAO-25-107795

The Department of Energy’s System 4 is a centralized data repository of personally identifiable information for all Energy employees and contractor staff.⁷ Several key applications of other systems are either centric to or interface with System 4, and numerous employees rely on these applications and the underlying data for managing the department-wide workforce. Additionally, System 4 is critical to payroll pre- and post-processing for all Energy employees.

Energy needs to modernize System 4 to address ongoing cybersecurity threats, and to support the legacy application as it becomes difficult and increasingly expensive to maintain. For example, some of the system’s applications use an obsolete programming language, COBOL. Officials from the Office of the Chief Financial Officer stated that they currently have the IT skills needed to maintain the system; however, it is extremely difficult to recruit COBOL programmers to support ongoing maintenance.

DOE intends to modernize the system’s desktop applications with web applications integrated with multi-factor authentication and to transition its monolithic application to a modern microservice architecture. The department intends to transform and modernize the applications in two groups.

Energy officials stated that they had prepared an initial modernization proposal in October 2023, but it was no longer viable. Officials stated that the department had requested funding through the fiscal year 2026 budget process, and they would update the modernization plan once funding was identified.

Although Energy does not anticipate cost savings, officials stated that modernizing System 4 would strengthen the department’s cybersecurity posture and enable it to better undertake future technology and business transformation. Officials also stated that modernizing the system would allow Energy to leverage intelligent cybersecurity tools; enhance scalability, flexibility, and faster product deployment into production, which would position the department to be better prepared for integration with future shared services for payroll processing; and enhance functionality and user experience.

⁷In general, personally identifiable information is any information that can be used to distinguish or trace an individual’s identity, such as name, date or place of birth, and Social Security number; or that otherwise can be linked to an individual.

System 5

Department of Health and Human Services—Indian Health Service
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 cybersecurity risk (as determined by agency): High
Capable of implementing zero trust? No
Known cybersecurity vulnerabilities that cannot be remediated without modernization? Yes
Reported number of users: 15,000
Reported annual operating costs: \$71 million^a
Reported status of modernization: In progress; planned completion end of fiscal year 2035
Reported cost of modernization: between \$4.0 and \$5.9 billion
Potential cost savings: Agency has not calculated
Other benefits: Avoiding cybersecurity risks, accessibility across locations, interoperability with other health care partners, and enhanced patient care
Status of modernization plans: Agency has documented modernization plans that partially include milestones to complete the modernization, partially describe the work necessary to modernize the legacy system, and partially include plans for the disposition of the legacy system

^aThis amount represents headquarters software development costs and required licensing only. It does not include hardware, software, and labor costs for federal, tribal, and urban health care facilities.

Source: GAO analysis of agency documentation and interviews. | GAO-25-107795

The Department of Health and Human Services’ (HHS) Indian Health Service’s (IHS) System 5 is a clinical and patient administrative information system that supports the full range of clinical and business operations at IHS, tribal, and urban Indian health facilities.

Officials from IHS’s Office of Information Technology stated that system modernization was necessary as it was operating with a highly vulnerable cybersecurity posture, is critical to the department’s mission, and is the agency’s oldest legacy system. The officials stated that System 5 is an aging system of systems that was originally implemented in 1969. System 5 is based on the MUMPS programming language.⁸ According to officials, IHS has relied on the originating agency’s expertise with the old programming language, but that expertise is dwindling with the transition away from the system. Further, officials stated that the system has reached an end-of-support status with the originating agency, necessitating its replacement. The department’s modernization business case stated that the current environment was no longer sustainable and did not provide patients or providers with the tools and functionality necessary to deliver a continuum of care.

This system was previously included in our 2019 list of the 10 most critical legacy systems in need of modernization. At that time, we found that HHS did not have a documented modernization plan for this system and made a recommendation for the department to develop a plan. The department implemented our recommendation by developing a plan dated March 2022, that included completed and future milestones, description of the work, and instructions for retirement of the system.

According to the plan, the department intended to transition from the legacy system with hundreds of locally managed databases at health care facilities nationwide to an enterprise electronic health record solution. According to an April 2024 program update, IHS selected a vendor to build, configure, and maintain the new enterprise electronic health records solution in November 2023. In addition, it planned to begin initial go-lives at pilot sites in late fiscal year 2025, followed by a multi-year rollout in cohorts that would end in fiscal year 2030. Further, the department planned to retire each instance of System 5 after the new solution is implemented at each site, and all system development and

⁸MUMPS was originally known as the Massachusetts General Hospital Utility Multi-Programming System. According to HHS officials, the programming language is highly vulnerable to cybersecurity exploitation and, with its last standard form approved 25 years ago, is considered both legacy and obsolete.

support would be concluded at the completion of the implementation phase, estimated for the end of fiscal year 2030.

In March 2025, agency officials stated that they are now expecting to complete the modernization in fiscal year 2035—5 years later than the original plan. However, they did not have updated plans that reflect the milestones and details for the new 2035 completion date and decommissioning of the legacy system. Officials stated that the schedule has had to be adjusted due to funding availability for the project. In addition, officials stated that a firm completion date on the effort will depend on how many tribal and urban Indian organization partners participate in implementing the solution. Officials further stated that the overall model and plan for the modernization initiative has not changed since the March 2022 plan, except for the schedule.

While IHS officials stated that they anticipated potential cost savings from modernizing the system, they did not have a specific estimate. Specifically, officials stated that they could avoid additional costs of locating specialized programming expertise and create savings by avoiding the technical burden and cybersecurity risks of an outdated system. Additionally, officials stated that modernizing to a system that is compatible with other like systems in the industry would help avoid indirect costs of data mapping, data conversion, and data storage when migrating to locations that use more updated systems. Further, officials stated that improvements in interoperability and care coordination could have positive impacts on patient access to care, care delivery, and health outcomes.

System 6

Department of Homeland Security—Office of Biometric Identity Management
Initial year of implementation: 1994
System hardware under warranty? No
Software vendor supported? Yes
Operating system(s) supported? Yes
Legacy programming language(s) used? No
System criticality (as determined by agency): High
System cybersecurity risk (as determined by agency): Moderate
Capable of implementing zero trust? Yes
Known cybersecurity vulnerabilities that cannot be remediated without modernization? Yes
Reported number of users: 6,700
Reported annual operating costs: \$156 million
Reported status of modernization: In progress; planned completion fourth quarter of fiscal year 2026
Reported cost of modernization: \$630 million
Potential cost savings: \$2 million per month
Other benefits: Support for increasing customer transaction volumes, storage requirements, and throughput speed; increased cybersecurity; and expanded interoperability with external biometric systems
Status of modernization plans: Agency has documented modernization plans that include milestones to complete the modernization, descriptions of the work necessary to modernize the legacy system, and plans for the disposition of the legacy system
Source: GAO analysis of agency documentation and interviews. | GAO-25-107795

The Department of Homeland Security’s (DHS) System 6 is used for biometric identity verification and determination and is operated and maintained by the Office of Biometric Identity Management.

Officials from DHS’s Office of Biometric Identity Management and OCIO stated that biometric identity management was one of two mission areas the department had prioritized for modernization.⁹ Officials also stated that the current legacy system contains deficiencies regarding storage capacity, scalability, complexity, and rising operations and maintenance costs that present challenges towards meeting key customer performance targets in the future. DHS officials further stated that modernization is needed to continue to provide biometric identity services to support the department’s goals and resolve critical system issues with the current system.

DHS intends to replace the legacy system by implementing increment 1 of a modernization program. Increment 1 is intended to establish the framework and system architecture, system components, and baseline system functionality and data, as well as decommission the legacy system. The department had documented modernization plans for increment 1 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. For example, according to a roadmap provided in August 2024, DHS planned to complete increment 1 by the fourth quarter of fiscal year 2026. The department also provided a disposition plan, dated May 2024, that addressed how the various components of the legacy system should be handled upon transitioning to the modernized system.

DHS officials stated that the projected cost savings for replacing System 6 is approximately \$2 million per month. Officials also said that benefits of the modernization include, among other things, fully addressing the risk of mission failure with the current system and achieving cost efficiencies for operations and maintenance. Further, they expect the system to provide support for increasing customer transaction volumes, storage requirements, and throughput speed; increased cybersecurity; and expanded interoperability with external biometric systems.

⁹Officials stated that the other mission area DHS prioritized for modernization was financial management.

System 7

Department of the Interior—Bureau of Reclamation

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 cybersecurity risk (as determined
by agency): Moderate

Capable of implementing zero trust? Not
applicable

Known cybersecurity vulnerabilities that
cannot be remediated without
modernization? Yes

Reported number of users: 46

Reported annual operating costs: \$2.3
million

Reported status of modernization: In
progress; planned completion August 2027

Reported cost of modernization: \$6.7
million

Potential cost savings: \$750,000 annually

Other benefits: Ability to adopt advanced
technologies and methodologies, and better
streamline operations

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

Source: GAO analysis of agency documentation and
interviews. | GAO-25-107795

Figure 2: Photograph of a Dam



Source: Department of Interior (photo). | GAO-25-107795

The Department of the Interior's Bureau of Reclamation's System 7 supports the remote operation of certain dams and power plants.

System 7 is approximately 23 years old and has not undergone a major system upgrade for 21 years. In July 2020, the system experienced a major failure and required a full system recovery. The project management plan states that several critical factors create a pressing need for replacing the current legacy system: limited support options, deteriorating and obsolete hardware, unsupported software, and a lack of interoperability in its hardware and software components with modern technology.

Additionally, according to Interior officials, the system contains legacy components, and multiple components are unable to receive software updates. Officials stated that the department is mitigating these risks through system isolation (i.e., it is not interconnected with other components or to the department's network or the internet). Further, according to a 2023 operational assessment, the authorization to operate for System 7 was revoked in August 2022 because of existing system security risks which were not addressed. Interior reported that

remediation actions were put into place to address these security risks, and conditional restoration of the system's authorization to operate was granted in September 2023, with requirements that needed to be met by March 2024. Officials further stated that they closed six of the highest priority plans of action and milestones by the March 2024 deadline, which improved the cybersecurity posture. They also said they established new deadlines for closing the remaining items by March 2025, when the current conditional authorization to operate was to expire.

This system was included in our June 2019 list of the 10 most critical legacy systems in need of modernization.¹⁰ At that time, we found that Interior had a documented modernization plan 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. We also reported that Interior had begun its modernization project in 2018 and it planned to complete the modernization project in 2020.

However, Interior officials have since stated that they had to terminate the system's contractor in April 2023 due to contractor nonperformance. Specifically, officials stated that they formed an internal investigative team due to the lack of contractor progress. They also said this team discovered multiple vulnerabilities, including cybersecurity deficiencies, inadequate administration, and incomplete contract specifications. According to officials, Interior had expended approximately \$4.2 million on the modernization of the system since 2018 and approximately \$2 million of that was paid toward the initial modernization contract that was terminated.

Further, Interior officials stated that they determined that the deliverables submitted by the terminated contractor were found to be inadequate for reuse. Specifically, officials said that key software components would likely require significant rework and the communication system did not comply with the agency's security standards and the equipment is now end of life.

In April 2024, Interior approved a new project management plan which included milestones and a description of the work necessary to complete the modernization. For example, the plan stated that the new project was to start in May 2024, construction of the new system was planned for

¹⁰[GAO-19-471](#) and concurrent limited official use only report GAO-19-351SU.

March 2025, and project completion was planned for August 2027—7 years later than originally planned. In January 2025, Interior developed a decommissioning plan for the legacy system. The plan included pre- and post-decommissioning requirements and detailed decommissioning activities.

Interior officials stated that they anticipated potential cost savings of \$750,000 annually once the system is modernized and the current specialized legacy support contract is no longer required. In addition, officials stated that modernizing the system would allow the department to adopt advanced technologies, methodologies, and implement best practices to streamline operations.

System 8

Department of Transportation—Federal Aviation Administration

Initial year of implementation: 1993

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): Moderately high

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

Capable of implementing zero trust? No

Known cybersecurity vulnerabilities that cannot be remediated without modernization? Yes

Reported number of users: 9,800

Reported annual operating costs: \$17.9 million^a

Reported status of modernization: In progress; planned completion 2030

Reported cost of modernization: Agency has not calculated

Potential cost savings: Agency has not calculated

Other benefits: Increased scalability, flexibility, and advanced data integration, among others

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

^aThis amount represents program management organization costs only and does not include technical operations costs.

Source: GAO analysis of agency documentation and interviews. | GAO-25-107795

The Department of Transportation’s Federal Aviation Administration’s (FAA) System 8 consists of 15 legacy aeronautical information systems. These systems support the collection, validation, management, and dissemination of aeronautical information.

For a previous report, FAA officials stated that its aging systems have been difficult to maintain due to the unavailability of parts and retirement of technicians with expertise in maintaining the aging systems.¹¹ In addition, there has been dramatic growth in airspace demand since the older systems were initially implemented. This has adversely impacted the ability of those systems to continue to support mission needs. Further, FAA officials stated that System 8 uses several legacy programming languages that it considers to be obsolete.

Officials stated that they adopted a multi-pronged strategy to modernize the system and mitigate risks, which included stabilizing the current system to improve reliability and developing a modernized solution.

However, FAA’s documented plans for the system modernization are incomplete. FAA developed a roadmap in August 2024 that included high-level milestones for implementing five modernization segments, from 2025 through 2030, but it did not describe the detailed work needed to modernize any of the systems. Additionally, the roadmap included time frames for decommissioning the systems, but they were very high-level. For example, the time frames bundled three to five systems together to show when they would collectively begin and end the decommissioning process (which could span for over 1 year), and did not specify any planned steps or whether the systems would be decommissioned all at once or sequenced over time. FAA officials stated that the roadmap was only intended to identify overall phases for the modernization, and that detailed work schedules and decommissioning plans would be developed with the vendor once a contract is awarded. However, they did not have a time frame for completion.

While FAA officials stated that they anticipated some potential cost savings from decommissioning legacy components that may have higher operational costs, they did not have a specific estimate. Officials also stated that the new solution’s capabilities and integration with broader aeronautical information management functions would enhance

¹¹GAO, *Air Traffic Control: FAA Actions Are Urgently Needed to Modernize Aging Systems*, [GAO-24-107001](#) (Washington, D.C.: Sept. 23, 2024).

operational efficiency and reliability, potentially leading to indirect cost benefits over time. Further, officials stated that modernizing the system would offer various benefits such as increased scalability, flexibility, and advanced data integration; enhanced user experience; and real-time data processing and intelligent automation.

System 9

Department of the Treasury—Internal Revenue Service
Initial year of implementation: 1965
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 cybersecurity risk (as determined by agency): Low
Capable of implementing zero trust? No
Known cybersecurity vulnerabilities that cannot be remediated without modernization? No
Reported number of users: No direct end users
Reported annual operating costs: \$331.8 million
Reported status of modernization: In progress; planned completion date not yet established
Reported cost of modernization: \$549 million^a
Potential cost savings: Agency has not calculated
Other benefits: Increased functionality, and improved processing time and data sharing
Status of modernization plans: Agency has documented modernization plans that partially include milestones to complete the modernization and partially describe the work necessary to modernize the legacy system; however, they do not include plans for the disposition of the legacy system
^aThis is the agency's initial estimated costs that was briefed to the Office of Management and Budget in December 2023. In April 2024, the program received an independent cost estimate from the Estimation Program Office of \$1.25 billion, which officials said was skewed higher because it assumed the modernization would have a larger scale and complexity. The agency plans to reconcile by refining the cost estimate to align with a more accurate scope for system modernization.
Source: GAO analysis of agency documentation and interviews. | GAO-25-107795

The Department of the Treasury’s Internal Revenue Service’s (IRS) System 9 is a batch file processing system that contains all tax data and related information pertaining to individual business income taxpayers. The system also reflects a continuously updated and current record of each taxpayer’s account.

According to IRS officials, System 9 is one of several systems the agency relies extensively on to carry out tax return processing and enforce tax laws. These systems were deployed in the 1960s and 1970s in the early days of computer mainframe tax processing data centers. Consequently, they consist of outdated technologies and are hosted in complex formats that over time have created substantial technical debt (e.g., hard coded business rules, decreasing skilled resources, and high effort for adding new features) for IRS. In addition, agency officials stated that the system depends on an obsolete programming language, assembly language code.

According to the agency, they intend to modernize the system by incrementally delivering value and moving to more timely and efficient account posting and settlement, while also enabling access to more consistent and comprehensive data for self-service and compliance. The program’s objectives aim to empower the agency to deliver modernized value faster, facilitate retirement of legacy systems, and concurrently deliver new features and legislative initiatives for business taxpayers.

According to agency officials, the system modernization is a 5-year initiative that began in November 2023. IRS approved a modernization plan in September 2024, which included milestones and the work necessary to modernize the legacy system from 2024 through 2026. For example, by the end of 2024, IRS planned to release a portal for employees to access system data and, by the end of 2026, modernize 50 percent of legacy code. However, the agency’s plans did not include any milestones or descriptions of the work necessary to complete the modernization beyond 2026, and did not include plans for the disposition of the legacy system following system modernization. IRS officials stated that they initially focused on delivering value as quickly as possible using an iterative and incremental approach. Thus, the agency initially developed a shorter-term roadmap outlining releasable features from 2024 through 2026. Officials stated that they are now shifting focus to future releases and further refining the plans to include releases for 2027 through 2029; however, they did not have an estimated time frame for completion.

IRS officials said that system modernization could potentially result in cost savings; however, they did not have a specific estimate. Officials also stated that modernizing the system has the potential to improve processing time and data sharing with other IRS systems and other agencies, and deliver increased functionality to business customers and taxpayers.

System 10

Department of the Treasury—Internal Revenue Service
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 cybersecurity risk (as determined by agency): Moderately low
Capable of implementing zero trust? No
Known cybersecurity vulnerabilities that cannot be remediated without modernization? No
Reported number of users: 75,000
Reported annual operating costs: \$15 million
Reported status of modernization: In progress; planned completion date not yet established
Reported cost of modernization: No estimate yet, but \$72 million is needed to develop a plan, prototypes, and investigational work
Potential cost savings: None
Other benefits: Elimination of legacy code, and improved integration with other tax processing systems
Status of modernization plans: Agency has documented modernization plans that partially include milestones to complete the modernization, descriptions of the work necessary to modernize the legacy system, and partially include plans for the disposition of the legacy system
Source: GAO analysis of agency documentation and interviews. | GAO-25-107795

The Department of the Treasury’s IRS’s System 10 provides for systemic review and consistency in case control, issues notices to taxpayers, and allows taxpayers to see the status of refunds.

According to the agency, System 10 is one of several systems the IRS relies extensively on to deliver customer services for tax return processing and to enforce tax laws. These systems were deployed in the 1960s and 1970s in the early days of computer mainframe tax processing data centers. Consequently, they consist of outdated technologies and are hosted in complex formats that over time have created substantial technical debt (e.g., hard coded business rules, decreasing skilled resources, and high effort for adding new features) for IRS. In addition, agency officials stated that the system depends on an obsolete programming language, COBOL.

While IRS developed the system’s retirement strategy in January 2022 that included the current and target state of capabilities that are to be modernized, this strategy did not include specific time frames. For example, the strategy included roadmaps detailing how the components of the capabilities would be modernized and decommissioned across nine releases, but the roadmaps did not include specific dates or identify the duration of a release. Officials stated that they have not yet established plans with specific dates because they are performing an analysis to identify a cost-effective path for delivering tax services. However, they did not have an estimated time frame for completion.

Officials stated that they did not anticipate cost savings from modernizing the system. They expect that modernizing and expanding existing system capabilities to meet the growing needs of IRS’s future state architecture and continuing support and expansion of those capabilities going forward will likely have a cost structure greater than the existing legacy application. The modernization of System 10 is expected to eliminate millions of lines of legacy code by modernizing the system to act as a central hub for case management, account management, and customer management functions. The modernized solution is also expected to integrate seamlessly with other IRS systems to enable a more digitally forward experience for customer service representatives and others who require access to case information.

System 11

Environmental Protection Agency
Initial year of implementation: 1973
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 cybersecurity risk (as determined by agency): Moderate
Capable of implementing zero trust? No
Known cybersecurity vulnerabilities that cannot be remediated without modernization? Yes
Reported number of users: 54
Reported annual operating costs: \$1.6 million
Reported status of modernization: In progress; planned completion first quarter of fiscal year 2028
Reported cost of modernization: \$2.5 million^a
Potential cost savings: \$166,000 annually
Other benefits: Increased security posture, minimized risks to availability and integrity of data, and improved monitoring of the network
Status of modernization plans: Agency has documented modernization plans that include milestones to complete the modernization, descriptions of the work necessary to modernize the legacy system, and plans for the disposition of the legacy system
^aAgency officials stated that they received \$2.5 million from the Technology Modernization Fund for modernizing the system.
Source: GAO analysis of agency documentation and interviews. | GAO-25-107795

The Environmental Protection Agency’s (EPA) System 11 enables the continuous monitoring and near real-time measurement of gamma radiation, which allows EPA scientists to detect any unusual changes.

EPA’s 2023 modernization plan for the system stated that it has historically been underfunded for hardware and software modernization, automated IT management and monitoring toolsets, and technical skillsets to address cybersecurity and network challenges. According to EPA’s 2021 analysis of alternatives for System 11, the legacy hardware (workstations and servers) was over 8 years old at the time, the scientific instruments were unable to upgrade their operating systems, it was operating on old database software, and some of the software had been internally developed and was supported by a retirement-eligible primary developer.

EPA’s modernization plan for the system, approved in March 2023, included milestones to complete the modernization and descriptions of the work necessary to modernize the legacy system. For example, the plans included implementing a firewall solution by the first quarter of fiscal year 2025. By the fourth quarter of fiscal year 2025, EPA planned to replace antiquated workstations to eliminate frequent hardware failures. Further, EPA planned to implement a vendor-supported, commercial off-the-shelf system to address future critical support concerns by the fourth quarter of fiscal year 2026. In February 2025, EPA approved plans for the disposition of the legacy system. The plan included details and time frames for decommissioning activities, noting that it should be completed by the first quarter of fiscal year 2028.

EPA officials stated that they estimated potential cost savings of about \$166,000 annually in licensing it would no longer need to acquire because the system would connect to EPA’s Wide Area Network that would allow the use of existing enterprise licensing. In addition, the modernization would increase the security posture, minimize risks to the radiation data, and increase the reliability and integrity of system data provided to the public website, among other things. The agency also stated that the implementation of a controlled access interface network solution could allow them to monitor all incoming traffic and use additional enterprise resources.

Appendix V: Comments from the Department of Defense



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

JUN 9 2025

Mr. Kevin Walsh
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Walsh,

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-25-107289SU, "INFORMATION TECHNOLOGY: Agencies Need to Plan for Modernizing Critical Decades-Old Legacy Systems," dated April 24, 2025 (GAO Code 107289). The department concurs with the content of the draft report. Enclosed is the detailed comment on the report recommendation.

The Department appreciates the opportunity to review this report. Mr. point of contact for this matter is Ms. Amanda Villwock, amanda.j.villwock.civ@mail.mil, (571) 372-4455.

Sincerely,

A handwritten signature in blue ink, appearing to read "K. Arrington", is located below the "Sincerely," text.

Katherine Arrington
Performing the Duties of the
Chief Information Officer of the
Department of Defense

Enclosure:
As stated

Appendix VI: Comments from the Department of Energy



Department of Energy
Washington, DC 20585

June 16, 2025

Kevin Walsh
Director, Information Technology
& Cybersecurity Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Kevin Walsh,

The Department of Energy (DOE or Department) appreciates the opportunity to provide a response to the Government Accountability Office's (GAO) Draft Report titled, *Information Technology: Agencies Need to Plan for Modernizing Critical Decades-Old Legacy Systems* (GAO-25-107289). DOE concurs with the one (1) recommendation listed in the report and plans to achieve compliance with OMB requirements where technically feasible by December 31, 2026.

GAO should direct any questions to Sandra Logan, Acting Deputy Chief Information Officer for Enterprise IT Policy and Governance at Sandra.logan@hq.doe.gov.

Sincerely,

DAWN
ZIMMER

Digitally signed by DAWN
ZIMMER
Date: 2025.06.16 10:44:04
-04'00'

Dawn Zimmer
Principal Deputy Chief Information Officer

Enclosure



Printed with soy ink on recycled paper

MANAGEMENT RESPONSE

GAO Draft Report,

*Information Technology: Agencies Need to Plan for Modernizing Critical Decades-Old Legacy
Systems GAO-25-107289*

Recommendation 4: The Secretary of Energy should direct the department CIO to document the department's modernization plans for its [REDACTED] system, to include milestones, a description of the work necessary to modernize the system, and details on the disposition of the legacy system.

Management Response: Concur

The [REDACTED] system has been in operation for over 25 years and is currently utilizing actively supported, cloud-based technology.

As part of a broader effort to modernize DOE's human capital IT, the management and support of the subject systems has recently been transferred from the DOE Office of the Chief Financial Officer to the DOE Office of the Chief Information Officer's (OCIO). Due to staff and organizational changes, the OCIO is in the process of revising its modernization strategy. We, along with the OCFO and Office of the Chief Human Capital Office (OCHCO), are actively migrating several functions with significant system dependencies on [REDACTED] to the Workday Software as a Service (SaaS) platform. This migration is scheduled for completion by December 31, 2026.

Following the completion of migration, the OCIO will undertake a formal modernization planning approach to address the remaining functions and dependent systems. In the interim, the [REDACTED] system hardware and software is continuously maintained with the latest patches and updates, in accordance with current System Security Plans (SSPs) and the Program Cyber Security Plan (PSCP).

Estimated Completion Date: December 31, 2028

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



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

May 23, 2025

Kevin Walsh
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Walsh:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, **"INFORMATION TECHNOLOGY: Agencies Need to Plan for Modernizing Critical Decades-Old Legacy Systems"** (GAO-25-107289SU and GAO-25-107795).

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

Sincerely,

Mitchell Hailstone

Mitchell Hailstone
Acting Assistant Secretary for Legislation
and
Principal Deputy Assistant Secretary

Attachment

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT - INFORMATION TECHNOLOGY: AGENCIES NEED TO PLAN FOR MODERNIZING CRITICAL DECADES-OLD LEGACY SYSTEMS (GAO-25-107289SU and GAO-25-107795)

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

GAO Recommendation 5:

The Secretary of Health and Human Services should direct the department CIO to include in the department's modernization plans for the relevant system, all milestones to complete the modernization, a description of all the work necessary to modernize the system, and all details on the disposition of the legacy system.

HHS Response:

HHS considers this action open.

The HHS Office of the Chief Information Officer (OCIO) continues to work with the Indian Health Service (IHS) to refine and execute modernization plans consistent with the observations and recommendations made as part of this engagement. This includes the development and implementation of all milestones necessary to undertake the relevant system modernization, and plans that provide greater insight on the disposition of the legacy system itself.

Appendix VIII: Comments from the Social Security Administration



SOCIAL SECURITY
Office of the Commissioner

May 23, 2025

Kevin Walsh
Director, Information Technology and Cybersecurity
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Director Walsh,

Thank you for the opportunity to review the draft report "Information Technology: Agencies Need to Plan for Modernizing Critical Decades-Old Legacy Systems" (GAO-25-107289SU). We continue to evaluate our legacy systems and make efforts to modernize and enhance them in accordance with our budgetary considerations. Our overarching goal is to improve Agency systems for the efficiency of our processes and ensure program integrity.

Please contact me at (410) 965-2611 if I can be of further assistance. Your staff may contact Amy Gao, Director of the Audit Liaison Staff, at (410) 966-1711.

Sincerely,

A handwritten signature in black ink, appearing to read "Chad Poist", written over a horizontal line.

Chad Poist
Chief of Staff

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Appendix IX: GAO Contact and Staff Acknowledgments

GAO Contact

Kevin Walsh, walshk@gao.gov

Staff Acknowledgments

In addition to the individual named above, the following staff made key contributions to this report: Jeanne Sung (Assistant Director), Paige Teigen (Analyst-in-Charge), Jillian Clouse, Becca Eyler, Hiama Halay, Kim LaMore, Jessica Steele, and Walter Vance.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [X](#), [LinkedIn](#), [Instagram](#), and [YouTube](#).
Subscribe to our [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

A. Nicole Clowers, Managing Director, CongRel@gao.gov

General Inquiries

<https://www.gao.gov/about/contact-us>



Please Print on Recycled Paper.