United States Government Accountability Office

Testimony

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

For Release on Delivery
Expected at 10:00 a.m. ET
Wednesday, May 31, 2023

INFORMATION TECHNOLOGY

DHS Needs to Continue Addressing Critical Legacy Systems

Statement of Kevin Walsh, Director, Information Technology and Cybersecurity

GAO-23-106853

GAO Highlights

Highlights of GAO-23-106853, a testimony before the Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Each year, the federal government spends more than $100 billion on IT and cyber-related investments. Of this amount, agencies have typically reported spending about 80 percent on operations and maintenance of existing IT, including legacy systems. DHS's expected IT spending for fiscal year 2023 is about $10.1 billion; operations and maintenance is expected to consume about $8.8 billion of that total.

Maintaining legacy systems (i.e., systems that are outdated or obsolete) can pose significant challenges. GAO reported in 2016 that agencies had system components that were at least 50 years old and vendors that were no longer providing support for hardware or software. In 2019, GAO reported that several critical federal legacy systems used outdated languages, had unsupported hardware and software, and were operating with known security vulnerabilities.

GAO was asked to testify on its past legacy system reports and DHS's efforts to modernize. Specifically, GAO summarized (1) DHS's critical legacy IT systems and plan for modernizing and (2) progress and challenges with selected DHS IT modernizations. This statement is based on issued GAO reports and updated information on the department's implementation of GAO's recommendations.

What GAO Recommends

In a 2019 report, GAO recommended to DHS that it develop a modernization plan for its most critical legacy system. The department implemented this recommendation and has implemented several GAO recommendations on modernizing other legacy systems.

View GAO-23-106853. For more information, contact Kevin Walsh at (202) 512-6151 or walshk@gao.gov.

May 31, 2023

INFORMATION TECHNOLOGY

DHS Needs to Continue Addressing Critical Legacy Systems

What GAO Found

GAO reported in June 2019 that, of the 65 critical legacy IT systems identified by federal agencies as needing modernization, the Department of Homeland Security (DHS) had three such systems (see table). Further, GAO identified DHS's System 4 as one of the 10 most critical legacy systems across the federal government in need of modernization.

Table: Critical Legacy Systems in Need of Modernization According to DHS, as of June 2019

System name[a]	Age of system, in years	Age of oldest hardware, in years	System criticality (according to DHS)	Security risk (according to DHS)
System 4	8-11	11	High	High
System L	9	2	High	Moderately low
System M	6	1	High	Low

Source: GAO analysis of Department of Homeland Security (DHS) data. | GAO-23-106853

[a]Due to sensitivity concerns, GAO substituted alphanumeric identifiers for the names of the agencies' systems. GAO assigned a number to identify each of the 10 most critical legacy systems in need of modernization and assigned a letter to identify the remaining 55 systems. The identifiers in the table reflect how DHS's system names appeared in the 2019 report (GAO-19-471).

In evaluating agencies' modernization plans for the 10 most critical legacy systems, GAO determined that DHS lacked a complete plan for modernizing System 4. Specifically, DHS's plan did not include milestones to complete the modernization and did not describe the planned disposition of the existing legacy system. In February 2022, DHS provided an updated modernization plan that included milestones for replacing the system and removing legacy hardware, which addressed our recommendation. By documenting its plan in sufficient detail, DHS increased the likelihood that the modernization will succeed.

GAO has also previously reported on DHS's efforts to modernize and replace other legacy systems that support financial management, biometric identity management, and grants management. Specifically,

- In February 2023, GAO noted that, after attempting to modernize its financial management systems for decades, DHS implemented a governance structure to oversee component-level financial systems modernizations. However, the Coast Guard was unable to declare full operational capability as expected because it had not remediated issues from operational testing.
- In June 2021, GAO reported that DHS's Homeland Advanced Recognition Technology program (intended to replace an outdated system for biometric identity management) was significantly behind schedule and had exceeded its estimated costs. GAO also found that DHS had not fully addressed key risk management and IT acquisition practices.
- In April 2019, GAO reported that the Federal Emergency Management Agency's Grants Management Modernization program (intended to replace 10 legacy systems) had not fully addressed leading practices for business process reengineering, requirements, and cybersecurity risk management. The program also did not meet leading practices for a reliable schedule.

DHS has now implemented 11 of the 19 recommendations GAO made in these reports. Implementing the remaining eight will help the department ensure these critical legacy systems are successfully replaced.

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

I am pleased to participate in today's hearing on the Department of Homeland Security's (DHS) legacy IT systems. Each year, the federal government spends more than $100 billion on IT and cyber-related investments. Of this amount, agencies have typically reported spending about 80 percent on the operations and maintenance of existing IT investments, including legacy systems.[1] DHS's expected IT spending for fiscal year 2023 is about $10.1 billion; operations and maintenance is expected to consume about $8.8 billion of that total.

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 and had vendors that were no longer providing support for hardware or software.[2] Likewise, in June 2019, we reported that several of the federal government's most critical legacy systems used outdated programming languages, had unsupported hardware and software, and were operating with known security vulnerabilities.[3]

As you requested, my testimony today discusses DHS's efforts to modernize its legacy IT systems. Specifically, it summarizes (1) DHS's critical legacy IT systems and plan for modernizing and (2) progress and challenges with selected DHS IT modernizations. This statement is based on issued GAO reports and updated information on the status of the department's implementation of GAO recommendations. Detailed information on the objectives, scope, and methodology for the issued reports can be found in the reports cited in this statement.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate

[1]The provisions commonly referred to as the Modernizing Government Technology (MGT) Act define a legacy IT system as a system that is outdated or obsolete. National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Div. A, Title X, Subtitle G, § 1076(8), 131 Stat. 1586, 1587 (2017).

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

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

evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Historically, the federal government has had difficulties acquiring, developing, and managing IT investments. As a result of these difficulties, we identified "Improving the Management of IT Acquisitions and Operations" as a high-risk area in 2015.[4] We designated DHS's management functions as high risk in 2003, and most recently narrowed the high risk area to "Strengthening DHS IT and Financial Management Functions" in 2023. Further, federal agencies have struggled with appropriately planning and budgeting for modernizing legacy systems, upgrading underlying infrastructure, and investing in high quality, lower cost service delivery technology. The consequences of not updating legacy systems has contributed to, among other things, security risks, unmet mission needs, staffing issues, and increased costs.

- **Security risks.** Legacy systems may operate with known security vulnerabilities that are either technically difficult or prohibitively expensive to address. In some cases, vendors no longer provide support for hardware or software, creating security vulnerabilities and additional costs. For example, in October 2017, the Office of Personnel Management's (OPM) Office of the Inspector General reported that the agency's IT environment contained many instances of unsupported software and hardware, where the vendor no longer provided patches, security fixes, or updates for the software.[5] The report noted that as a result, there was increased risk that OPM's IT environment contained known vulnerabilities that would never be patched and could have been exploited to allow unauthorized access to data.

[4]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 two years, we issue an update that describes the status of these high-risk areas and actions that are still needed to assure further progress and identifies new high-risk areas needing attention by Congress and the executive branch. We continue to identify this area as high risk. GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas,* GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

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

Additionally in November 2017, the Department of Education's Inspector General identified security weaknesses that included the department's use of unsupported operating systems, databases, and applications.[6] By using unsupported software, the department put its sensitive information at risk, including the personal records and financial information of millions of federal student aid applicants.[7]

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

- **Unmet mission needs.** Legacy systems may not be able to reliably meet mission needs because they are outdated or obsolete. For instance, in 2016, the Department of State's Inspector General reported on the unreliability of the Bureau of Consular Affairs' legacy systems.[9] Specifically, during the summers of 2014 and 2015, outages in the legacy systems slowed and, at times, stopped the processing of routine consular services such as visa processing. For example, in June 2015, system outages caused by a hardware failure halted visa processing for 13 days, creating a backlog of 650,000 visas.

  Additionally, in January 2023, we reported that the IRS' 60-year old system for individual tax data, the Individual Master File (IMF), needed to be modernized to help address business and technical challenges. Such challenges included the inability to get a real-time view of the taxpayer's account and provide additional information to combat fraud and identity theft. We reported that the IRS had

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

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

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

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

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

- **Staffing issues.** In order to operate and maintain legacy systems, staff may need experience with older technology and programming languages, such as the Common Business Oriented Language (COBOL).[10] Agencies have had difficulty finding employees with such knowledge and may have to pay a premium for specialized staff or contractors. For example, we reported in May 2016 that the Social Security Administration (SSA) had to rehire retired employees to maintain its COBOL systems.[11]

  In addition, having a shortage of expert personnel available to maintain a critical system creates significant risk to an agency's mission. For instance, we reported in June 2018 that the IRS was experiencing shortages of staff with the skills to support key tax processing systems that used legacy programming languages.[12] These staff shortages not only posed risks to the operation of the key tax processing systems, but they also hindered the agency's efforts to modernize its core tax processing system.

  Further, having a shortage of personnel with necessary expertise can lead to delays in modernizing legacy systems. As we reported in February 2022, OPM's legacy financial system, Trust Funds Federal Financial System, was outdated and consisted of unsupported software. In fiscal year 2017, OPM created the Trust Funds

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

[11]GAO-16-468.

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

Modernization Program to replace the legacy system. However, OPM had to extend the planned completion date of two project milestones by one year. OPM attributed the delay to a variety of reasons, including insufficient staff expertise regarding the legacy system.[13]

- **Increased costs.** The cost of operating and maintaining legacy systems increases over time. The issue of cost is linked to security risks, unmet mission needs, and staffing issues. Further, in an era of constrained budgets, the high costs of maintaining legacy systems could limit agencies' ability to modernize and develop new or replacement systems.

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

As we reported in June 2019, agencies cited several factors they consider prior to deciding whether to modernize a legacy system.[15] In particular, they reported evaluating factors such as the inherent risks, the criticality of the system, the associated costs, and the system's operational performance.

- **Risks.** Agencies may prioritize the modernization of legacy systems that have security vulnerabilities or software that is unsupported by the vendor.[16] However, limited system accessibility may also reduce the need to modernize a legacy system. For example, air-gapped

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

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

[15]GAO-19-471.

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

systems, which are systems that are isolated from the internet, may mitigate a legacy system's cybersecurity risk by preventing remote hackers from having system access.[17]

Conversely, we have also reported that air-gapped systems are not necessarily secure; they could potentially be accessed by other means than the internet, such as through Universal Serial Bus (known as USB) devices.[18] Even so, removing the threat of remote access is a mitigation technique used by agencies such as the Nuclear Regulatory Commission (NRC). According to NRC, the agency reduced the riskiness of using computers with unsupported operating systems by putting these computers on isolated networks or by disconnecting them from networks entirely.

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

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

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

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

and maintenance costs due to efficiencies gained through the modernization.

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

Executive Branch and Congress Have Made Efforts to Modernize Federal IT

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

- **National Cybersecurity Strategy.** In March 2023, the President released a strategy to elevate the cybersecurity posture of the federal government.[19] The strategy indicated that the Office of Management and Budget (OMB) would lead development of a multi-year plan to accelerate technology modernization. The plan would prioritize federal efforts on eliminating legacy systems that are costly to maintain and difficult to defend against sophisticated cyber threats. Specifically, the plan is to identify milestones to remove all legacy systems incapable of implementing the zero trust architecture strategy within a decade, or otherwise mitigate risks to those that cannot be replaced in that timeframe.[20]
- **Identification of High Value Assets.** In December 2018, OMB issued a memorandum that provided guidance regarding the establishment and enhancement of the High Value Asset program.[21] It stated that the program is to be operated by DHS in coordination with

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

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

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

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.[22]

- **Enactment of provisions commonly referred to as the Modernizing Government Technology (MGT) Act.** In December 2017, Congress and the President enacted a law to authorize the availability of funding mechanisms to improve, retire, or replace existing IT systems to enhance cybersecurity and to improve efficiency and effectiveness. The law, known as the MGT Act, authorizes agencies to establish working capital funds for use in transitioning from legacy systems, as well as for addressing evolving threats to information security.[23] The law also created the Technology Modernization Fund, from which agencies can obtain funds to retire and replace legacy systems, as well as acquire or develop systems.

  Subsequently, in February 2018, OMB issued guidance for agencies to implement the MGT Act.[24] The guidance was intended to provide agencies additional information regarding the Technology Modernization Fund, and the administration and funding of the related IT working capital funds. Specifically, the guidance allowed agencies to begin submitting initial project proposals for modernization on February 27, 2018.

  In addition, in accordance with the MGT Act, the guidance provides details regarding a Technology Modernization Board, which is to consist of (1) the Federal Chief Information Officer (CIO) (Chair); (2) a senior official with IT development technical expertise from the General Services Administration; (3) a member of DHS's National

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

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

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

Protection and Program Directorate;[25] and (4) four federal employees with technical expertise in IT development, financial management, cybersecurity and privacy, and acquisition, appointed by the Director of OMB.[26]

Congress initially appropriated $175 million in no-year funding to the Technology Modernization Fund through the annual appropriations process. On March 11, 2021, Congress and the President enacted legislation that appropriated an additional $1 billion to be available until September 30, 2025, to carry out the purposes of the fund.[27] 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 Management Board had approved 40 projects across 24 federal agencies, totaling about $713 million, as of May 2023.[28] For example, the board approved about $13.9 million for the Department of Housing and Urban Development (HUD) to modernize a mainframe and five COBOL-based applications that were expensive to maintain. According to OMB's website, the investment began in August 2018 and was closed out in August 2022, with no reported cost overruns and projected savings of about $8 million annually. According to HUD, securing these funds served as a catalyst inside the department and led to gathering strong support for this project.

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

[26]As of May 2023, these four employees were (1) the Federal Deposit Insurance Corporation's CIO, who is also the Chief Privacy Officer and Director of the Division of Information Technology; (2) the National Archives and Records Administration's CIO; (3) the National-Geospatial Intelligence Agency's Chief Technology Officer; and (4) the United States Digital Service's Administrator.

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

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

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

However, we reported in December 2021 that, for numerous Technology Modernization Fund projects, agencies had yet to realize any cost savings, narrowed their respective projects' scopes resulting in reduced award amounts, and continued to use unreliable cost estimates.[29] We stated that, given the significant expansion in available funds, it was increasingly important for OMB and the General Services Administration to implement our prior recommendations from December 2019. This included developing and implementing a plan to fully recover operating expenses with fee collection and developing detailed cost estimating guidance.[30]

DHS Identified Three Legacy Systems and Developed a Modernization Plan for Its Most Critical System

In June 2019, we summarized 65 systems that the 24 Chief Financial Officers Act of 1990 agencies identified as their critical legacy systems in need of modernization.[31] Of the 65 systems, DHS identified three legacy systems in need of modernization and, at the time, these systems were about 6-11 years old.

Table 1 provides a list of the critical legacy systems that DHS identified, as of June 2019, as well as agency-reported system attributes, including the system's age, hardware's age, system criticality, and security risk. Due to sensitivity concerns, we substituted alphanumeric identifiers for the system names and are not providing detailed descriptions. The identifiers in table 1 reflect how DHS's system names appeared in the

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

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

[31]GAO-19-471.

2019 report. GAO identified System 4 as one of the 10 most critical legacy systems in need of modernization.[32]

Table 1: Critical Legacy Systems in Need of Modernization According to DHS as of June 2019

System name[a]	Age of system, in years	Age of oldest hardware, in years	System criticality (according to DHS)	Security risk (according to DHS)
System 4	8–11[b]	11	High	High
System L	9	2	High	Moderately low
System M	6	1	High	Low

Source: GAO analysis of Department of Homeland Security (DHS) data. | GAO-23-106853

Legend:

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

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

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

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

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

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

[a]Due to sensitivity concerns, we substituted an alphanumeric identifier for the system names. We assigned a number to identify each of the 10 most critical legacy systems in need of modernization and we assigned a letter or letters to identify the remaining 55 systems. The identifiers reflect how DHS's system names appeared in the 2019 report (GAO-19-471).

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

Given the age of the hardware and software in legacy systems, the systems' criticality to agency missions, and the security risks posed by operating aging systems, it is imperative that agencies carefully plan for their successful modernization. Documenting modernization plans in sufficient detail increases the likelihood that modernization initiatives will succeed. Our review of government and industry best practices for the

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

modernization of federal IT[33] stressed that agencies should have documented modernization plans for legacy systems that, at a minimum, include three key elements: (1) milestones to complete the modernization, (2) a description of the work necessary to modernize the legacy system, and (3) details regarding the disposition of the legacy system.

In June 2019, we evaluated agencies' modernization plans for the 10 most critical legacy systems. DHS was among eight agencies that lacked complete plans for modernizing their respective systems. Specifically, DHS's modernization plan for System 4 did not include milestones to complete the modernization or describe the planned disposition of the existing legacy system. Accordingly, we made a recommendation to DHS in a "limited official use only" version of the report to identify and document a modernization plan for this legacy system. In February 2022, DHS provided an updated modernization plan that included milestones for implementing the replacement system and removing legacy hardware, which addressed our recommendation. By documenting its plan in sufficient detail, DHS increased the likelihood that this modernization will succeed.

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

DHS Made Progress in Addressing IT Modernization Recommendations, but Experienced Challenges in Meeting Program Goals

In the past several years, we reported on DHS's efforts to modernize and replace legacy systems that support various mission-critical activities, including financial management, biometric identity management, and grants management.[34] Although DHS made progress by fully implementing 11 of 19 recommendations we made to help improve these modernization efforts, all three modernizations experienced challenges in meeting program goals. For example, all three modernizations experienced significant schedule delays up to several years. Further, some of the programs experienced cost overruns, performance issues, or had past modernization attempts that were not successful.

- ***DHS Financial Management.*** In February 2023, we reported that DHS has faced significant internal control and financial management systems deficiencies since the department's creation in 2003.[35] To address its financial management issues, DHS has attempted to develop a department-wide integrated and comprehensive financial management system for decades. In 2014, DHS began its third financial management system modernization attempt, which consisted of a decentralized, component-level approach.[36] We reported that DHS defined and implemented a tiered governance structure to provide oversight of its financial systems modernization programs, developed plans for modernizing specific financial systems, and established a process for lessons learned.

  For example, the Coast Guard deployed its new financial management system in December 2021 as part of a $510 million modernization program, and declared initial operational capability in June 2022. However, as we reported in February 2023, the Coast Guard was not able to declare full operational capability as expected

[34]GAO, *DHS Financial Management: Actions Needed to Improve Systems Modernization and Address Coast Guard Audit Issues,* GAO-23-105194, (Washington, D.C.: Feb. 28, 2023); *Homeland Security: DHS Needs to Fully Implement Key Practices in Acquiring Biometric Identity Management System,* GAO-21-386, (Washington, D.C.: June 8, 2021); *FEMA Grants Modernization: Improvements Needed to Strengthen Program Management and Cybersecurity,* GAO-19-164, (Washington, D.C.: Apr. 9, 2019).

[35]GAO-23-105194.

[36]In fiscal year 2004, DHS first planned to develop an integrated and comprehensive financial management system department-wide. In fiscal year 2014, DHS revised its approach to focus its modernization efforts at the component level. In fiscal year 2018, DHS started to transition three components to a new financial management system, Financial Systems Modernization Solution (FSMS). These three components included Countering Weapons of Mass Destruction Office, Transportation Security Administration, and Coast Guard, and this effort is referred to as the Financial Systems Modernization (FSM)-Trio program.

in December 2022. Although DHS identified, documented, and tracked metrics to assess the Coast Guard's system deployment, the department found that the system was not achieving expected capabilities. This was because the agency did not address and remediate known issues identified in operational testing. DHS's subsequent operational testing and evaluation of the system found that it was not effective, responsive, or reliable, and therefore could not proceed to full operational capability. In April 2023, DHS approved the Coast Guard's remediation plan to address outstanding issues. Based on this schedule, the program office expected to submit a revised acquisition program baseline in February 2024.

Additionally, FEMA and U.S. Immigration and Customs Enforcement (ICE) were in the planning phases of their financial systems modernization efforts. In November 2022, DHS awarded contracts for software licenses and planned to award contracts for system integration services for these components. Resolving deficiencies identified by testing before proceeding to the next phase in the acquisition process can help reduce the risk that future system modernization efforts at FEMA and ICE will not meet mission needs or expected capabilities. We made four recommendations to address these issues. DHS concurred and described actions it has taken and would take to address them.

- ***DHS Biometric Identity Management.*** In June 2021, we reported that DHS was using an outdated system for providing biometric identity management services (i.e., fingerprint matching and facial recognition technology services).[37] This system, known as the Automated Biometric Identification System or IDENT, became operational in 1994 and was to be replaced by a multi-billion dollar program known as the Homeland Advanced Recognition Technology (HART), which was initiated in 2016. We reported that DHS had initially expected to implement the entire program by 2021; however, no segments had been deployed by 2021. The program was estimated to cost about $4.3 billion and DHS planned to deploy the first increment in December 2021, and later increments in 2022 and 2024.

  Although the program had suffered continuing delays, the DHS CIO did not update the evaluation it had provided in November 2019, and continued to report the program as low risk on the IT Dashboard, a website showing, among other things, the performance and risks of

[37]GAO-21-386.

agency IT investments. In May 2020, the Office of the CIO began developing a new quarterly process for assessing program risk, which led to the CIO elevating HART's rating from low to high risk and reporting this rating to the IT Dashboard in November 2020. Though we found that the DHS CIO fulfilled applicable oversight requirements for high-risk IT programs by, among other things, conducting a TechStat review of HART, we concluded that the department's associated policy was outdated and not consistent with the processes the CIO was actually using.[38]

DHS had also implemented four of seven risk management best practices and partially implemented the remaining three. Further, of 14 selected IT acquisition best practices related to agreement management, project monitoring and control, and requirements management, DHS fully implemented seven and partially implemented the remaining seven. Accordingly, we made a total of seven recommendations to DHS, four of which have been fully implemented. Until DHS addresses the remaining three recommendations regarding monitoring contractor work products, program costs, and stakeholder involvement, the department risks experiencing further schedule delays and cost overruns. Additionally, DHS risks developing a system that may not meet its needs or those of its partner agencies.

In April 2023, we reported that HART had breached its cost and schedule goals in 2020 due to technical challenges and rework resulting from an overly complex, high-risk design, and disagreements with the contractor on program requirements.[39] DHS approved a new baseline for the program in May 2022, which focused on achieving initial operational capability by September 2023 (about 4 years later than originally planned).[40] Initial capabilities were to consist of the infrastructure necessary to operate HART as the biometric services system of record and the decommissioning of the legacy IDENT system. The program's full operational capability date was also

[38]A TechStat review is an evaluation of high-risk IT investments to determine whether to terminate or turn around investments that are in danger of failing or are not producing results.

[39]GAO, *DHS Annual Assessment: Major Acquisition Programs Are Generally Meeting Goals, but Cybersecurity Policy Needs Clarification,* GAO-23-106701, (Washington, D.C.: Apr. 20, 2023).

[40]We have ongoing work reviewing the reliability of the HART program's 2022 cost and schedule estimates.

delayed, from September 2021 to an unknown date that would be determined when DHS begins planning for future HART capabilities in 2023.

- ***FEMA Grants Management.*** In April 2019, we reported that FEMA initiated the Grants Management Modernization (GMM) program in 2015 to streamline and modernize its complex grants management IT environment.[41] That environment supported the award of billions of dollars in grants annually to help communities prepare for, mitigate the effects of, and recover from major disasters. The program was intended to replace 10 disparate legacy systems (several of which had been in operation for decades) that led to labor-intensive manual processes and an increased burden for grant recipients. FEMA had previously attempted to modernize its legacy grants management systems in 2008, through a program referred to as the Emergency Management Mission Integrated Environment (EMMIE). However, that program experienced significant implementation challenges, which resulted in a solution that was missing important capabilities.

  In our April 2019 report, we found that FEMA's endeavor to modernize its grants management environment had fully addressed seven of 11, and partially addressed the remaining four leading practices for effective business process reengineering, requirements management, and cybersecurity risk management. Specifically, the program did not fully address plans for new business processes, traceability of system requirements, or security control assessments. Additionally, the program's initial cost estimate of about $251 million did not reflect key technical assumptions that had changed. Further, the program's schedule did not meet leading practices for a reliable schedule. Of particular concern was that the program's fast approaching, final delivery date of September 2020 was not informed by a realistic assessment of development activities.

  FEMA has implemented seven of the eight recommendations we made to address these issues. The agency has also taken steps toward implementing the remaining recommendation to ensure that all security controls are fully tested, but has not yet demonstrated that it fully tested all controls. In April 2023, we reported that the program had rebaselined its cost and schedule in January 2021 and had requested additional schedule relief in August 2022 related to COVID-19.[42] As a result, FEMA planned to extend its full operational

[41]GAO-19-164.

[42]GAO-23-106701.

capability date to no later than March 2024, which would be three and one-half years later than originally planned.

In summary, our June 2019 report emphasized the need and importance for agencies to develop complete plans to modernize their most critical legacy systems. DHS has done so for its most critical system that was identified in 2019. It is vital for the department to continue planning how and when it will modernize its mission-critical legacy systems. Once the department establishes such plans, further steps are needed to ensure that efforts to modernize critical legacy IT systems are successfully carried out. While DHS has implemented many of our recommendations, implementing the remaining eight for modernizing financial, biometric identity, and grants management systems would help ensure these critical legacy systems are successfully replaced.

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

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Kevin C. Walsh, Director of Information Technology and Cybersecurity, at (202) 512-6151 or walshk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Jeanne Sung (Assistant Director), Paige Teigen (Analyst-in-Charge), Lauri Barnes, and Kim LaMore.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548